

ESSENTIAL DESIGN COMPONENTS OF GENETIC DATA ENABLED MOBILE  
PERSONAL HEALTH RECORD SYSTEMS

A THESIS SUBMITTED TO  
THE GRADUATE SCHOOL OF INFORMATICS OF  
THE MIDDLE EAST TECHNICAL UNIVERSITY  
BY

ÖZLEM ÖZKAN

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF  
DOCTOR OF PHILOSOPHY  
IN  
THE DEPARTMENT OF MEDICAL INFORMATICS

JULY 2018



ESSENTIAL DESIGN COMPONENTS OF GENETIC DATA ENABLED MOBILE  
PERSONAL HEALTH RECORD SYSTEMS

Submitted by Özlem ÖZKAN in partial fulfillment of the requirements for the degree of  
**Doctor of Philosophy in Medical Informatics Department, Middle East Technical  
University** by,

Prof. Dr. Deniz Zeyrek Bozşahin  
Dean, **Graduate School of Informatics**

\_\_\_\_\_

Assoc. Prof. Dr. Yeşim AYDIN SON  
Head of Department, **Health Informatics**

\_\_\_\_\_

Assoc. Prof. Dr. Yeşim AYDIN SON  
Supervisor, **Health Informatics Dept., METU**

\_\_\_\_\_

Assist. Prof. Dr. Arsev Umur AYDINOĞLU  
Co-Supervisor, **Science and Technology Policy Studies,  
METU**

\_\_\_\_\_

**Examining Committee Members:**

Prof. Dr. Tolga CAN  
Computer Engineering Dept., METU

\_\_\_\_\_

Assoc. Prof. Dr. Yeşim AYDIN SON  
Medical Informatics Dept., METU

\_\_\_\_\_

Prof. Dr. Ahmet COŞAR  
Computer Engineering Dept., Turkish  
Aeronautical Association University

\_\_\_\_\_

Assist. Prof. Dr. Harun KAYGAN  
Industrial Design Dept., METU

\_\_\_\_\_

Assist. Prof. Dr. Rahime BELEN SAĞLAM  
Computer Engineering Dept., Yıldırım Beyazıt  
University

\_\_\_\_\_

**Date: 09.07.2018**



**I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.**

**Name, Last name : Özlem ÖZKAN**

**Signature : \_\_\_\_\_**

## **ABSTRACT**

### **ESSENTIAL DESIGN COMPONENTS OF GENETIC DATA ENABLED MOBILE PERSONAL HEALTH RECORD SYSTEMS**

**ÖZKAN, Özlem**

Ph.D., Department of Health Informatics

Supervisor: Assoc. Prof. Dr. Yeşim AYDIN SON

Co- Supervisor: Assist. Prof. Dr. Arsev Umur AYDINOĞLU

July 2018, 145 pages

The rapid growth in the use of genetic tests in healthcare has opened a new discussion on the redesign of electronic health records to cover genetic/genomic data. Today, this information is treated in the same way as ordinary health data. However, genetic data has many unique properties that raise concerns about privacy and security issues. Moreover, in many countries, there are specific laws and regulations to protect genetic/genomic data. We recommend PHR systems for this purpose since they are under the full control of the owner and thus have a great potential to address privacy concerns. Therefore, we carried out four sub-studies in order to identify critical design issues of genetic data-enabled mPHRs in the scope of this dissertation. First, current mPHRs available in application markets were evaluated to see what was included in existing applications and to identify the missing aspects. Second, with the help of the mPHR analysis results, a survey was developed and administered to 174 people, half of whom had genetic test experiences, to assess the public's concerns and views on genetic data being included in the mPHR. Third, 11 participatory design sessions with five participants were held. At the end of the meetings, a sample paper prototype of genetic data included in the mPHR was developed. Lastly, two focus group studies on the collection of genetic data and confidentiality of Turkish health information systems were organized with 18 experts. As a result of these studies, characteristics and necessities of a genetic data-enabled mPHR were determined.

**Keywords:** genetic data management, mobile personal health records, personal data privacy, personal data protection laws

## ÖZ

### GENETİK VERİLERİN DAHİL EDİLDİĞİ MOBİL KİŞİSEL SAĞLIK SİSTEMLERİ İÇİN GEREKLİ TASARIM BİLEŞENLERİ

ÖZKAN, Özlem

Doktora, Tıp Bilişimi Bölümü

Tez Yöneticisi: Doç. Dr. Yeşim AYDIN SON

Tez Yönetici Yardımcısı: Dr. Öğr. Üyesi Arsev Umur AYDINOĞLU

Temmuz 2018, 145 sayfa

Genetik testlerin sağlık alanında kullanımındaki hızlı artış, elektronik sağlık kayıtlarının genetik/genomik verileri kapsamı için yeniden tasarlanması konusunda yeni bir tartışma başlatmıştır. Bugün genetik veriler, sıradan sağlık kayıtlarıyla aynı şekilde değerlendiriliyor. Fakat, genetik verilerin gizlilik ve güvenlik konusunda endişeleri arttıran, kendisine has birçok özelliği ve hatta birçok ülkede uygulanan, genetik veriye özel yasa ve regülasyonlar var. Biz genetik verinin yönetimi için, veri sahibine kendi verisi üzerinde tam kontrol vererek gizlilik ve güvenlik endişelerini giderebilecek potansiyele sahip olduğundan Kişisel Sağlık Kayıtları (PHR) sistemlerini öneriyoruz. Bu nedenle de, bu tez kapsamında, genetik/genomik verileri içeren bir mobil PHR'nin temel tasarım bileşenlerini belirlemek için, dört farklı alt çalışma düzenledik. Uygulama marketlerinde bulunan mevcut mobil PHR uygulamaları değerlendirildi ve eksikliklerini tespit edildi. İkinci çalışma olarak, bu analiz sonuçları baz alınarak, halkın endişe ve görüşlerine ulaşmak için, bir anket geliştirildi ve yarısı genetik test deneyimleri olan 174 kişiye uygulandı. Üçüncü çalışmada, beş katılımcı ile birlikte 11 katılımcı yaklaşımli tasarım oturumu organize edildi ve toplantıların sonucunda genetik verilerin bulunduğu örnek bir mPHR prototipi tasarlandı. Son olarak, 18 uzmanın katılımıyla, genetik verilerin toplanması ve Türk sağlık bilgi sistemlerinde gizlilik konularında iki odak grup çalışması organize edildi. Tüm bu çalışmaların sonucu olarak, genetik verileri de içeren bir mPHR'nin karakteristik özellikleri ve gereksinimleri belirlendi.

Anahtar Sözcükler: genetik veri yönetimi, mobil kişisel sağlık kayıtları, kişisel verilerin gizliliği, kişisel verileri koruma yasaları

*To My Loves, Onur & Ulař*



## ACKNOWLEDGMENTS

During the course of this study, I got married, had a baby, changed the city, even the country I lived in and reached the age of 35. As a result, writing this dissertation has been one of the most challenging experiences and one of the most important achievements of my life. It means much more than a degree, and I am grateful to many people for making this possible.

I am most grateful to my darling and my best friend *Onur TIKİN*. He always supported my work from the beginning to the end of my PhD. Even in the most negative moments, this support never diminished. And of course, to Ulaş: He may have been the biggest obstacle in the path of my study, but he was also the funniest and happiest baby in the world during my thesis work. I would like to say special thanks to my heart Ulaş for making me the happiest mom in the world, and my son, if one day you read this, know that I was always feeling sorry for the nights that I had to go while you were crying.

I am greatly appreciative of my supervisor *Yeşim AYDIN SON* and my co-supervisor *Arsev Umur AYDINOĞLU* for their guidance and support throughout my study. They never lost their confidence in me.

I am grateful to the members of the thesis examining committee for their valuable directions and comments.

I would like to give special thanks to my mother *Ayşe ÖZKAN* for being the most talented woman in the world. Without her, it would have been much harder to finish this dissertation. My other family members, my father *Hasan*, my siblings *Orbay* and *Çiğdem* never let me feel alone during this period.

I would like to express my deepest gratitude to my dear friends *Meltem ŞEYHUN*, *Tansel MENGÜLOĞUL*, *Nurcan ALKIŞ*, *Sibel GÜLNAR*, *Neşe SEVİM*, *Çağlar FETTAHOĞLU*, *Defne ALTIÖK*, *Okan Bilge ÖZDEMİR* and *Melike ŞAHİNOL* who helped me with my dissertation efforts and/or encouraged me psychologically at any time I needed it. I feel very lucky for having such good friends.

Also, many of my other friends, especially *Kübra NARCI*, *Burcu YALDIZ*, *Alper DÖM*, *Onur BALOĞLU* and *Ahmet YALÇIN* were all great at sharing their knowledge and experiences during design meetings. I would like to say thank you again for sharing your valuable support and time with me.

The help of *Türk Tabibler Birliği*, especially *Av. Mustafa GÜLER* and *Av. Özgür ERBAŞ* is gratefully acknowledged. They were ready to support me with their valuable knowledge and experiences whenever I needed it

I would like to thank all participants of the meetings whose names are kept confidential for their contributions.

I am thankful to the *Staff of Informatics Institute, especially to Hakan GÜLER*, for their help at every stage of the bureaucratic procedure. I am also grateful to my thesis committee for their suggestions and valuable comments.

Lastly, I want to give my thanks to the cafes and libraries which allow researchers to use their workplaces, internet access, and/or resources without demanding anything in return: to S-café, to all Starbucks, to Jacob und Wilhelm Grimm, and to Salt Galata.

## TABLE OF CONTENTS

ABSTRACT .....	iv
ÖZ .....	v
DEDICATION .....	vi
ACKNOWLEDGMENTS.....	vii
TABLE OF CONTENTS .....	ix
LIST OF TABLES .....	xii
LIST OF FIGURES .....	xiii
LIST OF ABBREVIATIONS.....	xiv
CHAPTERS	
1. INTRODUCTION .....	1
1.1. Background .....	1
1.2. Motivation .....	2
1.3. Contributions of the Study .....	2
1.4. Organization of the Dissertation.....	3
2. BACKGROUND AND LITERATURE REVIEW.....	5
2.1. Data Privacy, Confidentiality and Security .....	5
2.2. Privacy and Confidentiality of Genetic Data .....	6
2.3. Health and Genetic Records in a Digital Environment .....	8
2.4. Personal Health Records and Personal Health Record Systems .....	9
2.5. Security of PHRs: Security Safeguards in Online Banking .....	10
2.6. Legal Issues Regarding Protection of Personal Data Internationally.....	12
2.7. Legal Status of the Protection of Personal Data in Turkey .....	15
2.8. Design Considerations.....	18
2.9. Summary of Background and Literature Review .....	19
3. MATERIALS AND METHODS.....	21
3.1. Analysis of Mobile Personal Health Record Applications.....	22
3.2. Survey Development .....	22
3.2.1. Pilot Study for the Assessment of the Survey.....	23
3.2.2. Ethics Clearance.....	25
3.2.3. Data Collection .....	25
3.2.4. Data Analysis .....	25
3.3. Participatory Design (PD) Meetings .....	25
3.3.1. Participatory Design.....	26
3.3.2. PICTIVE Technique .....	26
3.3.3. Participants.....	27
3.3.4. Focus Group Study with Potential Users and System Designers.....	28
3.4. Focus Group Meetings .....	28

3.4.1. Participants and Procedures .....	29
3.4.2. Data Analysis .....	30
3.5. Summary of Methods .....	30
4. RESULTS.....	33
4.1. Analysis of Mobile Personal Health Records (mPHR) Applications.....	33
4.1.1. Search, Identify and Download the mPHR Applications.....	33
4.1.2. Elimination of mPHR Applications .....	33
4.1.3. Analysis According to the Pre-Defined Criteria .....	35
4.1.4. Turkish Mobile Applications in the Markets .....	38
4.1.5. Data Elements and Features Covered by Applications .....	39
4.2. The Survey.....	39
4.2.1. Results of the Pilot Study .....	39
4.2.2. Participant Profile:.....	40
4.2.3. Reliability Analysis (Cronbach’s Alpha):.....	40
4.2.4. Survey Results.....	42
4.2.5. Demographics of Respondents.....	42
4.2.6. Level of Knowledge and Experiences on Health and Genetic Data .....	42
4.2.7. Attitudes Towards Health and Genetic Data Exchange .....	43
4.2.8. Views on Mobile Applications for Health/Genetic Data Management .....	45
4.2.9. Differences Between Groups .....	47
4.3. PD Workgroup.....	49
4.3.1. Session I .....	50
4.3.2. Session II .....	51
4.3.3. Session III.....	52
4.3.4. Session IV. ....	53
4.3.5. Session V.....	54
4.3.6. Session VI. ....	54
4.3.7. Session VII. ....	56
4.3.8. Session VIII.....	57
4.3.9. Session IX. ....	58
4.3.10. Session X.....	58
4.3.11. Session XI. ....	59
4.3.12. UML, Workflow and Dataflow Diagrams .....	60
4.4. Analysis of Focus Group Meetings .....	64
4.5.1. Lack of Access and Usage Regulations for Medical Data, E-Nabız.....	64
4.5.2. Management of Genetic Information in Electronic Health Records.....	70
4.5.3. Government’s Business Culture.....	73
4.5.4. Public Perception of Risks, Government Failure, Mishandling of Data.....	75
4.5. Summary and Conclusion of the Results.....	77
5. DISCUSSION .....	79
5.1. mPHR Analysis .....	79

5.2. The Survey .....	80
5.3. PD Workgroup .....	83
5.4. Focus Group Meetings .....	85
6. CONCLUSION.....	89
6.1. Limitation and Future Work.....	92
REFERENCES.....	95
APPENDICES .....	119
APPENDIX A .....	119
APPENDIX B .....	120
APPENDIX C .....	121
APPENDIX D.....	123
CURRICULUM VITAE .....	143

## LIST OF TABLES

Table 1 Countries with data privacy laws between 1973 and 2016 (Greenleaf, 2017)....	13
Table 2 Survey work flow .....	22
Table 3 Health and genetic information security questions .....	24
Table 4 Detail of PD group participants.....	27
Table 5 Details of focus group meeting participants.....	30
Table 6 Excluded applications .....	34
Table 7 mPHR applications in AppStore .....	36
Table 8 mPHR applications in Google Play.....	37
Table 9 Evaluation of e-Nabız .....	38
Table 10 Average percentage of mPHR data elements and features .....	39
Table 11 Frequency of family income, computer and smart phone literacy.....	40
Table 12 Responses to the item, “Have your medical records ever been inappropriately used or released without your consent?” .....	43
Table 13 Responses to the item, “Have you ever asked a doctor not to write down your health problem in your medical records, or asked the doctor to put a less serious or less embarrassing diagnosis into the record than was actually the condition?” .....	43
Table 14 Responses to the item, “Do you trust the following stakeholders to keep your genetic and medical data private?” .....	44
Table 15 Respondents’ views about the effectiveness of regulations proposed to protect their privacy and confidentiality .....	44
Table 16 Responses to the item, “What do you think about the security risks of storing the following information in a mobile application?” .....	45
Table 17 Cross tabulation of the participants’ views on storing bank account information in mobile applications and their experience with online banking .....	46
Table 18 Participants’ views on their children’s access to their genetic and medical data by age group. (The post-hoc computed achieved power for $w=0.3$ , $\alpha=0.05$ and $n=154$ was 96.1%).....	48
Table 19 Participants’ views on their doctor’s access to their genetic and medical data by level of computer and smartphone literacy. (The post-hoc computed achieved power for $w=0.3$ , $\alpha=0.5$ , and $n=160$ was 96.6%) .....	49

## LIST OF FIGURES

Figure 1 Special categories of data types in GDPR, Turkish PDP law, and EU Directive 95/46/EC .....	17
Figure 2 Methodological work flow followed during the study .....	21
Figure 3 Types of information the users wanted to see in a mobile health record application .....	45
Figure 4 Security features the participants would like to see in an internet-based health/genetic data record system .....	47
Figure 5 Comparison of the views of women and men regarding the rights of their spouse to access genetic data in their medical records (The post-hoc computed achieved power for $w=0.3$ , $\alpha=0.05$ and $n=165$ was 97.0%) .....	48
Figure 6 Comparison of the views of university graduates and those from other educational backgrounds regarding the rights of their doctor to access genetic data in their medical records (The post-hoc computed achieved power for $w=0.3$ , $\alpha=0.5$ , and $n=160$ was 96.6%) .....	48
Figure 7 UML Diagram .....	61
Figure 8 Dataflow Diagram .....	62
Figure 9 Workflow diagram .....	63
Figure 10 Summary of the data elements determined in PD Group, Survey, and mPHR analysis .....	84

## LIST OF ABBREVIATIONS

<b>EHR</b>	Electronic Health Records
<b>FG</b>	Focus Group
<b>GDPR</b>	General Data Protection Regulation
<b>MHR</b>	Medical Health Records
<b>mPHR</b>	Mobile Personal Health Record
<b>PD</b>	Participatory Design
<b>PDP</b>	Personal Data Protection
<b>PDPB</b>	Personal Data Protection Board
<b>PHR</b>	Personal Health Record



## CHAPTER 1

### INTRODUCTION

#### 1.1. Background

Human genome research has had an important impact on healthcare since the sequencing of the entire genome was first announced to be completed in 2003 (Guttmacher & Collins, 2003). Integration of genetic test results or personal genomic data into the electronic health records has become an emerging issue as genetic testing is utilized more often for the diagnosis of an increasing number of diseases. Especially in recent years, we have witnessed an impressive increase in genome sequencing as it has become much more affordable. It is predicted that many of the citizens in developed countries will have their genomes sequenced within the next ten years (Ayday, De Cristofaro, Hubaux, & Tsudik, 2015) and as an expected result, the amount of genetic information included in health records will increase continuously. The inclusion of genetic/genomic information in electronic records can have a great impact on personalized healthcare by informing physicians and patients about disease risks, differential diagnoses, or the appropriate doses of drugs, while assisting in the selection of effective treatment and preventive actions (McGuire et al., 2008). However, there are many unanswered questions about where, when, and how to conduct genetic/genomic data management in electronic health records (Shoenbill, Fost, Tachinardi, & Mendonca, 2014). Current electronic health record (EHR) systems handle genetic data like any other laboratory test results; however, EHR systems should be redesigned in order to be more efficient and secure for genetic/genomic data (Shoenbill et al., 2014). The privacy and confidentiality of genetic/genomic data presents unique challenges compared to other personal information (Ayday, Raisaro, Hubaux, & Rougemont, 2013; McGuire et al., 2008) due to its specific features (Alahmad, Hifnawy, Abbasi, & Dierickx, 2016).

