Wearable Devices and Measurement Data: An Empirical Study on eHealth and Data Sharing

Ala Sarah Alaqra
Information Systems & Computer Science
Karlstad University
Karlstad, Sweden
ORID:0000-0002-6509-3792

Bridget Kane
Information Systems
Karlstad University Business School
Karlstad, Sweden
ORCID:0000-0003-3211-6529

***Abstract*—The development of medical applications and services is growing but is hampered by security and privacy concerns and a lack of trust by users. This interview study with 29 users of wearable devices reports perspectives on privacy concerns towards sharing of measured data in general, and measured stress data in the workplace. Participants consider stress data to be sensitive (73%), and report that privacy protection is a requirement for both the technology and the workplace. Sharing behavior is shown to be strongly coupled with clear purposes and incentives. Sharing measured fitness data is accepted (72%), and sharing stress measured data for the common good (48%), despite privacy concerns. Over half mistrust the technology not to leak data. Technology solutions should provide clear and sound purposes for storing, sharing, and processing measured data, as well as provide assurances from workplace and cloud.**

***Index Terms*—eHealth, cloud, privacy preserving, data aggregation, wearable devices, measurement data, data sharing, behavior, incentives, work place, stakeholders, interviews**

I. Introduction

Advancements in technology allow the development of new devices, as well as new methods for data collection and management. In the area of health technology, wearable devices facilitate data measurement and improve well being [1], [2]. Having the measuring device in a wearable form involves comfort of use and unobtrusiveness of the device [2]. Data collection mechanisms through wearable devices are steadily increasing and vary from motion trackers to motivate exercise, to vital signs measurements, such as electrocardiography (ECG) and electroencephalography (EEG), for health monitoring [1]. When it comes to communicating health data, security is critical and technologies aim to facilitate secure sharing [3]–[8]. However, addressing human factors is a necessary consideration in eHealth; by understanding users' perspectives, attitudes, concerns, and further designing and developing solutions [9]–[11]. User studies show that privacy and security concerns are required to be addressed in eHealth applications [12]–[15]. Privacy concerns are thought to have the most influence on users' intentions to share electronic medical records [14]. In our user-focused study, we investigate users' perspectives on sharing health data measured by wearable devices, and their security concerns. The main contribution of this paper is providing insights on sharing behavior and privacy concerns, and guidelines to future solutions based on our empirical results.

This work is funded by the European Union's H2020 Research and Innovation Programme, under Grant Agreement no. 786767 (PAPAYA project).

A. Health Data Protection

In primary care, the digital medical record used is referred to as an Electronic Health Record (EHR) [16], [17]. However, the collection of health data outside of primary healthcare in portals for secondary uses is often called a Personal Health Record (PHR) [18]. PHRs contain health data to be utilized and managed by the individual, for maintaining their health and wellness [16], [19]. The availability of PHRs to doctors and patients (individuals dealing with illness) allow more data for enhancing decisions, health care experiences, and thus overall well being [16], [18], [20].

Not all health data are treated equally, for example in the case of mental health, data sharing is limited due to privacy concerns, and it is argued they can hinder a patient's well being [21]. An important factor to consider is human aspects, where studies show that there are user privacy concerns regarding the EHRs, whether it is adoption attitudes [22] or behaviors [23], trust is shown to be an important consideration.

Having health data, such as PHRs, present in cloud portals, there are privacy risks and concerns to be addressed [16], [19], [24], [25]. Many studies that address electronic health data in a cloud environment, focus on privacy and security enhancing mechanisms [26]–[30].

Considering the legal aspects, there are laws that exist to regulate the protection of data. Legislation in the United States that safeguards health data, with *privacy* and *security* rules specifically, is the Health Insurance Portability and Accountability Act (HIPAA) [31]. In the European Union, the General Data Protection Regulation (GDPR) regulates protection and privacy of personal data [32]. According to Art. 4 (1) "Personal data are any information which are related to an identified or identifiable natural person", therefore health data that relate to individuals fall into the "personal data" category [33].