Sooner or later, genetic data will find its place within electronic health records. According to Scheuner et al. (2009), patient portal/patient-entered data was considered the best method for genetics/genomics data because it should be managed where the owner feels secure. Hence, operations such as updating, deleting, and sharing should only be performed with authorization by the data owner. Furthermore, a privacy-by-design approach should be the basis for developing PHR applications, and these applications should have high security protection features to minimize disclosure risks. However, designing even the most private and most secure application may not be enough on its own unless the privacy of data is protected by governments through laws and regulations. As of 2017, personal data privacy is guaranteed by legal rules in 120 countries (Greenleaf, 2017). Turkey has been the most recent of these countries since the personal data protection law and related

regulations entered into force in 2016. However, there are many debates about these new legal developments, which have even been challenged in court. Besides domestic criticism, the European Commission, in the Turkey 2018 Report (EU Turkey 2018 Report, 2018, p. 42), asserted about the Turkish Personal Data Protection (PDP) law that “it is not yet in line with European standards” and it does not match the standard for data transfer with Europol.

## **1.2. Motivation**

The main purpose of this study is to identify all aspects of a personal health record system that includes genetic data: the visual components (data elements and features) and issues related with security, privacy, and ethics to be addressed in order to enable the inclusion of genetic/genomic data in health systems. For this aim, first, we analyzed mobile personal health record (mPHR) applications available in mobile application markets; second, we developed a survey to identify the public’s security and privacy concerns regarding genetic/health data in mobile health record systems; in parallel with the survey, we organized participatory design workgroups with potential users and designers of the application. Lastly, we held two focus group meetings with experts on privacy, confidentiality and security of Turkish health information systems, data privacy regulations, and management of genetic data.

In this way, we answered the following research questions:

- What are the essential characteristics of a health record application for the inclusion of genetic/genomic data?
- What are the opinions of ordinary users, stakeholders and experts on design issues of the application?
- What kind of security protections and regulations are needed for the application to reduce the public’s concerns about security and privacy?
- What are the ethical and legal problems of the Turkish electronic health system for health and genetic data exchange?

## **1.3. Contributions of the Study**

First of all, as a main outcome, the essential components of a genetic data-enabled PHR application were identified. The necessities of such a PHR design were elaborated under many aspects: besides the components of the application, interoperability with the Turkish health system and compliance with international and Turkish personal data protection laws were taken into consideration. In addition, necessary security measures to protect the privacy of genetic/genomic information were discussed within the scope of this dissertation.

There is plenty of research on PHRs in the international literature; therefore, when we did a search with the string “Personal Health Records” in Google Scholar, we found more than 3,280,000 results. Furthermore, there are many studies in the literature focusing on privacy and security issues of genetic data storage (Andrews & Jaeger, 1991; Belmont & McGuire, 2009; Carman & Britten, 1995; Hoffman, 2007; Lunshof, Chadwick, Vorhaus, & Church, 2008; McGuire et al., 2008).

Although we reached more relevant studies when the search was filtered, they covered only subparts of our study. For instance, there is research into PHR design inspired by banking systems (Botts, Horan, & Thoms, 2011) whose main idea is to design a personal health system that should be as easy to use as an ATM machine. However, it is not taking into consideration either the security measures of banking or the handling of genetic test data (ibid.). Even though some online banking security methods are in use for health information exchanges, such as ID password type and security cards (Smith & Eloff, 1999), this dissertation is proposing many additional safeguards. Adapting online banking security systems to a PHR is not researched in the literature. In that sense, this study is a first.

When searched the database of the Turkish National Thesis Center with the keywords “Personal Health Records,” “Genetic Records,” “Security/Privacy of Genetic Data,” and “Genetic Data in Health Records”, we reached six relevant theses related with Personal Health Records only (Almadani, 2016; Beyan, 2014; Canbay, 2014; Özdemir, 2010; Postacı, 2012). Five of these theses are not dealing with the security or privacy of genetic data or its inclusion in electronic records or the design of personal health record applications including genetic information. However, a PhD thesis written in the History of Medicine and Ethics Program of Kocaeli University aimed to examine the attitudes and opinions of physicians and subjects towards using genetic information in a clinical setting (Akpınar, 2010). The work is based on case studies asking the opinions and attitudes of physicians and subjects on each case.

When the literature in Turkey on the inclusion of genetic/genomic information was searched via Google Scholar, it was seen that there was a lack of studies in Turkey that investigate patients’ and practitioners’ experiences and preferences regarding the inclusion of genetic/genomic information in an electronic environment. These results will lead future studies on the development of other frameworks and security applications. To sum up, after these searches were completed, it was seen that the research topic would be an original contribution to the literature.

#### **1.4. Organization of the Dissertation**

The dissertation consists of six main chapters, namely Introduction, Background and Literature Review, Materials and Methods, Results, and Discussion and Conclusions. Details for the four sub-studies of the dissertation are given in the chapters Materials and Methods, Results, and Discussion.



## CHAPTER 2

### BACKGROUND AND LITERATURE REVIEW

This chapter briefly discusses the background and literature related to this study. The literature review is laid out in eight main sections: (1) data privacy, confidentiality and security; (2) privacy and confidentiality of genetic data; (3) health and genetic records in a digital environment; (4) personal health records and personal health record systems; (5) security of PHRs: security safeguards of online banking; (6) legal issues regarding protection of personal data internationally; (7) legal status of the protection of personal data in Turkey; and (8) design considerations. The chapter is concluded with summary of background and literature review section.

#### 2.1. Data Privacy, Confidentiality and Security

Privacy, confidentiality, and security are often confused since the differences between them are somewhat minor. Privacy is the right of a person to keep his or her personal information secret. On the other hand, confidentiality is a guarantee that identity information is not disclosed without the consent of the owner. Finally, security is a mechanism implemented in a system in order to provide privacy and confidentiality of the information (O'Brien & Yasnoff, 1999).

Confidentiality and privacy have always been controversial topics. The amount of data is continuously increasing. However, privacy concerns are growing in parallel with this increase. Recent news about data leaks in online information systems has an important impact on this skepticism. For example, 70 million customers of the second-largest discount retailer of the U.S., Target Corporation, were affected by hacking in November 2013. Besides the customers' personal information, their credit card information including verification number was accessed (McGrath, 2014). In the same year, one of the biggest healthcare companies of the United States, Anthem Inc., was in the headlines. Again, as many as 80 million U.S. subscribers' data, including social security numbers, addresses, and even employment information were exposed (Riley, 2015). The situation is not much better in Turkey. In addition to the media reporting on smaller privacy breaches on a daily basis, only in the past six years there was news about two serious situations relating to a breach of confidentiality. First, in November 2012, the Social Security Institution (SGK) sold millions of health records of Turkish citizens illegally ("SGK plan to sell health data to global pharma creates controversy", 2012; Kaya, 2018) and in April 2016, the personal details of 50 million Turkish citizens were leaked online (Tait, 2016).

Especially when the information is sensitive, the debates concerned are very challenging. Data records related with healthcare, finance, education, and employment are protected by privacy laws all over the world. Among these types of

data, health and genetic information is of special importance, and therefore there is an act specifically to protect the privacy of health data, called the Health Insurance Portability and Accountability Act (HIPAA). In addition, the EU General Data Protection Regulation (GDPR) specifies stricter rules for health and genetic data separate from any other kind of data. Genetic data is accepted to be the most confidential personal data (Ayday et al., 2015; McGuire et al., 2008) due to its unique properties. Furthermore, it is of special importance as it is related with private issues not only for the owner but also affecting his or her relatives (Alahmad et al., 2016).

## **2.2. Privacy and Confidentiality of Genetic Data**

Genetic information is of particular importance compared to all other kinds of sensitive information (Ayday et al., 2015; McGuire et al., 2008). Genetic/genomic information has several characteristic features that should be considered as requiring an appropriate level of protection (McGuire et al., 2008):

- **Uniqueness:** Except from identical twins, the genetic code of each individual is unique. Therefore, consolidated databases of genetic/genomic information could easily be mined and abused for identification purposes.
- **Predictive capability:** Genetic/genomic tests help to predict the likelihood of developing a given disease or the response to a specific drug. While this information is very valuable to inform preemptive action, it may also be used to discriminate based on predisposition.
- **Requirement of testing:** In contrast with other medical data, many genetic markers cannot be ascertained in the normal course of clinical care; they must be derived from a genetic/genomic test.
- **Historical misuse:** Eugenics initiatives, insurance companies and workplaces may be inclined to misuse genetic information.
- **Variation in public knowledge and perspectives:** There is wide variation in the individual understanding of the role of genetics in health and disease, personal sensitivity regarding genetic/genomic test information, and feelings about genetics.
- **Impact on family:** Genetic/genomic test information also has the potential to impact an individual's family members, as germline mutations (i.e., mutations contained in the sperm or egg that may be passed on to the offspring) may reveal information about medical risks of blood relatives. Thus, an individual's decision to undergo a genetic/genomic test could reveal information that suggests risks for relatives to develop a chronic or debilitating disorder.
- **Temporality:** Societal perspectives, the ability to interpret genetic/genomic test information and policies regarding the use of such information in healthcare decision-making will likely evolve over time.
- **Ubiquity and ease of procurement:** Genetic material is easy to procure. DNA can be obtained from saliva, blood, hair, and other tissues being shed. Thus,

an individual's genomic information can be readily obtained without his/her knowledge or permission.

These features give rise to a variety of ethical concerns and potentials for discrimination based on genetic background in areas such as employment or insurance (Hoffman, 2017; Joly, Ngueng Feze, & Simard, 2013; Knoppers & Godard, 1998; Mohammed et al., 2017; Sherwin & Simpson, 1999; Sommerville & English, 1999). However, there is no comprehensive security solution for protecting the privacy of genomic data. Even though several de-identification and aggregation techniques have been offered for the protection of privacy and security of EHR systems, their use in personal genomic data is limited since the genome itself is the ultimate identifier of an individual (Malin, 2005). Today, although privacy of genomic data is still an issue, the literature contains only a limited number of studies that propose solutions (Akgün, Bayrak, Ozer, & Sağıroğlu, 2015).

Despite the fact that genome sequences offer numerous opportunities, there are growing privacy and security concerns among the public as reported, among others, in the US by the Presidential Commission for the Study of Bioethical Issues (2012). In the EU and in the Turkish PDP Law no. 6693, genetic data is listed under special categories of personal data. In the United States, there is the Genetic Information Nondiscrimination Act (GINA) specifically regulating the usage of genetic data. By this regulation, the use of genetic information in health insurance and employment is prohibited (Jones, 2012). GINA was signed by President George W. Bush on May 21, 2008 and aimed to ensure that people can benefit from health insurance without discrimination due to genetic differences and to protect employees and applicants from genetic discrimination (Jones, 2012).

Concerns about privacy and confidentiality of genetic information have also been studied in the literature. Attitudes toward genetic testing of Finnish people were reported in a survey from 1995 (Hietala et al., 1995). In this controlled study, 82 AGU (Aspartylglucosaminuria) patients' relatives and a total of 1,169 Finnish people were enrolled. The results revealed that both groups had a positive attitude toward genetic testing. However, discrimination in employment or insurance policies is a commonly expressed reason to reject testing.

Henneman et al. (2013) made a comparison of the results of their questionnaires on public attitudes towards genetic testing administered in 2002 and again in 2010. Their results showed how people's thoughts and concerns about genetic testing had changed. While expectations of benefits and potential usefulness of genetic testing increased among the public in the specified time interval, concerns about inequity remained.

There was a more recent exploratory survey from Saudi Arabia about medical and genetic data confidentiality in the Saudi research biobank including 200 participants from Saudi Arabia (Alahmad et al., 2016). The participants consisted of five groups of equal size, comprised of researchers, physicians, medical students, donors, and laypersons. According to the majority of the participants' opinions, confidentiality of medical/genetic information is a necessity.

A study based on phone interviews was conducted with 30 respondents for two National Institutes of Health research protocols using genomic sequencing (Jamal,

2014). The respondents thought that the genome science was valuable; nevertheless, actions should be taken against discriminatory use of individual genome data.

According to the results of a survey on the impact of privacy concerns and awareness on sharing personal genetic information (n=273), people were mostly aware of the benefits of genome sciences but they were concerned about the privacy of their data (Heath, Ardestani, & Nemati, 2015). The international literature on people's opinions and attitudes regarding genetic confidentiality is quite broad; however, none of the available studies focuses on mobile and personalized health record systems. Similarly, such studies are lacking in Turkey as well.

### **2.3. Health and Genetic Records in a Digital Environment**

There are many different names used for systems keeping health records electronically. Even though the terms Electronic Medical Record (EMR), Electronic Health Record (EHR) and Personal Health Record (PHR) are sometimes used interchangeably, they do not refer to a single concept (Zhang & Liu, 2010). EMRs and EHRs are recorded and updated by authorized people, mostly by healthcare practitioners, while PHRs enable patients to manage their own health histories. EHR is used as a general term for keeping health records electronically as it is designed to hold information about all aspects of patients' wellbeing, while EMRs only hold electronic records of diagnoses (Garets & Mike, 2006). In short, EHR is a superset of EMR, while PHRs cover both lifestyle and medical records data in a personalized manner.

Privacy and security are the two prerequisites for applications working with sensitive information such as health data (Martínez-Pérez, Torre-Díez, & López-Coronado, 2015). Goldman (1998) indicated that patients cannot participate in their own healthcare completely without trust, as they have to share sensitive personal information with their doctors.

There is a myriad of research in the literature about people's perception regarding privacy of health data, especially in an electronic environment. A meta-study (Sankar, Mora, Merz, & Jones, 2003) examined 110 articles covering patient perspectives on medical confidentiality. The results can be summarized under four headings: people do not know which medical data is protected and how. Secondly, they are mostly concerned about specific issues, such as whether the doctor has shared their information with other hospital staff or if the data were seen by someone while they were going to the clinic, etc. Thirdly, they preferred health information to be used only for their treatments. The last and most alarming finding was that patients tend to postpone or forgo treatment due to worries about their privacy and/or they are hiding or altering their medical history because of concerns about privacy (Sankar et al., 2003).

Results of another survey, conducted in 2011 in Turkey (n=596), also revealed similar attitudes and opinions about medical data privacy (Özkan, 2011). According to these results, people are worried about the privacy and confidentiality of their personal information. In addition, they are mostly not sure about safety and security



of their health data in Turkey, and they are mostly unaware of their current rights to personal data privacy.

Furthermore, two government-funded telephone-based questionnaire studies carried out in Canada and the U.S., respectively, support these observations. The Canadian study enrolled 2,469 subjects (Canada Health Infoway & EKOS Research Associates, 2007) and the American project included 2,100 persons (Princeton Survey Research Associates, 1999). Both questionnaires were aimed at understanding the public's opinion about the privacy of medical records and to understand in how far the level of concern is important for healthcare users. The results of both surveys revealed high levels of concern about the safety and security of personal health information. In addition, while Canadians have a modest level of awareness, Americans were unaware of their rights.

Surely, genetic/genomic data should be a part of the health records. The inclusion of genetic/genomic information into electronic health records will greatly impact personalized healthcare by informing disease risk determination, appropriate drug dosage, and the selection of effective treatment or preventive action, yet the problem of security and privacy should be solved urgently before adoption of these records (McGuire et al., 2008). Since 2003, when the Human Genome Project (HGP) was concluded, genomic data has been increasing gradually and it has become a problem to keep records and to extract the necessary information from them.

Scheuner et al. (2009) conducted a project to assess genetic/genomic content in electronic health records. They had interviews with 4 different groups: primary care clinicians, medical geneticists, genetic counselors, and EHR representatives (senior management of companies marketing commercial EHR products and health information specialists or managers of EHR products developed within the health system). When the participants were asked which EHR data elements or functionality relating to genetics/genomics would be useful to clinicians, "Patient portal/patient-entered data" was considered the best health data recording method for exchanging genetics/genomics data (Scheuner et al., 2009). Furthermore, healthcare stakeholders such as policy-makers, healthcare providers, and health sector managers now attribute more importance to PHRs due to the positive feedback from patients' involvement in healthcare activities (Maria Piras & Zanutto, 2014). Additionally, according to the results of research conducted by Ford, Hesse and Huerta (2016), PHRs have a high adoption potential in the near future.

#### **2.4. Personal Health Records and Personal Health Record Systems**

The National Committee on Vital and Health Statistics report (2006) brought together the ideas of healthcare providers, patients, employers, funders, and societal/population health benefits stakeholders on key potential benefits of PHRs and PHR systems in the U.S.A. Among the most popular answers were the following:

- Improve patients' awareness of their health, self-care activities and disease prevention

- Improve sense of control over his/her records
- Making access to data of other doctors and patients easier
- Improve communication between patient and healthcare provider
- Increase public's knowledge about drug interactions and allergy problems
- Avoid duplication of testing or adverse drug events
- Support wellness and preventive care activities

However, there is a lack of information on genetic data coverage of PHRs in the literature. A recent study reviewed more than 5000 scientific studies related to PHRs published in the last 10 years (Roehrs et al., 2017). As a result, they indicated that genetic information is not frequently mentioned in the papers; they only listed two studies. One of these papers aimed to analyze the privacy and security characteristics of PHR privacy policies and only mentioned the necessity of including genetic information items in PHRs (Carrión Señor, Fernández-Alemán, & Toval, 2012). The second paper is a literature review on privacy and security safeguards of social network websites (Williams, 2010). It talks about the risk of secondary damage caused by genetic data disclosures, namely, the potential risk for a subject's family members due to possible breaches.

PHRs are good choices for patients who move or travel from one country to another, since the use of their own PHR enables more efficient and rapid solutions for their health management (Roehrs et al., 2017). Wireless and mobile technologies create opportunities to deliver health care services to patients. Moreover, mobile health applications are the fastest-growing sector for popular tools in the area of healthcare technologies. Currently, there are 325,000 mobile health applications available in major application stores (Pohl, 2017). Although there are still privacy and security concerns regarding these applications (Arora, Yttri, & Nilse, 2014; Atienza et al., 2015; Luxton, Kayl, & Mishkind, 2012; Martínez-Pérez et al., 2015), it is projected that the global revenue of mobile health devices and services will be around 35.8 billion dollars by 2020 (Statista, 2017). Problems regarding the security and privacy of health data on mobile platforms should be addressed and concerns should be reduced before a system can be widely adopted. However, the design of mobile health applications still lacks features that would overcome users' concerns, and applications with low security measures continue to be released on the market (Martínez-Pérez et al., 2015).

Even though PHRs have many advantages, there are also many challenges to be solved for a widespread adoption of PHR, which are mostly security and privacy related (Baird, North, & Raghu, 2011). In order to solve privacy problems, security practices should be applied (Li et al., 2013; Lafky & Horan, 2011; Ozok, 2014). There are many suggestions for security protections on PHRs. The recent trend was using cloud computing in PHRs (Li et al., 2013; Liu, Huang, & Liu, 2015).

## **2.5. Security of PHRs: Security Safeguards in Online Banking**

Using cloud computing helps to solve cybersecurity issue of PHRs (Wooten et al., 2012). Cybersecurity or IT security is information security as applied to computing

devices such as computers and smartphones, as well as computer networks such as private and public networks, including the Internet as a whole. However, it is only the physical protection which is mentioned here, while the providers still need to implement their own security measures for the software.

Many other branches of industrial-economic activities have found various solutions for these security issues. No doubt, internet banking is one of the biggest experts on security problems of online platforms. After Grabner-Krauter and Faullant (2008) investigated the effect of trust in technology on internet banking, they suggested that banks enhance system security to achieve a good level of customer trust. Internet banking started in 1994 (Yoo, Kang, & Kim, 2015), and at that time there were only 100 users in the whole system. However, this number has increased exponentially since then. According to data from the Banks' Association of Turkey, the number of registered online users that had used internet banking in Turkey at least once was 11,793,000 in March 2009 (Pala & Kartal, 2010). This number was 1,791,000 higher than the previous year's. Apparently, the security of the system of internet banking is sufficient to convince many people in Turkey.

Online banking systems security safeguards for user authentication can be listed as follows (Yoo, Kang, & Kim, 2015):

- ID password type: user defines an ID and password and then this ID and password are matched each time when the user enters the system
- Virtual keyboard: this is like a real keyboard, but the input system is different. The system uses a virtual keyboard to avoid keyboard logging
- Pre-inquiry response type: this means roughly asking for more information besides ID and password for user verification
- Security card and image verification type: their working principles are similar. The most famous application of image verification-type authentication is CAPTCHA
- Asymmetric key type: the digital certificate is an example of this. The authentication system matches personal and open keys, and when a personal key is sent within content, this content should be checked with the other match, the open key.
- Symmetric key type: a secret and private key between the user and system is identified in advance. Whenever it is needed, the user can use his or her key to produce a code for system login. OTP is a good example of this method.
- One-way type: a onetime-use password is defined and sent to the users via mobile connections or another channel. When the user receives the code, it is used as a system password
- Two-way type: this is a more developed version of the one-way type. Like the one-way type, a password is sent, then the two-way type wants a second confirmation via the channel, and as soon as it receives the user response, the request is ended (e.g. telephone approval service)
- Keyboard security: this is used for avoiding key input sniffing

As has been said in the previous paragraph, when genetic data is involved in the situation, more importance should be given to security and privacy measures. Actually, security and privacy are one of the biggest discussion topics concerning

health records in general. The National Committee on Vital and Health Statistics (2006) offers some security measures for PHRs. The recommendations can be listed as follows:

- PHR systems must have terms and conditions of use
- Users should have the control to see who has access to their records
- PHRs should provide industry-standard security and privacy schemes, but other security measures can be offered to the consumers, of course. However, when the vendors offer these additional security protection features as options to the users, they should take the risk of additional costs, mobility and supportability problems.
- Users of the system should have the ability to change the accessibility of their records. They should have the right to decide which of the records they would like to share with whom.

Privacy and security of a system are issues generally related with the system developers. However, the protection of personal privacy should be guaranteed by laws and regulations so that people feel comfortable and secure while using the system.

## **2.6. Legal Issues Regarding Protection of Personal Data Internationally**

In the modern world, with the help of computers and smartphones, people are producing a huge amount of digital data incredibly fast. According to the statistics for 2015, people had created more data in the previous two years than in the entire past of the modern world (Marr, 2015). Recording, editing, adapting, altering, correcting, examining, using, sorting, merging, and deleting this data are inevitable necessities posing complicated technological problems. The processing of personal data that are closely related to the individual must be subject to a legal arrangement in order to safeguard people's private lives and freedoms. That is why data protection is regulated by the law in many countries.

Europe was the first place that acted to prevent the uncontrolled use of personal data and began to take legal actions in this regard (Küzeci, 2010; Schriver, 2001). Germany adopted the first data processing regulation in 1970 and Sweden released the first national data protection law in 1973 (Schriver, 2001). Similarly, in 1978, France took a step towards this issue (ibid.). Since the establishment of the European Union in 1993, the importance given to this topic has increased exponentially, and larger and more comprehensive regulations have been issued (Andrews, 1998). The Data Privacy Directive was created by the Union in 1995, and it came into force in 1998 (ibid.). The Directive stated that privacy is a "fundamental human right" and regulated that the transfer of personal information to countries outside the EU can only be permitted if that country guarantees adequate protection for the information. The EU requires that these regulations are made for all commercial agreements involving data transfer:

ARTICLE 25 (Directive 95/46/EC of the European Parliament and of the Council) –  
(1) The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions

adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

This article is one of the reasons why other countries are regulating their privacy protection: to be able to conduct business with Europe.

The Data Protection Directive 95/46/EC was replaced by the EU General Data Protection Regulation (GDPR) on May 25, 2018. According to the official website, the regulatory policies of the new directive have changed significantly, given that the world is now “vastly different from the time in which the 1995 directive was established” (“Key Changes with the General Data Protection Regulation,” 2017).

Although some of them are not as “aggressive” (Fromholz, 2000) as Europe, today personal data is somehow protected by certain laws in 120 countries (Greenleaf, 2017) (see Table 1).

Table 1 Countries with data privacy laws between 1973 and 2016 (Greenleaf, 2017)

<b>Year</b>	<b>Country(s)</b>	<b>Year</b>	<b>Country(s)</b>
1973	Sweden	1997	Greece; Poland; Thailand
1974	United States	1998	Azerbaijan
1977	Germany	1999	Albania; Chile
1978	France; Austria; Denmark; Norway	2000	Argentina; Latvia
1979	Greenland; Luxembourg	2001	Cape Verde; Chad; Cyprus; Malta; Romania, Bosnia & Herzegovina
1981	Israel	2002	Armenia; Bulgaria; Liechtenstein; Paraguay; Zimbabwe
1983	Canada; San Marino	2003	Andorra; Bahamas; Croatia; Estonia; Seychelles; Vincent & Grenadines
1984	United Kingdom	2004	Burkina Faso; Gibraltar; Mauritius; Tunisia
1986	Guernsey; Isle of Man	2005	Macedonia (FYROM); Qatar FC
1987	Finland; Jersey	2006	Macao SAR; Russia
1988	Australia; Ireland; Netherlands	2007	Dubai IFC; Moldova; Nepal
1989	Iceland	2008	Colombia; Kyrgyz Republic; Montenegro; Senegal; Serbia; Uruguay
1990	Slovenia	2009	Benin; Morocco
1991	Portugal	2010	BES Islands; Curaçao; Faroe Islands; Kosovo; Malaysia; Mexico; St Maartens; Vietnam
1992	Belgium; Czech Republic; Hungary; Slovakia; Spain; Switzerland	2011	Angola; Aruba; Costa Rica; Gabon; India; Lesotho; Peru; St Lucia; Trinidad & Tobago; Ukraine
1993	Monaco; New Zealand	2012	Georgia; Ghana; Nicaragua; Philippines; Singapore; Yemen
1994	South Korea	2013	Antigua & Barbuda; Cote d’Ivoire; Dominican Republic; Kazakhstan; Mali; South Africa
1995	Hong Kong SAR; Taiwan; Japan	2015	Abu Dhabi GM; Madagascar
1996	Italy; Lithuania	2016	Turkey; Bermuda; Equatorial Guinea; Qatar; São Tomé and Príncipe; Indonesia, Malawi
Total: 120 Countries: Average per year for 44 years = 2.7			

The US has had regulations on data protection since 1974 when the Congress enacted the Federal Privacy Act (Greenleaf, 2017). The Act included regulations about government databases (Raul, Manoranjan, & Mohan, 2015). It also stated that privacy is a fundamental right protected by the Constitution of the United States (ibid.). The US Privacy Act is generally accepted as the first information protection principle and has inspired many other protection regulations. In addition, the European Union's 1995 Data Protection Directive is composed on the basis of the US Privacy Act (ibid.). However, there are fundamental differences between the EU and the US in the way of data protection (Schwartz & Reidenberg, 1996). Because of these differences, there was a conflict between the EU and the US, triggered by an Austrian Facebook user, law student and data privacy activist, Max Schrems, and his legal action against the collection of personal data of citizens of the EU by Facebook (Geller, 2016; McCusker, 2016). Eventually, the court ruled in favor of Schrems and on 6 October 2015, the European Court of Justice canceled the Safe Harbor agreement, which allowed data transfer between Europe and the United States (Raul et al., 2015; Robinson, 2016). Immediately after this decision, the European Commission and the US Government started to set up a new framework and on February 2, 2016, the EU-US Privacy Shield replaced Safe Harbor (EU 2016 Press release, 2016).

Privacy involves economic and social costs for governments, industry groups, or companies (Fromholz, 2000). Policies and regulations for data protection also produce additional workload for stakeholders and causes projects to be left unfinished (Diamond, Mostashari, & Shirky, 2009). The main reason of the avoidance to establish certain laws and regulations can be these costs. However, the aim of the principles of personal data protection is not to establish barriers in front of technological developments nor to prohibit data processing that may be useful or necessary: It is to ensure that these operations are carried out only by authorized persons and for legitimate purposes (Küzeci, 2010).

In many other countries, precautions for data privacy and security are being established; some countries are updating their existing regulations, some are enacting new ones. For instance, in Japan updates are done regarding the law for international data exchange, online marketing, etc.; Brazil and Russia allowed the storage of a copy of their data outside the country border; the Republic of Korea and Singapore have changed the penalties and data violation rules; Hong Kong and Israel have issued new privacy guidance (Raul et al., 2015).

In conclusion, changes are being made to existing laws or new legislation is being adopted to adapt to changing technologies in the world, except for a small number of countries: thus, neither China nor India have comprehensive legislation directed towards data protection or cybersecurity (ibid.).

## 2.7. Legal Status of the Protection of Personal Data in Turkey

As for Turkey, more recently, many significant steps have been taken on personal data privacy legislations. Although, Turkey signed of the Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data on January 28, 1981, there had not been any law dedicated to data protection up to March 24, 2016 (Raul et al., 2015) when the Turkish Personal Data Protection (PDP) Law, was accepted and published on official newspaper (Law number: 6693) (Kişisel verilerin korunması kanunu, 2016). Even if the draft PDP law was prepared in 2003, it was on hold for 13 years to come into force. Before that the privacy of personal data was protected within the scope of the law on privacy of private life in the Turkish Constitution of 1982 (ibid.).

Since the law came into effect, there have been many debates on its various articles, and even a lawsuit was filed demanding its cancellation. The biggest opposition party, the Republican People's Party (CHP), appealed to the Constitutional Court for the cancellation of the provisions of the law and for the suspension of its implementation on June 3, 2016 ("CHP kişisel verilerin korunması kanununun iptali için AYM'ye başvurdu", 2016). The case was concluded on 28/9/2017 and Constitutional Court rejected all requests by the CHP for the cancellation of certain articles of the Law on the Protection of Personal Data ("Anayasa Mahkemesinin 28/9/2017 Tarihli ve E: 2016/125, K: 2017/143 Sayılı Kararı", 2018).

There was another case between NGOs (Turkish Medical Association (TTB) and Turkish Dentists Association (TDB)) and the Turkish Minister of Health regarding the circular on the processing and protection of personal health information, which came into force in October 20, 2016 (Türk Dişhekimleri Birliği, 2016). There were two main common arguments for both cases: First, according to the complainants' claims, the exceptions defined in the circular and the law about collecting and processing personal data without the owner's consents are too wide (Article 6(1-3)). Second, a personal data protection board had not been established; therefore, contrary to what was stated in the law, measures which the board should determine had not been declared (Article 6(4)).

Article 6 was one of the subjects of litigation. Paragraph one defines sexual life and genetic data as special categories of personal data and gives some privileges to them and paragraph two states the necessity of explicit consent.

ARTICLE 6 – (1) Data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dressing, membership of association, foundation or trade-union, health, sexual life, criminal conviction and security measures, and biometrics and genetics are special categories of personal data.

(2) It is prohibited to process special categories of personal data without obtaining the explicit consent of the person concerned.

(3) Personal data other than those relating to health and sexual life indicated in Paragraph 1 may be processed without obtaining the explicit consent of the person concerned if processing is permitted by any law. Personal data relating to health and sexual life may only be processed without obtaining the open consent of the data subject for purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment, and care services, planning and management of health services and financing by people under the obligation of secrecy or authorized institutions and organizations.

(4) It is additionally required to take the adequate measures designated by the Board when special categories of personal data are processed.

In this paragraph, three exceptions are listed which allow to process data categorized as special without open consent.

There are also some differences between GDPR, PDP law, and EU Directive 95/46/EC on special categories of data types. These differences are summarized in Figure 1. Genetic and biometric data are added to Turkish PDP law and GDPR. Appearance and dressing is mentioned only in PDP law. Sexual orientation data and sex life data is specified separately in GDPR.

The Personal Data Protection Board (PDPB) is the other subject of these cases. Article 21 of the PDP law defines the board:

ARTICLE 21 - (2) The Board consists of nine members. Five members of the Board are elected by the Turkish Grand National Assembly, two members by the President, and two members by the Council of Ministers.

(3) In order to become a member of the Board, the following conditions are sought:

A) To have knowledge and experience in the subjects of duty of the institution.

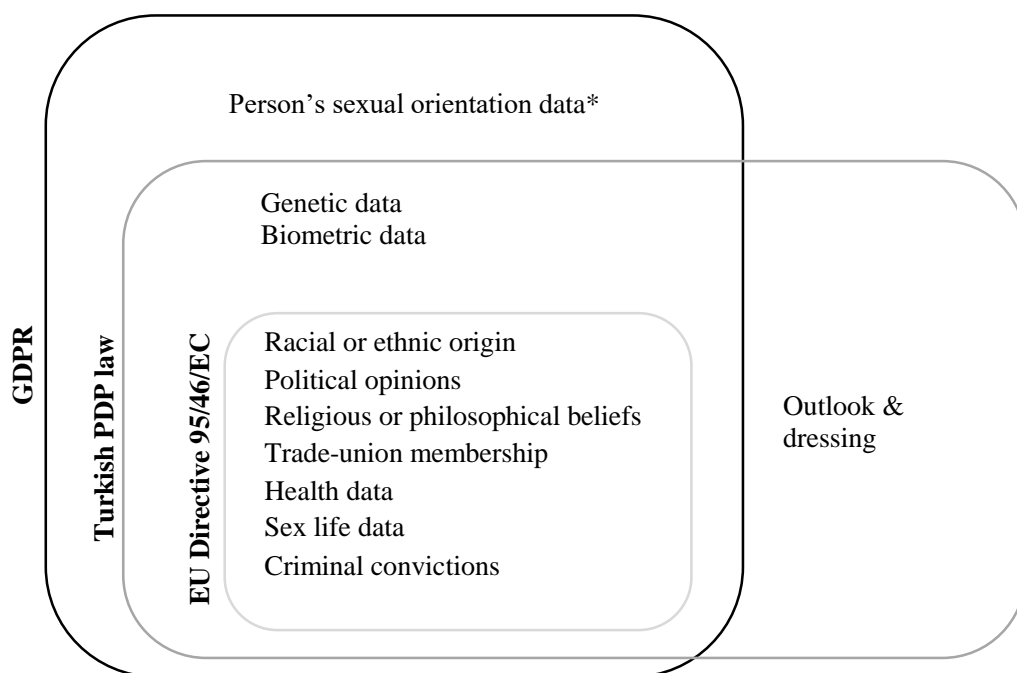
B) To carry the qualifications specified in sub-paragraphs (1), (4), (5), (6) and (7) of subparagraph (A) of the first subparagraph of Article 48 of the Civil Servants Law No. 657 dated 14/7/1965.

C) Not being a member of any political party.

Ç) Having graduated from at least four years of undergraduate study.

D) To have worked for at least ten years in public institutions and organizations, in international organizations, non-governmental organizations or public institutions or professional organizations.