B. PAPAYA *use case*

The context of our work is defined by our involvement in the European Union's Horizon 2020 research project called PAPAYA: PlAtform for PrivAcY preserving data Analytics

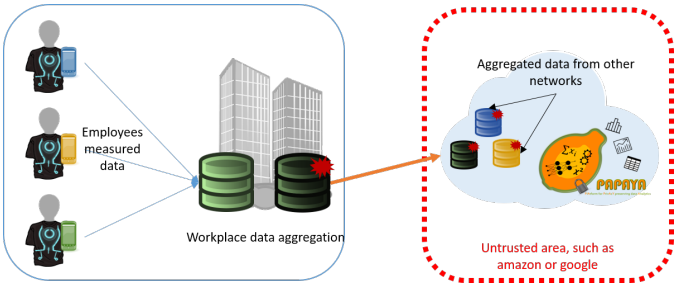

Fig. 1. use case illustration

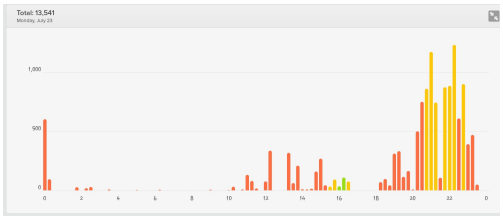

Fig. 2. Steps count throughout the day (24 hours)

[34]. In PAPAYA, machine learning is used to develop privacy preserving data analytics technologies. Having partners in industry, use cases which will benefit from PAPAYA's technologies are provided for application development [35].

The use case involves improving the working environment, specifically stress, through the research project. In that project, employees who volunteer to participate would wear a t-shirt that would collect data about their stress measurements. The data collected are aggregated by workplace and are then used to train a neural network for future stress-detection applications. Data are aggregated, anonymized, or de-identified so that no sets of raw data from a specific user are used, but instead a statistical summary, in order to preserve users' privacy. In the use case, a persona, Alex, is a fictional employee who is stressed and is considering volunteering to the project. Due to ethical considerations in our study, we asked participants to think of themselves as Alex, and respond as Alex: being employed and stressed. Thus, participants are not prompted to expose information on whether they are stressed or not. It is proposed that the company/workplace aggregates the data following its collection. Then these data are sent to the PAPAYA platform, where the company's data are combined with data from other networks for processing. The PAPAYA platform runs in a cloud, such as Amazon or Google.

C. Objective

In our study we start by investigating participants perspectives on data they believe are collected by a wearable device for a specified purpose by exploring their understanding of the types of data being collected. Our key objective to understand the main motivations and concerns for sharing measurable data so that stress-detection tools can be developed for workplaces.

II. METHOD

A structured interview, is a form of surveying where the researcher is asking predefined sequence of questions [36]. The format of structured interviews in our study, allows a uniformed questioning of participants and an agreement of their answers to the questions in case of uncertainty or misunderstanding. It allows us to survey their possible concerns regarding the technology involved, and their opinions about sharing measured data. We also inquire about the use case involving stress data sharing in workplace. In addition, a structured interview method is chosen for a couple of practical reasons, the first has to do with replicability across all interviews (interviews were conducted by two researchers), and the second is to limit possible sensitive data that is to be exposed during the interview from being recorded.

A. Participants and Sampling

We recruited participants through our personal network and social media. The main requirement is that participants are using or have used wearable devices, such as fitbit[1], to track their activity. Our reason for this requirement is because it corresponds to their mental model of being familiar with a wearable devices and its possible uses. We then sent invitation letters to those who responded containing the consent letter, and schedule of the interview. Apart from our snowball sampling, we intended to include participants with varied technical and athletic competences. Our aim is to investigate possible correlation of technical expertise to privacy awareness, and whether the athletic incentive is a drive to use and share measurable data.

B. Interview queries

The purpose of the interview was to elicit requirements concerning incentives for data sharing with PAPAYA in our Use Case. We introduced the purpose and structure of the interview, and presented the consent form. A brief demographic questionnaire was handed to them to fill out, it included: country, age group, gender, technical, and athletic backgrounds. After signing the consent forms, interviewees were given instructions not to disclose any personal health information, and were introduced to the persona called Alex.

The introduction is as follows:

"Meet Alex, who is healthy with no medical issues. He/She is using a wearable device such as Fitbit that measures his/her heart rate, movements (steps), and location. Alex is interested in the following activities for the specified reasons: (a) Track exercise activities and step count goals: to be active or lose some weight: see Figure 2; (b) Track sleep: to monitor sleep cycles and get better sleep quality: see Figure 3; and (c) A watch used to get notifications from the cellphone."

Interviewees were then asked questions on: (1) perceptions of data types collected by the device, (2) perceptions on where data are stored, (3) activities that participants would share and reasons, (4) hindrances to sharing activities data, (5) perception of sensitivity of stress measurements, (6) privacy protection

[1]https://www.fitbit.com

Fig. 3. Sleep cycles of one night and benchmark statistics

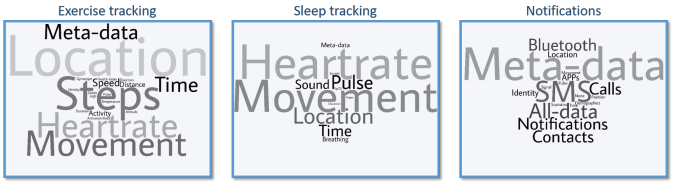

Fig. 4. Word cloud for data collected for all activities

opinions, (7) trust opinions, (8) sharing data for better results or common good, (9) incentives to motivate sharing, and (10) limitations, conditional sharing, and control.

C. Data Collection

All of our interviews took place face-to-face in Sweden and in Ireland. Each interview lasted between 25 and 35 minutes in total. Following the interview protocol, we collected and aggregated our data from our interviews into an overview record. We analyzed the data according to the themes we used for inquiry. In addition we followed by second exploratory analysis of the material for further patterns and themes.

D. Data Analysis

Since a semi-structured interview tool is used, the analysis follows the question structure. SPSS was used to manage the responses and to examine for patterns within the data. Two additional variables are constructed using Likert Scales, 'Trusting nature' and 'Concern for Privacy', based on interviewees responses to questions that revealed their expressed beliefs with regard to Trust and Privacy. Scores were independently and separately reviewed by us to improve reliability.

E. Ethical Considerations

Our study has been granted approval following the ethical review from Karlstad University. We took measures to minimize personal information exposure, such as not recording the interviews and the use of the persona "Alex" (as mentioned in Section I-B). Recording of the interviews was not required, since the format of the structured interviews allows sequential responses to specific topics. In addition to urging participants to not speak about their own personal preferences, we have excluded such comments from our results.

III. Results

Following briefing on the research and the use case, a total of 29 people consented to face-to-face structured interviews, which were conducted in 2019.

In total, 29 interviews were carried out between Ireland (10) and Sweden (12). Seven (7) interviewees prefer not to acknowledge their country of residence (where the interview was conducted). The Age range of the interviewees is between 21-60. 30% of interviewees are in the Age Group 50-60, and 27% are in Age Group 31-40. 50% of those interviewed are under 40. We achieve an almost equal gender balance among our interviewees, with 16 (53%) Males and 12 (40%) Females. One interviewee prefers 'not to say' their gender. Of the interviewees, 19 (63%) describe themselves as having a technical background and 12 (40%) as athletes. 7 (24%) describe themselves as both athletic and as having a technical background.

We summarize our findings in the following subsections that correspond to our interview topics.

1) Perceptions of Data Types collected: Typical responses to the question about the data types that are collected for the three activities are illustrated in Figure 4. Main responses for *exercise tracking* are: location (16), steps (13), heart-rate (10), and movement (10). Main responses for *sleep tracking* are: heart rate (15), movement (14), location (7), and pulse (6). Main responses for *notifications* are: metadata (11), SMS (7), all-data (5), and Bluetooth (4).