*\*The person's sexual orientation data and sex life data is mentioned separately in GDPR*

Figure 1 Special categories of data types in GDPR, Turkish PDP law, and EU Directive 95/46/EC

Actually, there had been a previous decision by the Council of State to stop collecting and processing the personal health data by the Ministry of Health in November 2015. The case had been brought by the abovementioned NGOs (TTB and TDB) against the Ministry of Health's circular regarding e-Nabız, the national electronic health record application, in February 2015. About nine months later, the Council of State stopped the implementation of the circular which gave the Ministry of Health the right to collect and process personal health data of the public (T.C. Danıştay Onbeşinci Daire, 2015).

The schedule of events related with the PDP law was below:

- November 24, 2015: The council stopped the collection of health data of Ministry of Health (e-Nabız Case)
- March 24, 2016: The first Turkish PDP law released
- June 3, 2016: CHP sued the law
- October 20, 2016: Regulation of Ministry of Health released
- December 15, 2016: NGOs sued the regulation
- September 2, 2017: CHP lost the case
- January 30, 2017: Personal Data Protection Board started working
- November 24, 2017: Regulation was revised
- April 17, 2018: EU Commission criticized the PDP "The law is not yet in line with European standards"

The acts had been taken to the full extent of the Turkish Data Privacy Law, as summarized below (Keser Berber, Ülgü, & Er, 2010):

- 2001 Medical Recording and Archiving Services Policies for Inpatient Treatment in Hospitals
- 2004 Additional Policy for Medical Recording and Archiving Services Policies for Inpatient Treatment in Hospitals
- 2005 Policy for the Security of Personal Health Records
- 2007 Security of Information for Administrators
- 2007 Security of Information for Staff
- 2007 Modification of the Medical Recording and Archiving Services Policies for Inpatient Treatment in Hospitals
- 2008 New Standards for Electronic Documents - TSE 13298
- 2010 Referendum for the Amendment of the Constitution, 20<sup>th</sup> Constitutional Provision

These are only the regulations and policies in place before the PDP law. The law of privacy of private life in the Turkish Constitution of 1982 was used for personal data privacy protection (Raul et al., 2015).

## **2.8. Design Considerations**

Today, almost every smartphone has high speed internet access, high quality imaging, video streaming, and e-mailing features, and almost every day, a new area of mobile phone usage emerges. Hence, the way to record health data, like many other traditional records, has been continuously evolving; first it was a paper-based system and later the data became remotely accessible by e-health (Chen, Liou, Chen, & Li, 2013). Eventually, the systems expanded to the mobile realm (m-health) (ibid.). In parallel to the increase in the use of mobile systems in every venue, health records applications are also migrating into mobile systems.

Mobile health applications use advantages of technology in an unusually diverse and versatile manner (Chiu, Lee, & Cheng, 2011; Luxton, McCann, Bush, Mishkind, & Reger, 2011; Sikka et al., 2012). Besides its advantages, there are some challenges for mobile health applications such as energy consumption limitations and security threats in wireless data transmission. Battery life of smart phones is not developing as fast as the other hardware technology in the phone. This is a big problem for mobile health interventions, since the transfer of a considerable amount of raw health data leads to energy consumption, which is a big limitation for mobile health applications (Baig, GholamHosseini, & Connolly, 2015). Wireless data transmission of mobile application data also seen as a security threat for especially sensitive data as health/genetic data (ibid.).

The effects of the gender, age and education differences also needs consideration while designing any system. In the literature, younger age has been associated with greater privacy concerns (Khan et al., 2014). Oliver et al. (2012) provided a very interesting interpretation for the difference between the age groups. According to the authors, the reason for older people having fewer concerns regarding the commercialization of their DNA is their belief that it would take years before a

person could be identified from their DNA on the Internet, and this would probably not be possible in their lifetime.

The situation was similar for the educational level. McGuire et al. (2011) reported that university degree holders were more likely to choose restricted data sharing similar to our participants' tendency to limit their doctors' access to their data.

However, there is an inconsistency in the literature on gender differences (Khan, Capps, Sum, Kuswanto, & Sim, 2014). These two studies observed that women are less willing to participate in genetic research or allow storage of their genetic data than men (Espeland et al., 2006; Matsui, Kita, & Ueshima, 2005). On the other hand, Mezuk, Eaton and Zandi (2008) found no association between gender and consent to donate a biological sample or allow genetic testing or storage of that sample, while Green et al. (2006) reported that mostly men denied private companies access to their DNA.

## **2.9. Summary of Background and Literature Review**

In this section, background information and an overview over the relevant literature are presented. Genetic/genomic data is special and more confidential than the other types of data because it is unique for the person and not possible to change. It is also related with other family members and have potential to provide more information on the owner's life in the future. Hence, the necessity of an appropriate level of protection as well as studies about the public's concerns regarding privacy and confidentiality of genetic information are discussed in this chapter. The literature indicates that the public has great concerns about privacy, security of health and genetic data. Moreover, there is ethical concerns and the discrimination potential rooted in genetic background information. The importance of the privacy of health and genetic data, research on people's perception on privacy of health data, and the importance of the inclusion of genetic/genomic information into electronic health records have been mentioned in this section. It is stated that PHR systems have both advantages and disadvantages. They give full control to the users, provide easy data access, help avoiding adverse events and duplications, and it is suitable for travelers or anyone who changes his/her country, security and privacy problems. However, dearth of studies on genetic data coverage in PHRs in the literature is emphasized in the section. The data protection status in the EU, the US, and the rest of the world is reviewed. Details about the Turkish PDP law and its background are given. There were 120 countries in the world which regulated data protection laws since 2017. Turkey was the last one among these countries.



## CHAPTER 3

### MATERIALS AND METHODS

The dissertation consists of four substudies. Each of the substudies uses a different methodology, and details are presented in this chapter. Firstly, mobile personal health record applications were evaluated according to predefined features in two popular application markets. Afterwards, using the results of this analysis, a descriptive survey was developed and administered to the public. As a parallel study, participatory design groups were formed with potential users and/or stakeholders related with the design of genetic-health record applications and 11 meetings were held. Lastly, two closed focus group meetings were organized with domain experts. The order of the dissertation's seven steps is shown in Figure 2.

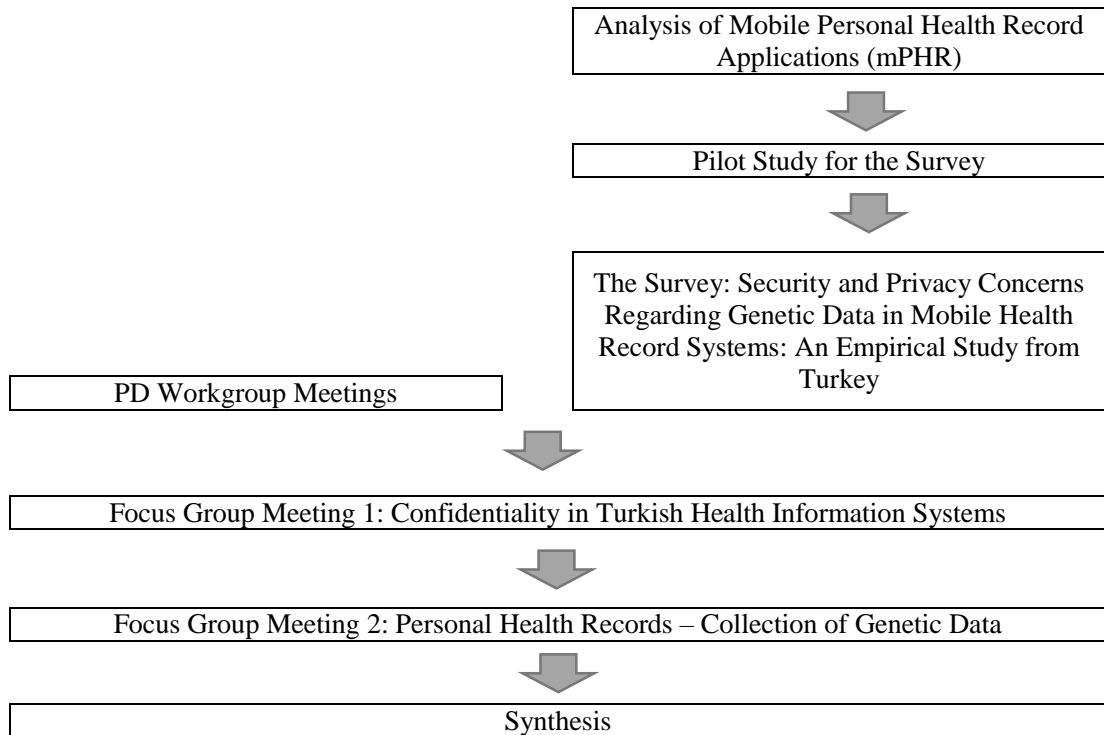


Figure 2 Methodological work flow followed during the study

### **3.1. Analysis of Mobile Personal Health Record Applications**

Within the scope of the thesis, the current mPHRs available in Android and IOS markets were analyzed and evaluated according to certain criteria defined by Kharrazi, Chisholm, VanNasdale, and Thompson (2012). The former study was updated with some additional criteria and modifications, and the scope was narrowed. Three modifications were made compared with the former study. Firstly, the analysis done by Kharrazi et al. (2012) included the BlackBerry market besides Android and IOS. We excluded BlackBerry from our target markets because it had a limited number of applications in its store compared to Google Play and IOS App Store. Secondly, in the scope of our study, because of the budget limitation only free applications were evaluated, whereas the reference study (ibid.) analyzed also applications that charged a fee below a certain limit. Lastly, some additional features were added to the criteria list, namely: security measures and inclusion of genetic information.

### **3.2. Survey Development**

The survey is designed as a descriptive study. Descriptive research (Jonassen & Driscoll, 2004) uses a methodology that is neither quantitative nor qualitative. It may utilize elements from both methods, usually in the same study (ibid.). Friedman and Jeremy indicated in their book (1997) that “even though they seem deceptively simple, descriptive studies can be highly informative”. This design also has many advantages, like low cost, efficient usage, and small number of ethical difficulties (Wingo et al., 1994).

Descriptive statistics try to answer the question of “what is?”, which means the results of descriptive studies give a direct answer to a direct question (Jonassen & Driscoll, 2004). For instance, in this survey the main question is “What are the opinions of people about a mobile health record application which they can use to record their health and genetic data?”. Furthermore, we inquired about the preferences of users regarding what they would share via these applications. To identify the critical design elements for the applications, we asked the participants which information they would store in a health record application and what kind of protections they would use to assure the security of their information. We proposed online banking safeguards as the gold standard for mobile information management and investigated whether these security protections are also reliable for the management of health and genetic information on a mobile platform.

While developing the instrument, we first collected expert views and then conducted a pilot study. The dates and details of these processes are given in Table 2.

In the pilot study, there were 28 questions in three sections: seven questions about demographic information, five on internet banking security protection and 16 regarding health and genetic information security.

Table 2 Survey work flow

<b>Date:</b>	<b>Work:</b>
30.10.2014	First Review with Advisor
07.11.2014	Expert Review (Dr. Neşe SEVİM)
11.11.2014	Advisor Review
19.11.2014	Expert Review (Assist Prof. Arsev Umur AYDINOĞLU)
01.12.2014	Last Review with Expert (Assist Prof. Arsev Umur AYDINOĞLU)
04.12.2014 -16.12.2014	Pilot Study

The first part included demographic questions about home town, date of birth, sex, level of education, income, and computer and smart phone literacy levels.

In the second part, questions concern internet banking and security protection:

- which internet security safeguards have been used until now,
- if participants previously used online banking applications and if so which one(s),
- if participants previously used mobile banking application and if so which one(s),
- what opinions the participants had on the adequacy of Internet banking security,
- if participants have been faced with any theft or similar situation while using online banking.

In the third part, under the title of health and genetic information security, the questions are generally about levels of knowledge, opinions and experiences about genetic and health information. The questions and references for this section are presented in Table 3.

Six of the questions were taken from two different sources and then translated into Turkish with the help of an expert in 2010 in the context of another thesis (Özkan, 2011).

After the survey development part was completed, a pilot study was performed with 20 Turkish participants between the dates 12/4/2014 and 12/16/2014. Details for the pilot study are given in the following subsection.

### *3.2.1. Pilot Study for the Assessment of the Survey*

The survey was conducted in Turkish as this is the participants' native language (See survey questions in English: Appendix C: The Survey Questions in English). A pilot study was performed with 20 participants to assess both timing and appropriateness of the survey items for the Turkish participants. After the pilot study, we conducted a follow-up interview with the participants to inquire about the clarity of the questions and, based on their responses, we revised three questions. Two questions were combined, and one of the questions was removed from the survey instrument as the

results showed that it was not informative. Hence, the final version of the survey consisted of 26 questions under three main categories: The first part covered demographic questions about city of residence, year of birth, gender, educational level, income, and computer and smartphone literacy levels. The second part aimed to obtain information about the participants' level of awareness regarding security tools and their general online banking experience. The last part of the survey investigated the participants' level of awareness, attitudes, and experience concerning data security and privacy, and management of genetic and health data in mobile applications. Three questions were directly taken from two external sources (Canada Health Infoway & EKOS Research Associates, 2007; Princeton Survey Research Associates, 1999) and four questions were modified to address issues about genetic data.

Table 3 Health and genetic information security questions

<b>Q#</b>	<b>Question</b>	<b>Source</b>
13	Knowledge level of access permissions to medical records	
14	Knowledge level of genetic science	
15	Experience with genetic testing	
16	Level of concern about information leaks in Turkey	
17	Experience of avoiding being tested in case someone can see your results	(Princeton Survey Research Associates, 1999)
18	Experience of asking doctor to write down a different medical condition in the medical records	(Princeton Survey Research Associates, 1999)
19	Feeling about the usage of an electronic device as medical record storage	(Canada Health Infoway & EKOS Research Associates, 2007)
20	Opinions on health and genetic information storage security safeguards	
21	Opinions on access levels to health records demanded for specified people or organizations	(Canada Health Infoway & EKOS Research Associates, 2007)
22	Opinions on access levels to genetic test results demanded for specified people or organizations	
23	Opinions on access levels to the whole genome map demanded for specified people or organizations	
24	Opinions about stated regulations on privacy and confidentiality of medical and genetic records	(Canada Health Infoway & EKOS Research Associates, 2007)
25	Level of trust in confidentiality of health information in medical records made accessible to specified people or organizations	(Canada Health Infoway & EKOS Research Associates, 2007)
26	Level of trust in confidentiality of genetic test results in medical records made accessible to specified people or organizations	
27	Level of trust in confidentiality of the whole genome map in medical records made accessible to specified people or organizations	
28	Opinions about using an internet-based application for personal information	



### *3.2.2. Ethics Clearance*

The pilot study was conducted at Middle East Technical University (METU). Permission for the study was obtained from the Practical Ethics Research Board at METU on 07/01/2015 (see Appendix A: Approval Letter of the Practical Ethics Research Board and Appendix B: Example of Participant Consent).

### *3.2.3. Data Collection*

Data collection was undertaken using two methods: online and in-person. A snowball sampling method was used for online data collection between May 5 and August 2, 2015. An e-mail including the survey link was sent to university students and shared on Facebook pages with more than 15,000 users consisting of the students and staff of Middle East Technical University and people from the vicinity of the university. The participants were specifically asked to distribute the survey to people who or whose family members had undergone genetic testing. Total of 124 people responded to the surveys. After the elimination of 19 incomplete surveys, the remaining 105 were included in the analysis. In order to reach more participants with different demographic profiles and increase the number of participants who were familiar with genetic testing, in-person data collection was implemented in two centers: a private genetic diagnostic center and a medical genetics department of a university hospital. Sixty-nine people responded to the on-site surveys; thus, the total number of completed surveys was 174.

### *3.2.4. Data Analysis*

We used SPSS (version 23.0.0) for statistical analysis. Descriptive statistics were reported as frequencies. Pearson's chi-square test was used to test whether there were any differences within the following seven parameters: gender, age ( $\leq 35$  versus  $>35$  years), educational level (university degree versus other), income [ $\leq 2000$  Turkish Liras versus  $>2000$ ], computer literacy ( $<4$  versus  $\geq 5$ ), smartphone literacy ( $<4$  versus  $\geq 5$ ), and genetic testing [tested (himself/herself or a family member) versus non-tested]. Post-hoc achieved powers were computed using G-Power 3.1.9.2. (Erdfelder, Faul, & Buchner, 1996). Cronbach's alpha coefficient was used for reliability analysis (Pallant, 2013).

## **3.3. Participatory Design (PD) Meetings**

We implemented a participatory design approach to create a discussion platform and develop a sample prototype for a mobile PHR including genetic/genomic data. A focus group method and PICTIVE technique were used in the discussions. In this chapter, PD meetings are presented under four subheadings: participatory design, PICTIVE technique, participants, and focus groups with potential users and system designers.

### *3.3.1. Participatory Design*

Participatory Design (PD) is a design approach originating from Scandinavia in the beginning of 1970s (Floyd, Mehl, Resin, Schmidt, & Wolf, 1989). At first, Scandinavian participatory design sought to democratize workplace design to represent the interests of intended system users better (Bums, Cottam, Vanstone, & Winhall, 2006; Dust & Jonsdatter, 2008). It necessitates the direct participation of users and non-designer stakeholders (managers, producers, users, workers, etc.) in the design processes of a system they would use that are specified and facilitated by designers (Floyd et al., 1989; Dust & Jonsdatter, 2008; Sanders & Stappers, 2008). PD involves stakeholders, end-users, and the team into the design process in order to help ensure that the end-product meets the needs of users (McGrenere et al., 2002). So, direct participation to the design, provides better support to describe the needs of the systems (ibid.).

Our study group, consisted of five participants, and 11 meetings are organized. The meetings were held mostly weekly and each lasted around one hour. Except for one participant, the group members previously knew one another. No asymmetric power relationship, power struggles or hierarchy within the group was observed. The researcher had an active role as facilitator of the discussions the way the focus group method suggested (Morgan, 1996). With verbal permissions from the participants, the first discussion was audio-recorded, and the remaining ones were video-recorded. Again, with the verbal permissions of the participants, personal identifiers are not anonymized.

### *3.3.2. PICTIVE Technique*

PICTIVE is an experimental participatory design technique. The acronym stands for Plastic Interface for Collaborative Technology Initiatives through Video Exploration (Muller, 1991). This technique enhances user participation in the design process. It combines low technology and high technology components. As low technology, ordinary office material in a range of bright colors including pens, highlighters, paper, Post-It™ notes of various sizes, stickers and labels and paper clips are used (ibid.). The aim of the low-tech material is to supply equal conditions to the developers and designers. The high-tech material included in this technique is video recording. The use of videotaping as a high-tech method has several advantages. First, it gives a message to the participants that their views are important, as they are going to be recorded, while at the same time making the record-keeping process relatively effortless. Second, participants' and researchers' access to the video records are equal in contrast to researcher's private notes. Third, it provides a full record of the design processes and all of the decisions being taken in the discussions (ibid.).

PICTIVE was used as a technique to create a discussion platform on the essential characteristics of an mPHR that can manage genetic/genomic data along with other medical records and healthcare data. In the first meeting, a presentation was given to the participants about the implementation of the method and the low and high technology components involved.

Table 4 Detail of PD group participants

<b>Participant number</b>	<b>Info</b>
<b>P1</b>	<ul style="list-style-type: none"> <li>• health application developer</li> <li>• a co-founder of a bio technology and health informatics company</li> <li>• biologist</li> <li>• has a bioinformatics master's degree</li> <li>• medical informatics PhD student</li> </ul>
<b>P2</b>	<ul style="list-style-type: none"> <li>• chronically ill patient</li> <li>• health application developer</li> <li>• a co-founder of bio technology and software development company</li> <li>• a molecular biologist</li> <li>• biology PhD student</li> </ul>
<b>P3</b>	<ul style="list-style-type: none"> <li>• a medical doctor - geriatrist</li> </ul>
<b>P4</b>	<ul style="list-style-type: none"> <li>• a genetic laboratory worker</li> <li>• a molecular biologist</li> <li>• has a bioinformatics master's degree</li> <li>• medical informatics PhD student</li> </ul>
<b>P5</b>	<ul style="list-style-type: none"> <li>• chronically ill patient</li> <li>• has a bioinformatics master's degree</li> <li>• medical informatics PhD student</li> </ul>

### 3.3.3. Participants

Participants were chosen with maximum variation sampling method (heterogeneous sampling) of a purposive sampling technique (judgment sampling). Purposive sampling is a nonrandom technique that allows the researchers to select people who can provide the information needed for the research (Bernard, 2017). Besides knowledge and experience, willingness to participate, availability, and/or ability to communicate experiences and opinions can be other reasons for selection (Spradley, 1979).

Maximum variation sampling (heterogeneous sampling) is a suitable method when the sample size is very small (Etikan, Musa, & Alkassim, 2016). The sample should be a small representation since it includes outliers and average representatives of the area in a balanced way (ibid.). Therefore, our participants were chosen among representatives of system users from different fields: a medical doctor, a genetic laboratory worker, chronically ill patients, and company co-founders. Moreover, the participants have varied backgrounds. For instance, one participant is a chronically ill patient, health application developer, molecular biologist, and company co-founder, etc. (Details are presented in Table 4). In this way, we were able to have better representation within a small group.

We gathered five participants for 11 meetings in order to define the necessary design elements of an mPHR prototype. The participants consisted of potential users and

developers of the system. For ease of reference, the participants are called P1 to P5 throughout this dissertation (Table 4).

#### *3.3.4. Focus Group Study with Potential Users and System Designers*

The focus group method was used for data collection of the PD group study. It is a method frequently used throughout the social sciences (Krueger & Casey 2000; Madriz, 2003). With this method, data is collected while the group is discussing a subject determined by the researcher (Morgan, 1996). The data sources of the method are the group interactions and discussions (ibid.).

As mentioned above, the group members already knew one another. P3 could not attend the first meeting because of an emergency situation. Hence, all group members came together for the first time in the second meeting. In the first meeting, in order to learn about the participants' backgrounds, a short questionnaire was administered to collect demographic data: name, year of birth, education, occupation, and current job.

The meetings started with an overview about the principles of the participatory design method. Then, the mPHR analysis results and first results of the survey study were presented. The first meeting was only audio-recorded. During the rest of the meetings, the participants of the PD group discussed the topic while applying the PICTIVE technique for creating the paper prototype. As PICTIVE necessitates, these meetings were video-recorded. We took notes and wrote memos of the meetings.

### **3.4. Focus Group Meetings**

We held two focus group meetings eight months apart (May 2016 and January 2017) to discuss the electronic health records, data privacy and security, and specifically e-Nabız (an e-government service to manage electronic health records of Turkish citizens). Focus groups are “intended to provide researchers with means for collecting data that can be used to construct a descriptive account of the phenomena being investigated” (Dollar & Merrigan, 2002).

As participants interact and build on one another's comments, the researcher is able to generate large amounts of data that describes, explains, compares, and evaluates a phenomenon. Moreover, through a facilitator, discussions can be probed for further details.

The main aim of the meetings was to figure out the legal, ethical, and security requirements of a health record system including genetic data in general. Moreover, we aimed to evaluate the current situation of health information systems in Turkey and to receive expert opinions and experiences on data security and confidentiality of these systems by creating a discussion platform on current legal issues and measures.

The participants represented organizations with a broad understanding of the topic (electronic health records, genomic data, and data ethics), a strong opinion, and some even had an active role in the policy process. Both groups engaged in heated discussions of their topics through a dynamic exchange of ideas among all the participants. The first discussions were concentrated especially on the new PDP Law and the management of sensitive information. Since the PDP legislation had entered

into force just recently at the time of the first group meeting and the members of the focus group were also among the main actors in the data protection field, the discussions were unsurprisingly focused on legal issues in Turkey. The second group's main topic was genetic information management in health records as it was titled.

#### *3.4.1. Participants and Procedures*

Participants were chosen with purposive sampling technique, an expert sampling method. In this method, experts are chosen to be research subjects (Etikan, Musa, & Alkassim, 2016).

The first focus group meeting included seven participants (three females, four males) and one moderator (female) from academia, NGO, and industry (insurance and wearable technology sectors). Representatives from the Ministry of Health were invited but were unable to attend the meeting. Participants with various carrier tracks attended to the study: two lawyers from an NGO overseeing the medical sector, a journalist focusing on information technologies and society, an academic who specializes in cryptology and information security, an insurance company representative, a director for relations with the Ministry of Health of a big IT company, and lastly, an entrepreneur from a wearable devices company. The moderator was also an academic specializing in the health and bioinformatics fields (Table 5). The meeting lasted a little over two hours. The moderator introduced topics to be discussed. The open-ended interview guide, which was developed with input from earlier studies, is used to moderate the discussions.

The second focus group was more focused. Eleven participants (three females, eight males) gathered to discuss the collecting of genetic data (Table 5); however, the discussions covered a wide range of topics from electronic health records to comparisons of different models in other countries to genomic data itself. In the second focus group, the participants made a short presentation on their specializations regarding genetic data which was followed by discussions. There was no need to facilitate the group as the presentations already triggered lively discussions. The participants consisted of a representative from an NGO, seven academics with medical training focusing on medical genetics, bioinformatics, and medical ethics, two NGO lawyers who worked on regulations of the protection of personal health information, a lawyer practicing in the health sector, and a representative from the industry (medical diagnostics center). This session lasted for almost six hours.

Information on the participants' ages was not collected since the participants were experts of the topic and age was not an important variable. With the participants' permission, both discussions were audio-recorded (permissions obtained verbally for the audio-recording) and transcribed verbatim for analysis. In order to protect the participants' anonymity in the focus groups, two-letter abbreviations and feminine third person pronouns were used for all participants.

Table 5 Details of focus group meeting participants

<b>Focus Group:</b>	<b>Participants:</b>
<b>First</b>	<ul style="list-style-type: none"> <li>• two lawyers from an NGO overseeing the medical sector,</li> <li>• a journalist focusing on information technologies and society,</li> <li>• an academic who specializes in cryptology and information security,</li> <li>• an insurance company representative,</li> <li>• a ministry of health relations director of a big IT company,</li> <li>• an entrepreneur from a wearable devices company</li> </ul> <p>The moderator: an academic specialized in the fields of Health and Bioinformatics</p>
<b>Second</b>	<ul style="list-style-type: none"> <li>• a representative from an NGO,</li> <li>• seven medical doctors from academia with specialization in:               <ul style="list-style-type: none"> <li>• medical training focusing on medical genetics,</li> <li>• bioinformatics,</li> <li>• medical ethics,</li> </ul> </li> <li>• two NGO lawyers who worked on the regulation of the protection of personal health information,</li> <li>• a lawyer practicing in the health sector,</li> <li>• a founder of a genetic diagnosis laboratory</li> </ul>

### 3.4.2. Data Analysis

The following steps of thematic analysis were undertaken (Braun & Clarke, 2006):

1. Familiarizing yourself with your data: The record of the first meeting was transcribed within two weeks after the event and the second one was outsourced. Immediately after receiving the transcriptions and editing the text for typographic errors, we started to sketch our ideas.
2. Generating initial codes: First, a preliminary analysis was conducted in order to get a general sense of the data and reflect on its meaning. Second, the entire data set was organized, specified, simplified, and reduced. Then initial codes were given to the related parts separately.
3. Searching for themes: Each code was re-read and the elements were defined. Appropriate codes were decided after long discussions. Then, the initial codes came together and turned into potential themes.
4. Reviewing themes & 5. Defining and naming themes: potential themes were organized. Some of the themes were collapsed and some were merged. Eventually, clear definitions and names for each theme were generated.

### 3.5. Summary of Methods

Because of the interdisciplinary nature of the study, mixed methods were used. Firstly, current mobile PHRs (in Turkish and English) from two popular application

markets were reviewed according to criteria defined in the literature (Kharrazi et al., 2012) in order to see what was available in the application markets. Some new criteria were added and thus the literature was updated and extended. Secondly, a descriptive survey was developed with the help of the results of this analysis and administered to the public online and face-to-face. Thirdly, with a participatory design method, five experts selected by the maximum variation sampling method of purposive sampling technique came together for 11 meetings. The group members were a medical doctor, chronically ill patients, a genetics laboratory worker, and health application developers. Some of them were also bioinformaticians and/or molecular biologists. PICTIVE technique was used for creating a sample paper-prototype of a mobile PHR including genetic data. Lastly, expert opinions were collected regarding the requirements for the compatibility of a health record system including genetic data with the current health system and data privacy laws. Two focus group meetings were organized for these aims. There were in total 18 participants who were experts and stakeholders in the fields of data privacy regulations and/or genetics and health data management: lawyers and representatives from NGOs, a journalist, an insurance company representative, a medical diagnostics center representative, a ministry of health relations director of a big IT company, an entrepreneur from a wearable devices company and many academics (from medical genetics, bioinformatics, genetic medicine, and medical ethics).





## CHAPTER 4

### RESULTS

The dissertation consists of four sub-studies. First of all, popular application markets were scanned and the mPHR applications were evaluated. Secondly, with the help of the results from this analysis, a public survey was developed, a pilot study was conducted, and the survey was implemented. As a parallel study, a participatory design group was formed with potential users and health application designers (n=5). The participants started to work on the prototype of an mPHR with the help of the first results of the survey. Lastly, in order to collect expert opinions two focus group meetings were organized to discuss design issues, regulations, problems, and deficiencies of genetic/health data systems in Turkey.

#### **4.1. Analysis of Mobile Personal Health Records (mPHR) Applications**

The review was done in three steps: (1) searching, identifying and downloading the mPHR applications; (2) excluding faulty applications; (3) doing tests according to determined features.

##### *4.1.1. Search, Identify and Download the mPHR Applications*

As stated before, for the scope this study only Google Play and Apple Store were scanned between the dates December 2014 and January 2015. The keywords “Personal Health Record” and “PHR” were used for the searches and free applications were selected, which left us with 138 applications (77 applications in Apple Store and 61 applications in Google Play).

##### *4.1.2. Elimination of mPHR Applications*

A set of rules was defined for the selection of applications: (1) mPHR should serve as a mobile application and be completely free from desktop applications. Any features should be used exclusively on the mobile platform; (2) applications which are limited to a specific kind of illness or patient group were excluded; (3) applications should be error-free; (4) applications should be working without the necessity of an Internet connection; (5) applications should not be specific for one place or country (Table 6).

Table 6 Excluded applications

<b>IOS App Store</b>		
<b>Number of Apps excluded:</b>	<b>Reason:</b>	<b>Details:</b>
32 Apps 12 Apps	connected to a website specified only for one issue or limited to a specific hospital	<ul style="list-style-type: none"> <li>• 3 for specific hospital patients</li> <li>• 3 for depression</li> <li>• 1 for children</li> <li>• 1 for HIV patients</li> <li>• 1 for radiology</li> <li>• 1 for report storage and organization</li> <li>• 1 for blood tests</li> <li>• 1 for diabetics</li> </ul>
6 Apps	had special request to be online	<ul style="list-style-type: none"> <li>• 4 Apps required customer invitation or verification code</li> <li>• 1 Application required membership</li> <li>• 1 Application required US citizenship</li> </ul>
5 Apps 4 Apps	not working related with wellness and sports	
2 Apps 1 App	had different aims than PHR was not qualified enough	
In the Apple Store, 62 Applications were excluded and only 15 applications were chosen for analysis		
<b>Google Play applications:</b>		
<b>Number of Apps excluded:</b>	<b>Reason:</b>	<b>Details:</b>
12 Apps 10 Apps	same as Apple Store connected with webpage and did not work on their own	
7 Apps 7 Apps	had different aims than PHR only for a specific country (no English version)	<ul style="list-style-type: none"> <li>• 1 Spanish</li> <li>• 6 Chinese</li> </ul>
6 Apps	specified for only one issue or specific for animals	<ul style="list-style-type: none"> <li>• 1 pregnancy</li> <li>• 1 diabetics</li> <li>• 1 vaccination</li> <li>• 1 laboratory results</li> <li>• 1 family health track only</li> <li>• 1 for pets</li> </ul>
5 Apps	not PHR (for wellness and healthy life)	<ul style="list-style-type: none"> <li>• 4 diet, water consumption and healthy life</li> <li>• 1 cigarette, alcohol</li> </ul>

3 Apps	not working
2 Apps	not qualified enough: they were PHRs with few features
1 App	wanted a US phone number for registration

---

In Google Play store, 57 Apps were excluded and only 4 applications were chosen for the next step.

---

#### *4.1.3. Analysis According to the Pre-Defined Criteria*

After the elimination procedure, the remaining applications were evaluated according to 10 pre-defined data elements: Allergies, Insurance, Problems/conditions, Lab Results, Procedures, Immunizations, Medications, Family history, Providers, Emergency contact and four features: ICE feature (In Case of Emergency), Import/export, Password, Images.

Except for security and coverage of genetic information, the results are given as binary code in results shown in Table 7 and Table 8; existence of a property is marked with “1” and “0” for its absence.

Table 7 and Table 8 show the results in detail. The highest score was 0.8/1 (three applications). In addition to the results tables (Table 7 and Table 8), the coverage of genetic information was searched across the selected applications. Nevertheless, none of the applications had any features related with genetics, so it was seen that there is still a big gap in application markets for mobile PHRs that also store genetic information.

The security measures were also checked and evaluated in the chosen applications. Except from one application, every application had at least one security protection mechanism. The security measures used were:

- User name (ID) – password login: Except from 2 applications all applications had this safeguard (17 Apps)
- E-mail confirmation – activation: 6 applications had this property
- Security questions: 2 applications had security questions defined at the first login
- Security key: only 1 application

When we look at these results, we can see that there are limited kinds of security protections for personal health record applications and they are mostly basic measures like password, security questions, etc. There is lack of examples of multiple security safeguards for mobile PHRs. None of the applications has CAPTCHA, Mobile Signature, One Time Password, One Time SMS Password, Process Limitations, Welcome Message and/or Picture, or Virtual Keyboard security properties.

The symbols “\*\*\*\*” and “\*\*\*\*\*” in Table 7 and Table 8 mean that the applications are the ones that fit the purpose best and have a user-friendly design.