2) Perceptions on where data are stored: With regard to where these data are stored, interviewees mostly identify that the data are stored in 'the cloud' or 'server', or some specified '3rd party'. Several mentioned the company of the wearable device or that data are stored on the 'phone', 'device', or the 'app'. The instances mentioned by interviewees, some mentioned multiple locations, of where data are stored are represented in the illustrations in Figure 5.

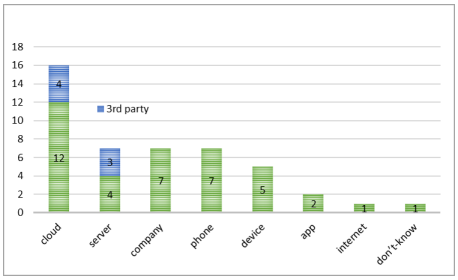

Fig. 5. Responses on where data are being stored

3) Activities that participants would share and reasons: When asked about the data that Alex might share, some say that Alex would only share certain data, and might only share a certain type of data with particular individuals, depending on the context. An overview of these responses is given in Table I. Over one-quarter (28%) would not see a need to share any of these data, while over one-fifth (21%) have no reservations about sharing any of these data. Reasons for sharing are typically 'to avail of a service' and 'if medically necessary'; to 'share with a coach or trainer', to 'compare with friends', or 'show to followers'. Location and medical data, such as heartrate, are less likely to be shared than steps or exercise as these are considered particularly private or personal. When asked with whom would Alex share data, some participants

TABLE I
ACTIVITIES THAT PARTICIPANTS WOULD SHARE

Which of the 3 activities would Alex share?	Frequency (%)
None	8 (28)
Exercise tracking only	6 (21)
Exercise tracking & Sleep data	6 (21)
Exercise tracking, Sleep data & Notifications	6 (21)
Specific Data type	3 (10)
Total	29 (100)

highlight a difference between sharing data voluntary and sharing data involuntary (i.e. necessary to use a service and allowing data to be in the cloud). For voluntary sharing of data, 31% say they would share with no-one if they are to choose, whereas 38% say they would share with friends and family only. There are 8 (28%) who say that they would share with community and common interest circles only, shown in Table II. Four of these 8 respondents are athletic and say that Alex would share for competing purposes, to compare with others within that community. Two of the 8 highlight that Alex, being 'proud of her achievements', has an incentive to share.

TABLE II
WITH WHOM WOULD ALEX SHARE THESE DATA?

With whom would Alex share the 3 activities:	Frequency (%)
No-one, n/a	7, 2 (31)
Community with common interests only	8 (28)
Friends and Family only	11 (38)
Anyone	1 (3)
Total	29 (100)

4) Hindrances to sharing activity data: Interviewees were asked about the factors that would hinder Alex from sharing any activity data, and the comments made (27) typically relate to the consequences of sharing the data. Other than two interviewees who say that if someone is interested, e.g. in a club, then they would share. Others (25) are negative and express concern about how the data might be misused, especially health data. It is felt by few that health data are private and information could be used against a person to cause embarrassment, lessen their employment prospects, impact their insurance cover or expose the individual to personalized, unwanted, marketing initiatives.

5) Perception of sensitivity of stress measurements: Following the recounting about Alex, who works at a company that would like to improve the working stress environment using the PAPAYA project, interviewees were presented with questions about stress and if there are privacy requirements on the data being encrypted.

The majority of respondents (22 (73%)) consider stress measurements as sensitive data. Three respondents (10%) say it depends on the context, and four (13%) either "Don't know" or skipped this question. One person (3%) does not consider stress measurements to be sensitive. In responding to this closed question, if stress measurements are sensitive, several interviewees made comments such as "Absolutely!", "In the case of being stressed then, yes, it's personal.", "It's a grey zone. Depends on what stress is dependent on." and "Yes, maybe. Depends to whom the data are disclosed. If family/closest family (they might know). But maybe one doesn't want work to know".