Table 7 mPHR applications in AppStore

	<b>mPHR name</b>	<b>Problems/ Conditions</b>	<b>Procedures</b>	<b>Medications</b>	<b>Providers</b>	<b>Allergies</b>	<b>Lab Results</b>	<b>Immunizations</b>	<b>Family history</b>	<b>Emergency contact</b>	<b>Insurance</b>	<b>Average data elements covered by each mPHR</b>	<b>Password</b>	<b>ICE feature</b>	<b>Import/ Export</b>	<b>Images</b>
1	Secuera***	1	1	1	1	1	0	1	0	1	1	0,8	1	1	0	0
2	inPHR	1	0	1	1	1	1	1	0	1	0	0,7	1	1	0	1
3	Pocket Health	1	1	1	0	1	1	1	0	1	0	0,7	1	1	0	1
4	Clarus PHR Lite	1	1	1	1	1	0	1	0	0	0	0,6	0	0	0	0
5	Health tracker & manager	1	0	1	1	1	1	0	1	0	0	0,6	1	0	0	1
6	Healthmemo	1	0	1	0	1	1	1	0	0	1	0,6	1	0	1	1
7	HealthStylus	1	0	0	1	0	1	1	1	0	1	0,6	1	0	0	0
8	YourHealthRecord Mobile	1	0	1	1	1	0	1	1	0	0	0,6	1	0	0	0
9	Axilla	1	1	1	0	1	0	1	0	0	0	0,5	0	0	0	1
10	MyClinicNotes	1	1	1	0	0	1	0	0	0	0	0,4	1	0	0	0
11	IUVOHealth***	1	0	1	1	1	0	0	0	0	0	0,4	1	0	1	1
12	Healee	1	0	0	0	1	1	0	0	0	0	0,3	0	0	0	0
13	Health Companion	1	0	1	0	1	0	0	0	0	0	0,3	1	0	1	0
14	PersonalHX	0	0	1	0	1	0	1	0	0	0	0,3	0	0	0	0
15	Thareb Alhayat PHR	0	0	1	0	0	0	0	0	0	0	0,1	1	0	0	0

Table 8 mPHR applications in Google Play

	<b>mPHR name</b>	<b>Problems/ Conditions</b>	<b>Procedures</b>	<b>Medications</b>	<b>Providers</b>	<b>Allergies</b>	<b>Lab Results</b>	<b>Immunizations</b>	<b>Family history</b>	<b>Emergency contact</b>	<b>Insurance</b>	<b>Average data elements covered by each mPHR</b>	<b>Password</b>	<b>ICE feature</b>	<b>Import/ Export</b>	<b>Images</b>
1	ITRIAGE****	1	1	1	1	1	1	1	0	0	1	0,8	1	0	0	1
2	Continous Care	1	1	1	1	1	1	1	0	1	0	0,8	1	1	0	1
3	Track My Medical Records	1	1	1	0	1	0	1	0	1	0	0,6	1	1	0	0
4	EasyMed	1	0	1	0	1	0	1	0	0	1	0,5	1	0	1	0

#### 4.1.4. Turkish Mobile Applications in the Markets

The Turkish translation of the keywords “Personal Health Records” and “Health Records” only, that is “Kişisel Sağlık Kayıtları” and “Sağlık Kayıtları,” were searched in IOS and Google Play. However, there were no results in IOS and in Google Play; there were only foreign PHRs and some Turkish training and diet applications. Therefore, the keyword “Health” – “Sağlık” – was searched on the IOS platform. There were 354 results, none of which was for health records. There were some private hospital applications, but none of them could be used as medical data storage. In these applications, the user can mostly see lab results, get an appointment, and ask questions to his or her doctor. The rest of the applications were mostly about wellness, diet, and exercise.

In July 2015, a mobile version of e-Nabız was released; hence, we could repeat the analysis for e-Nabız, which was developed by the Ministry of Health in January 2015 as a web-only personal health record system.

E-Nabız was also evaluated according to our criteria, and the results are presented in the later paragraphs; however, the results showed that there is no independent Turkish mobile PHR in the markets. So, there is a deficiency both in markets and in the literature.

This application is important for our study because of two main reasons. First, it is the only application in Turkish and has countrywide user profile. Secondly, it has the online banking security safeguards that we were using as gold standard for the next part of the following study (the survey). Therefore, it was good to see which safeguards they used and how they applied them to the system.

Actually, e-Nabız does not fit rules IV and V: it is a country-specific application (for Turkey) and it is not working without an internet connection. However, e-Nabız has a privilege since it is the only Turkish application and it has many security protections we proposed.

E-Nabız was evaluated according to 14 pre-defined criteria in Table 9 (“-” for absent, “+” for available).

Table 9 Evaluation of e-Nabız

Problems/conditions	+	Allergies	+	Insurance	-
Procedures	+	Lab Results	+	Password	+
Medications	+	<i>Immunizations</i>	-	<i>ICE feature</i>	-
Providers	+	Images	+	Emergency contact	+
<i>Family history</i>	-	Import/export	+		

Three of the 10 data elements (*Problems/conditions, Allergies, Procedures, Lab Results, Medications, Immunizations, Insurance, Providers, Emergency contact and Family history*), three were not covered by e-Nabız: *Family history, Immunizations and Insurance*. Hence the total score is 0.7. Apart from these, there are *Password, Images and Import/export* features. Nevertheless, the *ICE* feature (*In Case of Emergency*) is not included in the application. Although the score of the application is high, more importantly, the security protection of the application is at the highest level compared to all the applications that we analyzed. Username/Password login and One-time SMS passwords are used as protection.

#### 4.1.5. Data Elements and Features Covered by Applications

The percentages of data elements and features covered by the selected 20 applications (including e-Nabız) are given in Table 10. Data elements called *Problems/conditions, Medications, Providers, Allergies, Lab Results* and *Immunizations* reach a percentage of 50% or more and *Password* is the most frequent feature of mPHRs in mobile markets.

Table 10 Average percentage of mPHR data elements and features

<b>Data elements/Features</b>	<b>Percentages</b>
<i>Problems/conditions</i>	<b>90</b>
Procedures	45
<i>Medications</i>	<b>90</b>
<i>Providers</i>	<b>50</b>
<i>Allergies</i>	<b>85</b>
<i>Lab Results</i>	<b>50</b>
<i>Immunizations</i>	<b>65</b>
Family history	15
Emergency contact	30
Insurance	30
<i>Password</i>	<b>80</b>
ICE feature	25
Import/export	25
Images	45

## 4.2. The Survey

### 4.2.1. Results of the Pilot Study

IBM SPSS Statistics v22 was used for the analysis of the questionnaire results and the details of these results are given in the following parts: Participant Profile, Reliability Result, and Analysis of Participants' Responses and Changes for Actual Survey.

#### 4.2.2. Participant Profile:

There were in total 20 participants in the pilot study, eight women and 12 men. Education levels of the participants varied between PhD and primary school. A degree coding method is used to scale education levels; participants with a PhD or a master's degree are coded as five and primary schools as one. The average level of education in this study was 3.75. The participants were mostly living in Ankara (65%) and Istanbul (25%).

The age ranged between 20 and 66 years and the average age of the group members was 36.6 years. The minimum family income among the participants was 700 TL, the maximum 7,000, and the mean income of the participants was 3,729 TL. According to Türk-İş January 2015 Annual Report (Ocak 2015 Açlık ve Yoksulluk Sınırı, 2015), the poverty limit for a family in Turkey was an income of 3,772 TL, and the mean value in our study came quite close to it.

The mean values of the Computer and Smart Phone values are very close to average. Hence the participant profile is very close to the average considering the demographic variables (see Table 11).

Table 11 Frequency of family income, computer and smart phone literacy

		Family income	Computer literacy	Smart Phone literacy
N	Valid	19	20	20
	Missing	1	0	0
Mean		3,728.947	2.6	2.5
Range		6,300.0	4.0	4.0
Minimum		700	1.0	1.0
Maximum		7,000	5.0	5.0

#### 4.2.3. Reliability Analysis (Cronbach's Alpha):

Reliability analysis was performed in this study to calculate internal consistency of the scale. Cronbach's alpha is the most common way to indicate internal consistency (Pallant, 2013). The results of the analysis should be at least 0.7 or above in order to talk about a consistency (ibid.) and it is calculated as 0.708 in the study.

The pilot showed that it was necessary to make modifications, extraction and additions to the current questions in the questionnaire.

There are some questions in the questionnaire that ask for an experience of a situation that may happen very rarely. These questions are,

- Experience of avoiding to be tested in case someone can see your results
- Experience of asking a doctor to write down a different medical condition in medical records



The pilot showed that the responses to these questions were very valuable, so we decided to add one more question, which is asking if you or a member of your family have ever experienced a serious breach where your personal health information was used inappropriately or released without your consent.

“Have you ever experienced a serious breach where your personal health information was used inappropriately or released without your consent?” (Princeton Survey Research Associates, 1999)

Five of the 20 participants indicated that the questions are mostly long; especially question 24 is too long and confusing. Therefore, instead of deleting the whole question, we took out the least informative sub questions B, C and D.

24 - B: Establishing new regulations that explain in detail who can see and use which of your medical records,

24 - C: Establishing new legislations with serious punishments for people or organizations that violate medical privacy

24 - D: Having all the rights to access and use your medical records,

The family income questions do not give us any idea without knowledge about the number of family members. This question is updated under control of an expert and it is changed from an open-ended question to a multiple choice-scaled question.

5: Income:

Section break before the 8<sup>th</sup> question caused a misunderstanding with the question: “if you use any of the following security safeguards”. However, because of the title it is observed that people think only about online banking safeguards. The title is changed in order to solve this misunderstanding.

Section break: Questions about Internet Banking Security Protections  
8. Which of the following security protections have you previously used?

Three of the 20 participants indicated that many sub questions of question 24 are long and confusing, so the question A is shortened under the control of experts.

24 – A: Having the right to share medical data without identification information with hospitals and other health care providers who need medical information

Two of the participants indicated that questions 21, 22, 23 and 25, 26, 27 include too many repetitive words and are boring. Therefore, by taking into consideration the main aim of the questionnaire, which is the design of a mobile PHR for both health and genetic information, the questions are combined into one question.

21, 22, 23: Which level of access do you want to give the following people or organizations to your health records containing genetic information?

25, 26, 27: Which of the following people or organizations do you trust about the privacy of your health records containing genetic information?

#### *4.2.4. Survey Results*

The internal consistency of the instrument was tested using Cronbach's alpha coefficient for the analysis of reliability. Ideally, Cronbach's alpha coefficient is expected to be greater than 0.7 (Pallant, 2013), and the current scale was found to meet the required value (0.72).

#### *4.2.5. Demographics of Respondents*

The sample consisted of 174 people (100 women, 74 men) from 21 different cities in the Republic of Turkey. The average age of the participants was 34.09 ( $\pm$  8.98). The average monthly income of the participants was between 2,001 and 4,000 TL. In Turkey, the hunger line was 1,257 TL and the poverty line for a family of four was 4,094 TL in 2015 ("Ocak 2015 Açlık ve Yoksulluk Sınırı," 2015). The participants were from various educational backgrounds, the highest frequency being bachelor's degree holders (50.6%), followed by graduate degree holders (35.1%). The percentages of other educational levels were as follows: high school graduates 10.3%, middle school graduates 2.9%, and primary school graduates 1.1%. Most of the participants stated that they had an above-average (70.7%) or average level of computer literacy (20.7%), and similar rates for smartphone literacy were reported: 73.6% for above-average level and 13.8% for average level.

#### *4.2.6. Level of Knowledge and Experiences on Health and Genetic Data*

In the online survey, we reached 16 people who or whose family members had previously taken a genetic test. In addition, 69 people from two genetic testing centers completed the questionnaires. Thus, in the sample pool, the total number of people who or one of whose family members had previous personal experience with genetic testing was 85 (48.9%). Furthermore, to acquire the views of other participants who had not taken a genetic test before, the following question was added to the survey: "What would you do if you were offered genetic testing?" As a result, 96.6% of the non-tested participants reported that they would take a test if necessary.

A great majority of the participants (60.9%) stated that they did not know who had the right to access their medical records. Only a small number of the participants (7.4%) believed to have comprehensive knowledge about the topic. When asked about their knowledge of genetic science, 47.6% of the respondents indicated that they knew nothing or had very little knowledge. The rest of the participants (52.4%) had either average or above-average level of knowledge in this area.

Three items in the questionnaire (Q17-Q19) aimed to reflect participants' experience about the sharing of their health data. Seventeen participants (9.7%) responded that their medical records had previously been inappropriately used or released without their consent (see Table 12).

Table 12 Responses to the item, “Have your medical records ever been inappropriately used or released without your consent?”

	n	%
Yes, my data has been shared with a third party without my consent.	4	2.3
Yes, my data has been shared with my employer/my insurance company without my consent.	11	6.3
Yes, my data has been used in research without my consent.	2	1.1
No / I don’t know.	156	89.7
No response	1	0.6

In addition to the breach of medical confidentiality, 15.1% of the respondents stated that they had avoided being tested to prevent others from accessing their results. Moreover, six participants (3.5%) asked their doctors not to write their symptoms/diagnosis in their medical records or enter a less embarrassing alternative rather than the actual condition (see Table 13).

Table 13 Responses to the item, “Have you ever asked a doctor not to write down your health problem in your medical records, or asked the doctor to put a less serious or less embarrassing diagnosis into the record than was actually the condition?”

	n	%
Yes, I have asked a doctor not to include my health problem in my records.	1	0.6
Yes, I have asked a doctor to provide a less embarrassing condition for my records.	5	2.9
No, I haven’t.	166	95.4
No response	2	1.1

#### 4.2.7. Attitudes Towards Health and Genetic Data Exchange

We observed that the participants were sensitive about sharing their health/genetic data with third parties and they thought some regulations were needed for the protection of their privacy. Question 21 (Q21) concerned the level of access rights regarding genetic data included in medical records, and the majority of the participants (94%) responded to this question by stating that they should have full access. Approximately half of the participants stated that their children (57.5%), parents (55.7%), doctors (52.5%), spouses (50.3%), and other doctors or hospital staff (45.9%) should have limited access rights. Lastly, a considerable number of participants did not want to give any access rights to their neighbors/friends (83.9%), drug companies (83.2%), employers (81.4%), close relatives (65.4%), insurance companies (62.2%), or pharmacies (59.4%).

The responses to the item (Q24), “Do you trust the following stakeholders to keep your genetic and medical data private?” revealed that for the majority of the participants

(61.2%), doctors were the only trustworthy providers. The least trusted were insurance companies (82.6%), followed by information technology specialists (71.3%), the government (68.6%), pharmacists (63.9%), and nurses and other hospital staff (53.8%) (Table 14).

Table 14 Responses to the item, “Do you trust the following stakeholders to keep your genetic and medical data private?”

	<b>Yes</b>	<b>No</b>	<b>Not sure</b>	<b>No response</b>
Your doctor	61.2%	17.6%	21.2%	
	101	29	35	9
Nurses and other hospital staff	16.7%	53.8%	29.5%	
	26	84	46	18
Pharmacist	14.8%	63.9%	21.3%	
	23	99	33	19
The government	12.8%	68.6%	18.6%	
	20	107	29	18
Information technology specialists	7%	71.3%	21.7%	
	11	112	34	17
Insurance companies	4.5%	82.6%	12.9%	
	7	128	20	19

Table 15 Respondents’ views about the effectiveness of regulations proposed to protect their privacy and confidentiality

<b>Options</b>		<b>Sum of 1-2 rates</b>	<b>Sum of 3-5 rates</b>	<b>Not sure</b>	<b>No response</b>
C3: Using trustworthy security systems that use passwords and encrypted data on the device where your information is stored	% n	10.8% 17	82.8% 130	6.4% 10	17
C4: Having the option to see when and by whom your records are retrieved	% n	14.5% 23	79.8% 127	5.7% 9	15
C1: Ensuring that doctors and healthcare providers who need access to your medical information only use data that does not contain any personal identity information	% n	22.3% 35	65.6% 103	12.1% 19	17
C2: Having the option to see, correct, or even delete your medical records	% n	35.9% 56	49.3% 77	13.2% 23	18

Four regulations were proposed to the participants for the protection of the confidentiality and privacy of genetic data included in their electronic records (Q22). A

five-point Likert-type scale was used for the evaluation of this question, and according to the results, three of the four suggested regulations were found to be potentially effective (Options 1, 3 and 4). Option 2 was neither supported nor rejected. Details are given in Table 15.

#### 4.2.8. Views on Mobile Applications for Health/Genetic Data Management

We collected the participants' views concerning the use of mobile applications for health/genetic data management. Q23 inquired about the kind of information the participants would like to keep in a health record application installed on their smartphone. We also wanted to determine whether the participants were willing to keep their genetic data in their mobile health record application; therefore, we added "Inherited diseases" to the options. The participants were allowed to choose more than one option for this question. All the options were chosen by more than 50% of the participants. The top six responses were allergies (84.2%), medication (83%), in case of emergency (ICE) number (81.9%), diseases and health problems (77.8%), operations (72.5%), and vaccines (71.3%). Even if the option of inherited diseases had a lower response rate compared to the others, it was still chosen by more than half of the participants (56%). The details of the responses are presented in Figure 3.

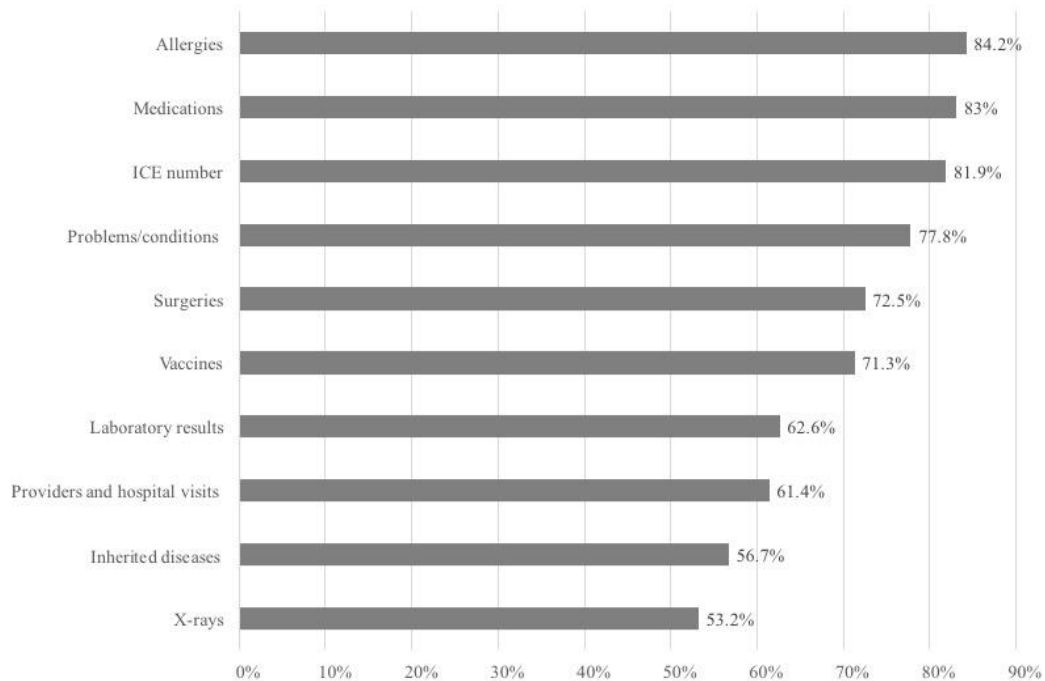


Figure 3 Types of information the users wanted to see in a mobile health record application

Q25 was related to the participants' attitude concerning the privacy requirements of different types of information and risks involved in storing it in a mobile application. The responses to this question are presented in Table 16. The results demonstrated different attitudes towards health and genetic information. A significantly higher number of participants considered that genetic information was at a higher security risk (62.2%)

than health information (44.6%) stored in mobile applications ( $p=0.00$ ), and the respondents were concerned about the security of their genetic information nearly as much as their identity and personal information.

Table 16 Responses to the item, “What do you think about the security risks of storing the following information in a mobile application?”

	Security risk	No security risk	Not sure	No response
Health information	44.6% 74	38% 63	17.5% 29	8
Genetic information	62.2% 102	23.8% 39	14.0% 23	10
Address, phone and other personal information	66.5% 107	23% 37	10.6% 17	13
Identity information	68.1% 111	21.5% 35	10.4% 17	11
Bank account information	81.5% 132	8% 13	10.5% 17	12

In terms of online banking, most participants (87.4%) reported that they had used these services before, and only 16.1% of these participants considered online banking safeguards to be insufficient for protecting the security of their information. Moreover, eight participants (4.8%) previously had negative experience when using online banking; one of them still believed that using online banking was secure while three were not sure about it. The responses to Q25 showed that the majority of the participants either thought that none of their information could be safely stored on mobile platforms or were not sure about the risks involved. Bank account information was at the top of the list, being chosen by 81.5% of the participants. Despite these negative views, our analysis showed that almost all the participants had used or were using online banking systems (Table 17).

Table 17 Cross tabulation of the participants’ views on storing bank account information in mobile applications and their experience with online banking

	Bank account information			Total
	Security risk	No security risk	Not sure	
<b>Have you ever used online banking?</b>				
Yes	114	12	15	141
No	18	1	2	21
Total	132	13	17	162

Q20 was directed at the participants to determine their preferences related to the security measures in an application that would store their medical and genetic data. The participants were allowed to choose more than one option for this question. Almost all the respondents (96%) preferred the application to have at least one security feature, with the prominent responses being ID/password login (73.6%), one-time password (OTP) over SMS (55.7%), and mobile signature (43.1%) (Figure 4). In addition to the options we provided for online banking security, we included the ‘other’ option for participants to make their own suggestions. Three participants suggested using fingerprint and one participant suggested voice authorization system as a security feature.

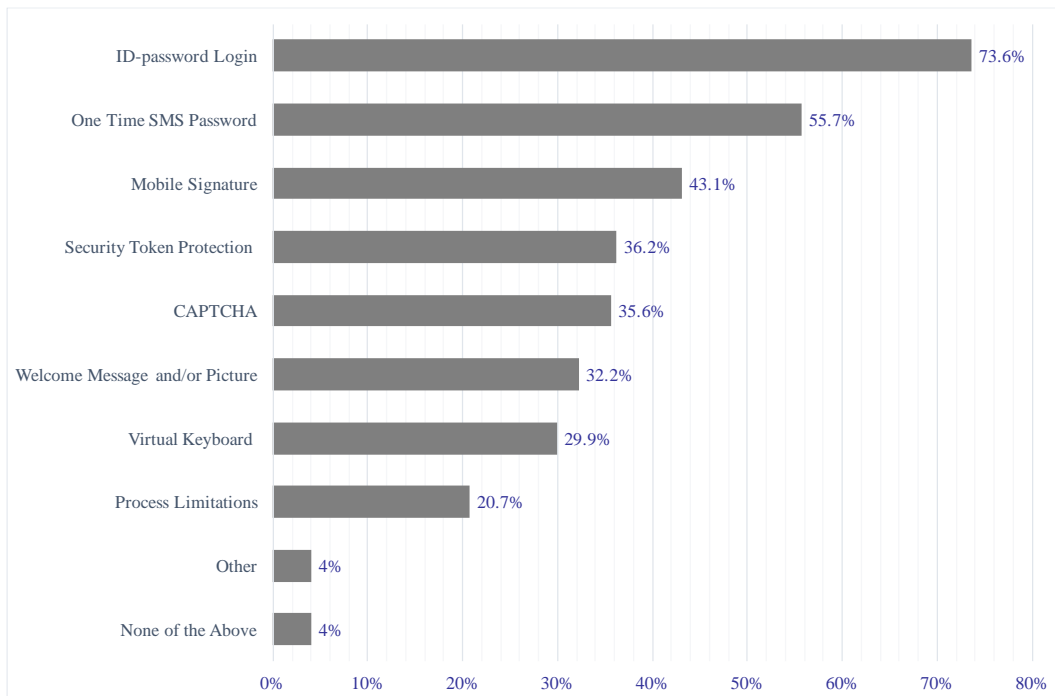


Figure 4 Security features the participants would like to see in an internet-based health/genetic data record system

#### 4.2.9. Differences Between Groups

Sex, age, educational level, and computer and smartphone literacy levels were found to have a significant effect on the participants’ views. No significant differences were observed in the income and experience of the genetic testing categories. Sex was found to affect the participants’ views concerning the access rights of their spouses significantly ( $p=0.04$ ). Unlike men, women tended to give limited or no access rights to their spouse (Figure 5).

A significant difference ( $p=0.02$ ) was found between university graduates and those from other educational backgrounds in terms their views on the rights of their doctor to access their medical and genomic data. Unlike the participants with a lower level of

education, most participants with university degree or above preferred their doctors to have limited or no access to their medical and genomic data (Figure 6).

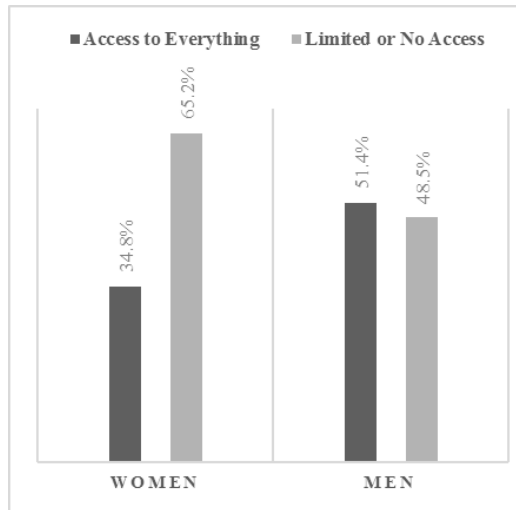


Figure 5 Comparison of the views of women and men regarding the rights of their spouse to access genetic data in their medical records (The post-hoc computed achieved power for  $w=0.3$ ,  $\alpha=0.05$  and  $n=165$  was 97.0%)

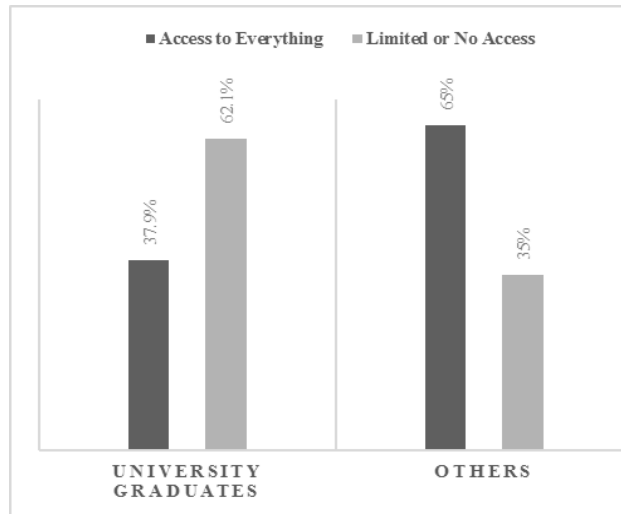


Figure 6 Comparison of the views of university graduates and those from other educational backgrounds regarding the rights of their doctor to access genetic data in their medical records (The post-hoc computed achieved power for  $w=0.3$ ,  $\alpha=0.5$ , and  $n=160$  was 96.6%)

When the chi-squared test was repeated for the age groups, a significant difference was seen in the preferences of access by third parties for respondents under the age of 35 ( $p=0.00$ ). Although the majority of the age groups tended to give their children limited or no access to their medical and genomic data, participants younger than 35 had more concerns about sharing their data with their children (see Table 18).

Table 18 Participants' views on their children's access to their genetic and medical data by age group. (The post-hoc computed achieved power for  $w=0.3$ ,  $\alpha=0.05$  and  $n=154$  was 96.1%)

	Access to everything	Limited or no access	Not sure	No response	<i>P</i>
≤35	24	99	4	16	.00
>35	15	16	0		

Furthermore, the intra-group comparison of computer and smartphone literacy groups demonstrated a significant difference of opinion between the participants regarding their doctors' right of access to their genetic and medical data. People with a high level of literacy in both areas chose to give their doctors limited or no access compared to those with a lower level of literacy (Table 19).



Table 19 Participants' views on their doctor's access to their genetic and medical data by level of computer and smartphone literacy. (The post-hoc computed achieved power for  $w=0.3$ ,  $\alpha=0.5$ , and  $n=160$  was 96.6%)

	Access to everything	Limited or no access	Not sure	No response	<i>p</i>
Low Computer Literacy	27	19	1	12	.00
High Computer Literacy	39	75	1		
Low Smartphone Literacy	23	17	1	12	.02
High Smartphone Literacy	43	77	1		

### 4.3. PD Workgroup

There were five participants in the PD group, referred to as P1 to P5 in this report.

Starting points of the discussions were both the results of the mPHR analysis and public opinions gleaned from the first results of the survey. At the end of the 11 participatory design meetings, a sample paper prototype of an mPHR including genetic data was drawn. Its main pages were titled *Login and Sign Up Pages, Profile Page, Main Page, Medications, Medical History, Lab Results, Calendar, Genetic/Genomic Information Page, Genetic Test Result Page, Social Page, Preventive Medicine Page, Doctors' Page, Profile Page, and 'Add to Main Page' Page*. The sample prototype had a total of 20 design templates as shown in Appendix D: Paper Prototypes of PD Workgroup.

The general rules of mPHR design obtained from 11 discussions can be summarized briefly as follows.: Since data privacy is very important for the highly sensitive information stored in the application, there should be a *Terms and data policy* information page on the opening screen including the rules of data sharing as well as the data privacy laws and regulations in Turkey. The content must be simple and understandable as suggested by GDPR ("General Data Protection Regulation (GDPR)," 2017).

All participants agreed that it is absolutely necessary to log in with at least one security measure, and for data privacy reasons, this should not include sensitive user information, such as national identity numbers. An e-mail address would be more convenient for *Login*.

Elements such as big buttons or add and remove options for ease of use were emphasized in the discussions. That is, on a single screen, there should be a maximum of nine big icons. As for frequently used pages, there could be an *Add to main page* icon on each inner page. If the icons were more than nine, more screens could be added to the page with the help of a slide.

The discussions revealed that the application should encourage the users to input information with minimal workload. Short and simple questions in the questionnaires,

autocomplete search boxes, Q-R/Barcode readers, and video camera usage were added to the sample paper prototype. Hence, the *Profile* and *Genetic Illnesses pages* direct a minimum number of short questions to the user, given that such requests may cause people to give up using the application. Furthermore, autocomplete search boxes were added to the pages of *Problems & Conditions/Medical History, Procedures, Allergies, Surgeries, Medications, Genetic Tests* and *Lab Results*. In this way, typing errors could be minimized and the process could be shortened. Q-R code and barcode readers are very basic technologies and easily added to an application, so it was planned to use them to automate adding a medication to *Medicines* page. With the help of the camera, the *Lab Results* would be easily added as .pdf or .jpg files to the application.

A *Preventive medicine* page was suggested by P3, a physician, in order to give physicians an opportunity to forward information on preventive actions they could suggest to their patients according to their health status and age.

A page for information on *Inherited disease/Genetic illnesses/Family history* was drawn from scratch in these meetings under the title *Genetic/Genomic Information*. A pedigree tool was added to the sample prototype since pedigree illustrations are used in genetic labs to show inherited disease relations in a family; this is found to be the most convenient way of genetic data storage and annotation.

With the input of the doctor (P3) and chronic patient members (P2 & P5) of the PD group, a *Calendar* was suggested as a menu that would be frequently used in such an application to follow up daily symptoms and give reminders for patients with chronic illnesses. Emergency information (e.g. blood type, allergies and chronic diseases) should be selected by the users and published on the *Emergency social page*. This information should always be accessible for anyone in case of an emergency situation.

The details of the 11 sessions are reported in the following sections.

#### 4.3.1. Session I.

Although, the participant group consists of five people, the first group meeting was held with four participants due to an emergency event the physician participant (P3), had to attend. However, two days later a personal meeting was organized with P3 and the first session was summarized to him in detail, so that he could catch up with the other members in a personal meeting the following week.

Since the group members already knew one another, the session, which was taped on a voice recorder, did not include an introduction part. Therefore, only one small questionnaire was administered to them, an overview of Participatory Design (PD) was presented, and discussions on the application design survey and mPHR analysis results were held.

After a small introduction about the project and a brief explanation of the participatory IT design method, the discussions were started looking at the results of the survey and the mPHR analysis. In the public survey, there had been ten choices for the main titles, determined according to the mPHR analysis,

All the titles were examined and with general agreement, all of them would be included in the application. In addition to the titles, the idea of adding an emergency social page came up in the discussion. This page would be a social media page and users might decide which user information would be on it. This information could be blood type, allergies, or chronic diseases that the user would like to share, so in case of an emergency situation, this information would become available to anyone who needed it.

#### *4.3.2. Session II.*

The second session was held about 4 weeks after the first one. The break was long because time was needed for the analysis of the new application version of the e-Nabız project. This analysis was done within the scope of the previous study (mPHR analysis). Even though it was not a pure PHR, it had different security protection features compared to the rest of the mPHR analysis result. Hence, a detailed analysis was needed to understand what it really offered as a PHR.

In this session, for the first time all the group members were in the meeting together. At first, P3 met with the others and introduced himself to the group. Then, a brief summary of what had been done up to that date including the first meeting was provided. After the introduction part, a participatory design technique, PICTIVE, was presented to the participants since this technique would be used in this and future sessions for paper prototyping. After a 5-minute presentation on PICTIVE, the group began by gathering around a table with our low-tech material to construct mock user interfaces. There were Post-it notes in various sizes and colors, pens, pencils and highlighters in many different colors, scissors, glue, big cartons, etc. Each carton represented one screen of the application. The session lasted approximately two hours and was videotaped as agreed. At first, the team members held a small consultation to choose a starting point for the session and agreed to focus on the main page. Nevertheless, when the group started to work on it, they realized that there should be two more pages to reach the main page which they had not thought about before. The first one was a login screen as a starting page, as it was obligatory to provide initial security to the application. The second one was a sign-up page for new users.

#### *Login and Sign Up Pages*

While working on the Login page design, the members understood that there were many details to consider for a simple login screen that we had not thought about until then; for example: What would be the user name? Choices discussed were e-mail address, TC Identity Number, or a unique user name chosen by the owner. Group members thought that e-mail would be the best choice since every person who uses a smart phone must have at least one e-mail address. Lastly, if users forgot their passwords, they only needed to enter their e-mail address in a popup box to receive a reminder. Appendix D: Paper Prototypes of PD Workgroup shows the design of the Login page with low-tech materials.

#### *New User Registration Page*

After the Login page, the group started to work on the “New User Registration” page. As mentioned above, two of the participants were health application programmers;

therefore, they had a base knowledge about interfaces for common pages like this one. Hence, the biggest contribution for this page came from them. P1 and P2 thought that the amount of information requested should be balanced in order to prevent users losing interest. Name, surname, year of birth, sex, e-mail, password, and repeat password were the only bits of information wanted on the sign-up page (see Appendix D: Paper Prototypes of PD Workgroup) and answers are suggested as mandatory fields. Questions about year of birth and sex were added to the small questionnaire for later health analyses and warnings. As mentioned, it was decided to use the e-mail address as a user name for the login. However, subsequently the group thought that e-mail activation was not a practical procedure for a mobile application and it was also not essential for security. It was decided that when usage of e-mail became necessary for the first time, the activation could be done by asking for a combination of e-mail and password.

#### *Terms and Data Policy*

While the group was talking about the regulatory issues, they realized that there should be a “*Terms and Data Policy*” that people should accept before login. These policies and terms would consist of the rules of data sharing in addition to data privacy laws and regulations in Turkey in an understandable short summary. The terms and data policies could be approved by clicking an unchecked checkbox before signing up for an account, proving explicit consent. The users could read these policies by clicking on the link and a document would appear in a pop-up window.

#### *4.3.3. Session III.*

The 3<sup>rd</sup> session was arranged for a week later and subsequent activities became weekly, so the group decided to come together every Thursdays during lunchbreak unless there were any obstacles. In the previous meeting, the group had decided to direct the users to a profile creating page after the first login. Just after the login page, it would appear on the screen and ask some basic questions about the general profile of the user. Hence, in this session, a Profile Page was designed by the group.

#### *Profile Page*

As stated above, this page would be seen after the first login. Later, there would be a quick link available on the main screen, too. There would be a small two-page questionnaire in order to investigate life styles and demographic information of the users. The group decided that there should be as few questions as possible in this mini questionnaire to avoid users getting tired. Firstly, the demographic part would appear on the screen: blood type, height, weight, education, occupation, current place of residence, marriage status, number of children (see Appendix D: Paper Prototypes of PD Workgroup). Input of the blood type would be asked in a two-part dropdown menu, first selecting the letter(s) and then the Rhesus factor symbols (Rh+, Rh-). Height and weight would be entered into double input-type textboxes. Education and occupation could be chosen from dropdown menus, the latter only including occupations associated with occupational diseases. There would be an “other occupation” button for the rest. The current residence input would be suggested by GPS location; in case the person did not allow the use of GPS for the application or would like to change the suggested city, a list

of cities would be available as an alternative option. The marriage status would be a radio button (Yes/No) and the number of children would be an integer-type textbox.

The second page of questions would be about the user's lifestyle. Smoking, alcohol consumption, and exercise habits would be investigated in this part.