6) Privacy protection opinions: When asked if privacy protection is a requirement at the PAPAYA platform 25 (83%) say "Yes", two (7%) say "No". Two others (7%) say they "Don't know" and one person skipped this question. All of our interviewees expressed concern about their privacy. While 3 (10%) express a low concern, the majority, 24 (83%), are clearly concerned about their online privacy. The results are presented in Table III. In addition, 4 respondents state that privacy concerns in the workplace are more critical than of PAPAYA platform.

7) Trust opinions: Of those interviewed, 17 (59%) say that Alex would not trust PAPAYA not to leak data. Of those who would not trust their data not to be leaked, eleven added comments. Most would not trust that there would not be leaks regardless of assurances, and many highlighted that it doesn't necessary mean they won't use it. Two would trust their data would not be leaked, if they were give than assurance by PAPAYA, and particularly if there were a 3rd party auditor involved.

Interviewees were asked if there are any special privacy /security guarantees that should be provided (in addition). While several would not trust PAPAYA under any circumstances, others suggested that if the process were transparent and regulated at both the workplace level and PAPAYA it would help. Proof of compliance by a government authority is deemed a requirement by some, and an emphasis on protecting privacy at the workplace aggregator level was suggested by 8 of respondents.

8) Sharing data for better results or the common good: A significant proportion (14 (48%)) is willing to share their data if they can get a higher quality result, and the same proportion (48%) is willing to share their data for the common good. Thirteen of these interviewees answered 'yes' to both questions. One of the 14 who would share to obtain better quality information says 'no' to sharing for the common good; and one who would not share for improved quality of information, is willing to share if sharing will benefit others.

The reasons that 2 interviewees give for sharing their data would be: to get a better quality result, and one would wear the t-shirt in order to get a personal report. Apart from these 3 interviewees, all other comments express reservations at minimum, with most expressing a lack of trust, that 'data are too private, because it is a workplace', 'better be safe than sorry' or 'in case I am an outlier'. The notion of 'trade-off' is introduced by one, saying 'depending on the context and circumstances' and 'I'm aware that my data is money'.

9) Incentives to motivate sharing: We asked about the incentives that would motivate sharing and for some (5) nothing would motivate them to share their data. 'Having personal feedback directly to Alex' (4) or for Alex to experience a personal health benefit is cited as a potential motivator for

TABLE III
RESPONSES TO INTERVIEW QUESTIONS

Question	Frequency (%)				
	Yes	No	Unsure	Comment [# (%)]	TOTAL
Does Alex consider stress measurements as sensitive data?	22 (76)	1 (3)	3 (10)	It depends 3 (10)	29 (100)
Does Alex think that in this scenario privacy protection at the PAPAYA platform is a requirement?	24 (83)	2 (7)	2 (7)	More at workplace 8 (28)	29 (100)
Would Alex trust that PAPAYA would not leak data to e.g. Google?	5 (17)	17 (58)	3 (10)	It depends 4 (14)	29 (100)
Would Alex share/contribute data to get a better quality result?	14 (48)	13 (45)	-	Conditional 2 (7)	29 (100)
Would Alex share/contribute data for the common good (benefit of others)?	14 (48)	11 (38)	1 (3)	Conditional 3 (10)	29 (100)
Would Alex, if participating, share all or part of the data e.g. make restrictions that only data collected during working hours be used?	Share all 2 (7)	No Sharing 6 (21)	1 (3)	Only work-hours 20 (71)	29 (100)

several (9). Recognition of workplace stress was raised by several (7). If the organization were to act to reduce the stress for employees, such as by giving extra time off, or employing more staff it would be an incentive to share the stress information. Two people say that financial incentives may work. The potential incentives identified are tempered with the need to assure security and privacy of the data.

10) limitations, conditional sharing, and control: In the case where Alex would share or contribute her/his data, interviewees were asked if Alex would be willing to share all of it or not. The results are given in Table III. All except two interviewees consider it inappropriate for the employer to monitor stress outside of the workplace. A distinction is made between private at work, which might be shared with employer in instances for example where the employer is aiming to find ways to reduce workplace stress, and more 'personal private' times such as use of the toilet in working hours. Outside of the workplace is almost taboo, encapsulated in the response "Surprised!" why would they see data off-work hours!!". For the two who would agree to share, one considers that there is little difference between workplace and non-workplace data, and the second is motivated by their interest in a personal report afterwards.

We conduct analyses for patterns with respect to attitudes and gender, Age, Group, Country of residence and whether the interviewee described themselves as athletic or not, and if they have a technical background. There are no statistical differences in attitudes towards Trust or Privacy based on any of our demographic variables, except for Technical background. Those describing themselves to have a technical background appear to demonstrate less a Trusting attitude than those with no technical background Spearman's Correlation $p \leq 0.05$. We also note that although not statistically reliable, only 2 of the Irish interviewees felt that Alex would share results either to get better quality, or for the common good, suggesting that there may well be cultural differences in how individuals share their data. However, we interpret this result with caution because of our sample size and recommend further research to explore potential differences.

IV. DISCUSSION

In our study, all our interviewees had data privacy concerns, with 83% indicating that privacy protection is a requirement in the use case. However when discussing data sharing, 21 of the participants indicated that they would share a data type, an activity, or more. However, the exercise activity was mostly accepted to be shared, which is reasonable given the purpose for using the wearable device in the first place. Interestingly, those who would share with community and common interest (8) indicated that they would not share with family/friends due to lack of purpose and thus considered it privacy intrusive. Furthermore, sharing stress data, which was considered sensitive data by most, for both better quality and common good purposes was accepted by 48% of our participants. Feedback results to oneself was shown to be an incentive for sharing stress data. Our results indicate that in order to have an appropriate judgment, clear purposes/incentives are important for sharing data despite privacy concerns. In addition, social influences such as competition and common interest were motivations of sharing data by our participants (8). This relates to contextual integrity, where information flow and disclosure is based on social factors and contextual settings [37]. Clear purposes and motivating factors are key to understanding users' appropriate reasoning and their privacy behavior. Consequently, unexplained purposes, such as measuring stress data outside of office hours, has been strongly criticized by our interviewees. When it comes to hindrances for sharing data, participants mentioned consequences such as mis-use of data, which implies the need of protection and therefore sense of privacy. Acting according to fear of consequences for those experiencing privacy invasions, has been reported in the case of social media privacy invasions [38]. Trust of the workplace has been put into question for aggregating data, and workplace consequences have been mentioned. However, trusting PAPAYA has been shown to be difficult to acquire despite assurances, but it doesn't necessary mean it would hinder use. Therefore in order to facilitate trust, transparency and clear usage of data should be communicated to users.

V. CONCLUSIONS

Awareness of collected data or where it is stored has shown to be satisfactory by our participants. Privacy concerns and data protection needs are significant in our results. However, when it comes to privacy and sharing behavior, purposes and incentives, such as sharing for the common good, play a bigger role than privacy concerns. Future solutions should provide

clear purposes for storing, sharing, and processing of data, communicate incentives, and provide assurances and means to mitigate privacy and security risks from the workplace and cloud.

ACKNOWLEDGMENTS

We would like to thank Simone Fischer-Hübner for her help with the ethical approval application and interview questions.

REFERENCES

[1] M. Haghi, K. Thurow, and R. Stoll, "Wearable devices in medical internet of things: scientific research and commercially available devices," *Healthcare informatics research*, vol. 23, no. 1, pp. 4–15, 2017.

[2] Y.-L. Zheng, X.-R. Ding, C. C. Y. Poon, B. P. L. Lo, H. Zhang, X.-L. Zhou, G.-Z. Yang, N. Zhao, and Y.-T. Zhang, "Unobtrusive sensing and wearable devices for health informatics," *IEEE Transactions on Biomedical Engineering*, vol. 61, no. 5, pp. 1538–1554, 2014.

[3] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE transactions on parallel and distributed systems*, vol. 24, no. 1, pp. 131–143, 2012.

[4] B. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," *Information Systems*, vol. 48, pp. 132–150, 2015.

[5] D. Thilakanathan, S. Chen, S. Nepal, R. Calvo, and L. Alem, "A platform for secure monitoring and sharing of generic health data in the cloud," *Future Generation Computer Systems*, vol. 35, pp. 102–113, 2014.

[6] M. Johnson, M. Jones, M. Shervey, J. T. Dudley, and N. Zimmerman, "Building a secure biomedical data sharing decentralized app (dapp): Tutorial," *Journal of medical Internet research*, vol. 21, no. 10, p. e13601, 2019.

[7] D. Thilakanathan, R. A. Calvo, S. Chen, S. Nepal, and N. Glozier, "Facilitating secure sharing of personal health data in the cloud," *JMIR medical informatics*, vol. 4, no. 2, p. e15, 2016.

[8] X. Zheng, S. Sun, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Meré, "Accelerating health data sharing: A solution based on the internet of things and distributed ledger technologies," *Journal of medical Internet research*, vol. 21, no. 6, p. e13583, 2019.

[9] J. Goldman and Z. Hudson, "Perspective: Virtually exposed: Privacy and e-health: Privacy concerns are keeping consumers from reaping the full benefit of online health information." *Health Affairs*, vol. 19, no. 6, pp. 140–148, 2000.

[10] T. Sahama, L. Simpson, and B. Lane, "Security and privacy in ehealth: Is it possible?" in *2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013)*. IEEE, 2013, pp. 249–253.

[11] I. Wagner, Y. He, D. Rosenberg, and H. Janicke, "User interface design for privacy awareness in ehealth technologies," in *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2016, pp. 38–43.

[12] W. Wilkowska and M. Ziefle, "Perception of privacy and security for acceptance of e-health technologies: Exploratory analysis for diverse user groups," in *2011 5th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth) and Workshops*. IEEE, 2011, pp. 593–600.

[13] X. Bellekens, A. Hamilton, P. Seeam, K. Nieradzinska, Q. Franssen, and A. Seeam, "Pervasive ehealth services a security and privacy risk awareness survey," in *2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA)*. IEEE, 2016, pp. 1–4.

[14] M. Abdelhamid, J. Gaia, and G. L. Sanders, "Putting the focus back on the patient: how privacy concerns affect personal health information sharing intentions," *Journal of medical Internet research*, vol. 19, no. 9, p. e169, 2017.

[15] E. Vodicka, R. Mejilla, S. G. Leveille, J. D. Ralston, J. D. Darer, T. Delbanco, J. Walker, and J. G. Elmore, "Online access to doctors' notes: patient concerns about privacy," *Journal of medical Internet research*, vol. 15, no. 9, p. e208, 2013.

[16] P. C. Tang, J. S. Ash, D. W. Bates, J. M. Overhage, and D. Z. Sands, "Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption," *Journal of the American Medical Informatics Association*, vol. 13, no. 2, pp. 121–126, 2006.

[17] S. Urowitz, D. Wiljer, E. Apatu, G. Eysenbach, C. DeLenardo, T. Harth, H. Pai, and K. J. Leonard, "Is canada ready for patient accessible electronic health records? a national scan," *BMC medical informatics and decision making*, vol. 8, no. 1, p. 33, 2008.

[18] C. Safran, M. Bloomrosen, W. E. Hammond, S. Labkoff, S. Markel-Fox, P. C. Tang, and D. E. Detmer, "Toward a national framework for the secondary use of health data: an american medical informatics association white paper," *Journal of the American Medical Informatics Association*, vol. 14, no. 1, pp. 1–9, 2007.

[19] M. J. Ball, N. Carla Smith, and R. S. Bakalar, "Personal health records: empowering consumers," *J Healthc Inf Manag*, vol. 21, no. 1, p. 77, 2007.

[20] T. Irizarry, A. D. Dabbs, and C. R. Curran, "Patient portals and patient engagement: a state of the science review," *Journal of medical Internet research*, vol. 17, no. 6, p. e148, 2015.

[21] J. Greene, "Behavioral health data in the electronic health record: privacy concerns slow sharing," *Annals of emergency medicine*, vol. 62, no. 4, pp. A19–A21, 2013.

[22] C. M. Angst and R. Agarwal, "Adoption of electronic health records in the presence of privacy concerns: The elaboration likelihood model and individual persuasion," *MIS quarterly*, vol. 33, no. 2, pp. 339–370, 2009.

[23] T. Dinev, V. Albano, H. Xu, A. D'Atri, and P. Hart, "Individuals' attitudes towards electronic health records: A privacy calculus perspective," in *Advances in healthcare informatics and analytics*. Springer, 2016, pp. 19–50.

[24] A. Abbas and S. U. Khan, "E-health cloud: privacy concerns and mitigation strategies," in *Medical Data Privacy Handbook*. Springer, 2015, pp. 389–421.

[25] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *Journal of biomedical informatics*, vol. 46, no. 3, pp. 541–562, 2013.

[26] R. Wu, G.-J. Ahn, and H. Hu, "Secure sharing of electronic health records in clouds," in *8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*. IEEE, 2012, pp. 711–718.

[27] L. Demuynck and B. De Decker, "Privacy-preserving electronic health records," in *IFIP International Conference on Communications and Multimedia Security*. Springer, 2005, pp. 150–159.

[28] J. J. Rodrigues, I. de la Torre, G. Fernández, and M. López-Coronado, "Analysis of the security and privacy requirements of cloud-based electronic health records systems," *Journal of medical Internet research*, vol. 15, no. 8, p. e186, 2013.

[29] T. Ermakova and B. Fabian, "Secret sharing for health data in multi-provider clouds," in *2013 IEEE 15th Conference on Business Informatics*. IEEE, 2013, pp. 93–100.

[30] A. Alaqra, S. Fischer-Hübner, J. S. Pettersson, and E. Wästlund, "Stakeholders' perspectives on malleable signatures in a cloud-based ehealth scenario." in *HAISA*, 2016, pp. 220–230.

[31] U. D. of Health and H. Resources, ""health information privacy hhs.gov"," https://www.hhs.gov/hipaa/index.html, 1936, [Accessed on 03/05/2020].

[32] E. Union, "Regulation (eu) 2016/679 of the european parliament and of the council," *REGULATION (EU)*, vol. 679, p. 2016, 2016.

[33] "Article 4 eu gdpr "definitions"," https://www.privacy-regulation.eu/en/article-4-definitions-GDPR.htm, (Accessed on 03/05/2020).

[34] PAPAYA, "Platform for privacy preserving data analytics," https://www.papaya-project.eu/, eU H2020 project(Accessed on 11/30/2019).

[35] E. Ciceri, S. Galliani, M. Mosconi, M. Azraoui, and S. Canard, "Papaya deliverable "d2.1: Use cases and requirements"," https://www.papaya-project.eu/node/153, 2019.

[36] Y. Rogers, H. Sharp, and J. Preece, *Interaction design: beyond human-computer interaction*. John Wiley & Sons, 2011.

[37] H. Nissenbaum, "Privacy as contextual integrity," *Wash. L. Rev.*, vol. 79, p. 119, 2004.

[38] B. Debatin, J. P. Lovejoy, A.-K. Horn, and B. N. Hughes, "Facebook and online privacy: Attitudes, behaviors, and unintended consequences," *Journal of computer-mediated communication*, vol. 15, no. 1, pp. 83–108, 2009.