Because the P3 (Doctor) stated that there was a difference between a person who never smoked and one who had quit smoking, the relevant question would be in multiple-choice format with the following choices:

- Yes, I am smoking
- No, I quit smoking
- No, I've never smoked

If the user chose the "Yes" answer, there would be a question which asked, "Do you want to be informed about your general risk level?" If the user replied "Yes", then he or she would be asked to give more information about his or her habit.

- How many packets do you smoke daily?
- How many years have you been a smoker?
- What kinds of cigarettes are you smoking?

The rest of the questions and choices:

Alcohol (multiple choice):

- Don't drink
- Very rarely
- Weekly
- Every day

Exercise habits (multiple choice):

- I am exercising regularly
- I am not exercising

In the exercise part, there would be questions about the users' daily work lives as well. However, this part would be activated with the "Yes" response to the occupation question of the demographic part.

Level of movement in daily work life (multiple choices): High; Middle; Low.

#### *4.3.4. Session IV.*

##### *The Main Page*

The main page was discussed in the fourth session. According to the group's opinion, using big icons as smartphone interfaces would promote the ease of use. Therefore, the final decision was to put a maximum of nine icons on one screen. Some of these icons would be placed by default whereas others would be accessible via sub links under these icons. There would be an "add to the main page" button for all these sub links; if the users wanted, they could add them to the main page as icons.

In this session, the group defined the default icons which would be seen on the screen when the application was first installed and the sub links titles (see Appendix D: Paper Prototypes of PD Workgroup). The names of the default icons and sub links were:

- *Medical History*: Diseases, Surgeries, Allergies
- *Test Results*: Laboratory test results, Radiologic images
- *Medicines*: Add medicine (With prescription and Without prescription), My medicines, Medicine reminder, Report reminder
- *Emergency Button*: Default SMS, ICE number
- *Calendar*: Appointment reminder, Medicine reminder, Report reminder, Preventive medicine reminder
- *Preventive Medicine*: Calendar (Link to Preventive medicine reminder under Calendar), Cancer screening, Cardiovascular disease screening, Eye screening, Dental screening, Vaccines, Blood pressure and diabetes measures (with a graphic), Weight tracking (with a graphic)
- *Genetic Information*: Genetic diseases, Genetic tests/results, Genetic report
- *Social Page*: Blood type, Allergies

#### 4.3.5. Session V.

In the fifth session, the group worked on the details of the main titles, starting with the Medications page.

##### *Medications Page*

The sub links of the *Medications* part were defined last week as: *Add medicine (With prescription and Without prescription)*; *My medicines*; *Medicine reminder*; *Report reminder*. On the first page, these links would appear on the screen with small icons in front of them, and when the *Add medicine* link was clicked, page 3.1 would be opened (see Appendix D: Paper Prototypes of PD Workgroup). There would be a Q-R code and a barcode reader which the user could use to read the code on the pillbox, adding it automatically to his or her medicine list. There would also be an opportunity to choose the medicine from a drop-down menu instead of using the code reader. Dose and frequency were also dropdown menus and there would be “other option” available for the doses. When the frequency was chosen, the *Reminder* would be active, and it would connect to the *Calendar’s Medicine reminder* section. An open-ended *Note* input field would be found after the remind question. If the medicine was entered under the “with prescription” link, there would be an extra section opened under the note field which asked if the user needed to be reminded to get a report. This report could be annual or biennial.

*My medicine* was another link under the *Medicines* button and its aim was to list all the medicines recorded to the application. There would be an edit option under this link, too. The reminder pages would be identical with the *Calendar’s* ones and they would be presented under that title.

#### 4.3.6. Session VI.

In the 6<sup>th</sup> week of the meetings, the group started to work on the heading *Medical History* and its subheadings *Diseases and conditions* and *Surgeries and Allergies*.

### *Medical History*

As shown in Appendix D: Paper Prototypes of PD Workgroup, there would be small icons behind and a plus sign (+) in front of each title. This design features (plus sign and mini icon) would be the default for all the other subheadings. With the help of the plus sign, the menus would be expanded and become clickable. The *Disease & Condition* page would have two slide menus to *Show* and *Add Diseases or Condition*. The *Add disease or condition* slide would include a search box and all the diseases would be listed below alphabetically. When the user started to write down the name of the disease, the list would be narrowed, and the users could stop writing whenever they saw what they were searching. After the disease was entered into the system, other fields would be opened: the name of the doctor, the hospital, the date, and there would be a link to the pages of *Medicines*, *Picture*, *Lab result*, *Surgeries*, *Reminder for appointment* to connect disease and other information. There would also be a system that recorded the name of the doctors and hospitals in order to remind the users for their next data input. Moreover, according to the disease entered by the user, an appropriate preventive medicine question would be asked. For example, if the user had diabetes, the system would ask “if you want to use sugar follow-up” or for a pregnant woman “whether you wanted to be informed about the necessary tests and controls about pregnancy”. The *Show Disease or Condition* slide would be used to see all the diseases added to the system as a list of disease names, and when one of them was clicked, the details would be presented in a popup window. There would be details written by the user when it was formed and the ICD10 code on this page. An edit button would be at the end of the window, and when it was clicked the *Add disease page* would be opened.

The opening page of the *Surgery* section would be the same as the *Disease and condition* page, so there would be slide pages again for the Add and Show submenus. However, a different design idea came to the group members’ mind while they were brainstorming about the *Surgery page*: to add a body sketch to the add link of the *Surgery* section. In other words, when the user clicked on the *Add a surgery* button, an outline of a human body (of the same sex as the user) would appear and the user could select the part where he/she had surgery. Then, an *add* page would be opened with a related list of surgery options. For example, if the user selected the chest, surgeries related with heart, breasts, liver, nerves, skin etc. would be listed and the user would be able to select the relevant organs, bones, or tissues. After selection, details would be asked on date, doctor, hospital, date of control, notes, and a connection to the Medicines page would be shown to add related medicine (see Appendix D: Paper Prototypes of PD Workgroup)

The allergies page had the same design, too (see Appendix D: Paper Prototypes of PD Workgroup). A slider menu for *Show* and *Add* options was used for this section as well. The *add* section of the allergen field would be a text box where the user could write anything. At first, the group thought of a prepared list like on the *Surgery* and *Disease and Condition* pages. Then they realized that there were a million kinds of allergies,

some of which were even unique to the patient. Therefore, they decided to use an open-ended textbox for this field. The other details are:

- allergy level (1 to 5),
- reaction to the item (textbox),
- medicine (link to *Medicines* page) and
- notes.

The *Show page* was designed the same way as the others for consistency.

#### 4.3.7. Session VII.

In this session, the *Lab results* and the *Calendar* pages were discussed. The group designed the sample interfaces as shown in Appendix D: Paper Prototypes of PD Workgroup.

##### *Lab Results*

The page would be opened showing a list of results, and if there was no result recorded to the system, the message “There is no result on the list” would be shown on the screen. Otherwise, the results would be listed as a summary on the screen, and by clicking on each one, the details would be shown in a popup window. The *Add result* button would be in the right top corner and when clicked, the *Add result* page (see Appendix D: Paper Prototypes of PD Workgroup) opened. The fields of the *Add Result* page were:

- Result title
- Date
- Name of the lab
- Add a picture
  - Gallery
  - Take a photo
  - Add a link
  - Add a file
- Notes

##### *Calendar*

After the *Lab result* page, the group had still time to work on the *Calendar* page (see Appendix D: Paper Prototypes of PD Workgroup). An electronic calendar and the current month would be on the screen. The days would be shown in different colors previously chosen by the user when he/she entered a reminder. The group thought that people might use the same color for the same event; for instance, yellow for report reminders or blue for medicine reminders, etc. When a date was clicked, a menu would appear at the bottom of the page showing a list of reminders with the time and title. At the top right, there would be plus sign (+), list and search buttons. By selecting a date and then clicking the plus sign, the user could add a reminder to that date. The fields in *Add a reminder* page were:

- Title (Textbox)
- All day long (Checkbox)



- Beginning time
- Ending time
- Repeat the warning
  - On the time
  - 5 minutes
  - 1 hour before
  - 1 week before
- Notes
- Color palette

#### 4.3.8. Session VIII.

During this session, the group started to talk about the *Genetic/Genomic information* page. They decided which information they should request from the users and how to display it on the interface. The *Genetic/Genomic information page* was planned to include data on Inherited diseases/Genetic illnesses/Family history.

##### *Genetic/Genomic Information Page*

The first question planned to be directed to the user was “Do you have any genetic disease you know of?” The user can choose his or her disease via a search box under the question. The second question would appear according to the sex choice of the user; hence if the user was female, the question “Have you had a miscarriage?” would be shown.

Gazi University Genetic Research Center was consulted about genetic/genomic data collection. At the center, pedigrees were used to collect and present the data. The group approved the idea and decided to ask the use questions about family history in order to set up a pedigree. According to the advice from the consultants, the pedigree should represent three generations. Hence, if the user did not have any children, the grandmothers’ and grandfathers’ information should be investigated. In the graph, a circle represents a female and a square represents a male individual (Bennett, French, Resta, & Doyle, 2008).

The questions which should be asked to users:

- Are you married?
- Do you have any children?
- How many siblings do you have?
- Are there any known diseases in your family?
- Siblings, children, father, mother, grandfather, grandmother: Do they have any diseases? Do they have children? Did they have any miscarriage?

Then, the group decided to take information about the numbers of the user’s relatives: How many siblings, children, aunts (maternal and paternal sisters), uncles (maternal and paternal brothers) do you have? The user’ marital status would automatically be seen on this page. If the user had not answered the question before, it would be repeated here.

Some genetically-based diseases such as diabetes, cardiac diseases and cancer types would be listed and the user would be asked whether any of his or her relatives, specifically mother, father, a sibling, grandmother, grandfather, children, aunt (mother and father's sisters), or uncle (mother and father's brothers) have any of these diseases. Finally, the pedigree will emerge on the screen (see Appendix D: Paper Prototypes of PD Workgroup). The symbols on the pedigree would be clickable, and when the users click on the lines, squares, or circles, they can see or update the related information.

#### *4.3.9. Session IX.*

In the 9<sup>th</sup> session, the group continued working on the genetic information page and designed a genetic test results page (see Appendix D: Paper Prototypes of PD Workgroup).

##### *Genetic Test Results Page*

In the top right corner, there would be an “*Add a test result*” button as in the other result pages. The results would be listed in the opening page with a title and a date. When one of them was clicked, details would appear on the screen. Details are notes, images, disease, the test type (Chromosome, Gene, Array, etc.), result, comment, and an edit button.

##### *The Social Page*

After the group finished the genetic test page, they started to design the *Social page*. They planned this page as a social media page which would be reachable without any ID/password login restrictions. Blood types and allergies of the users would be published on this page as a default. The information published here could be reachable from other users' social pages and on a webpage. The users would have the right to hide or publish any information about themselves. If it was sensitive information, the application would give a warning and request a second confirmation from the user. The first time the page was clicked, the application would ask which of their current diseases they wanted to share on this page. The current diseases of the patient would be listed under the question. There would be a warning saying that “this information could be seen by other users”. Then the system would offer to join forums about the user's diseases. The users could log into these forums with a user name instead of real name or e-mail address. Furthermore, they could show their blood type and see announcements relevant to their blood type in the right corner. Lastly, an edit profile button would be in the right corner of the page (see Appendix D: Paper Prototypes of PD Workgroup).

#### *4.3.10. Session X.*

In this session, the group talked about the *Preventive medicine* page. This page was proposed by the doctor participant, P3, of our design group, and he consulted the group about which preventive actions the doctors would like their patients to take according to their health status and age.

### *Preventive Medicine Page*

At the first run of the page, there would be an alert reminding the users about the genetic information part: “If you fill in the genetic information part of the application, the alerts and information under this heading will be more accurate for your health status”. This information would be on the screen with a warning saying, “Please consult your doctor before starting to apply any of these instructions.” Then the system would ask:

- Do you have any other chronic diseases, in addition to your diseases selected in the *Diseases and Condition* page?
- If you are female, “Are you pregnant?”

The preventive medicine information will be listed under 10 headings:

- Eye
- Tooth
- Cardiovascular Diseases
- Cancer
- Pregnancy
- Vaccines
- Tests (CAGE, Obesity, Framingham, etc.)
- +65 Tests
- General Suggestions
- Others

These titles would be presented as listed above. When the user selected the combo box “Show only relevant ones”, the system eliminated the headings that were not relevant to the user’s profile. For example, if the user was not over 65, the title “+65 Tests” would not be seen on the list (see Appendix D: Paper Prototypes of PD Workgroup).

#### *4.3.11. Session XI.*

This session was the last of our meetings. During the session, the group talked about three different pages (*Doctors*, *Profile page* and *Add to main page*) and necessary security protections of the application (see Appendix D: Paper Prototypes of PD Workgroup).

#### *The Doctors Page*

The doctors that the user had visited before are presented as a list with five empty ranking stars on the opening page. When the users clicked on them, they could see the details about the doctor and they had the opportunity to edit the information there. Adding a new doctor would be possible including Name, Surname, Department, and Hospital Information.

#### *The Profile Page*

The Profile Page would be reachable via a small icon in the top right corner of the *Main Page*. It would store general and lifestyle information. General Information includes Name and Surname; Age (Date of Birth); Gender; User Name (e-mail); Password; Blood

Type; Education; Occupation; Marriage Status; and Number of Children of the user. Lifestyle information included Smoking habits; Alcohol use; and Exercise habits.

#### *Add to Main Page*

Lastly, the group talked about the “*Add to main page*” Page. When clicked, a map of the application would be seen consisting of main headings and subheadings. The user can add any of them as an icon to the main page.

#### *Security Protections*

The group thought that there need to be at least one security measure beside ID/Password login, a terms and conditions page, and a control to see who has access to their records.

As a result of the discussions, possible solutions for needs of a mobile personal health record application including genetic/genomic data were discussed and with the help of the PICTIVE method, a paper-prototype was created page by page.

#### *4.3.12. UML, Workflow and Dataflow Diagrams*

UML, workflow and dataflow diagrams were drawn according to the sample paper prototype developed by the PD group (see Figure 7, Figure 8 and Figure 9).

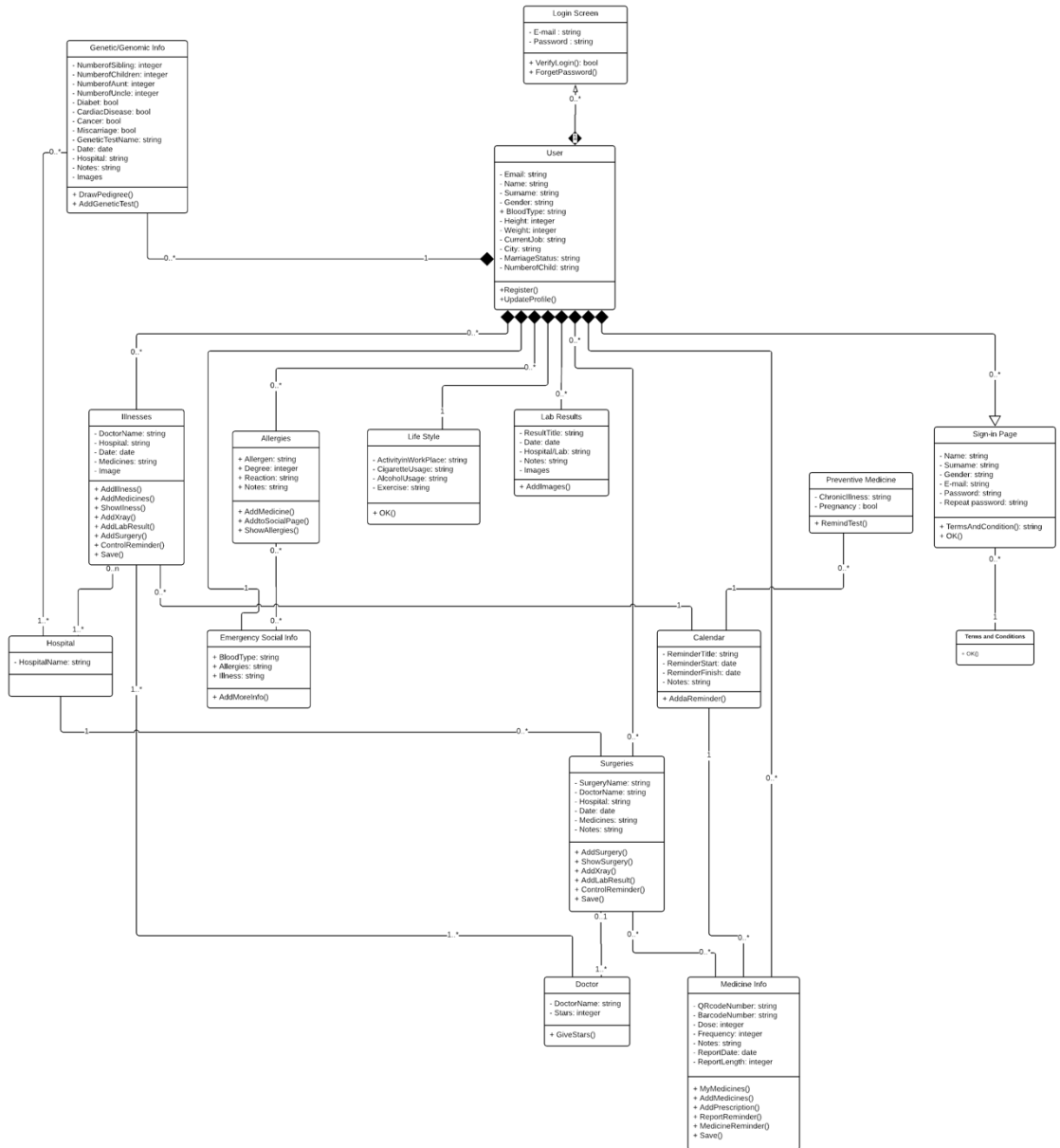


Figure 7 UML Diagram

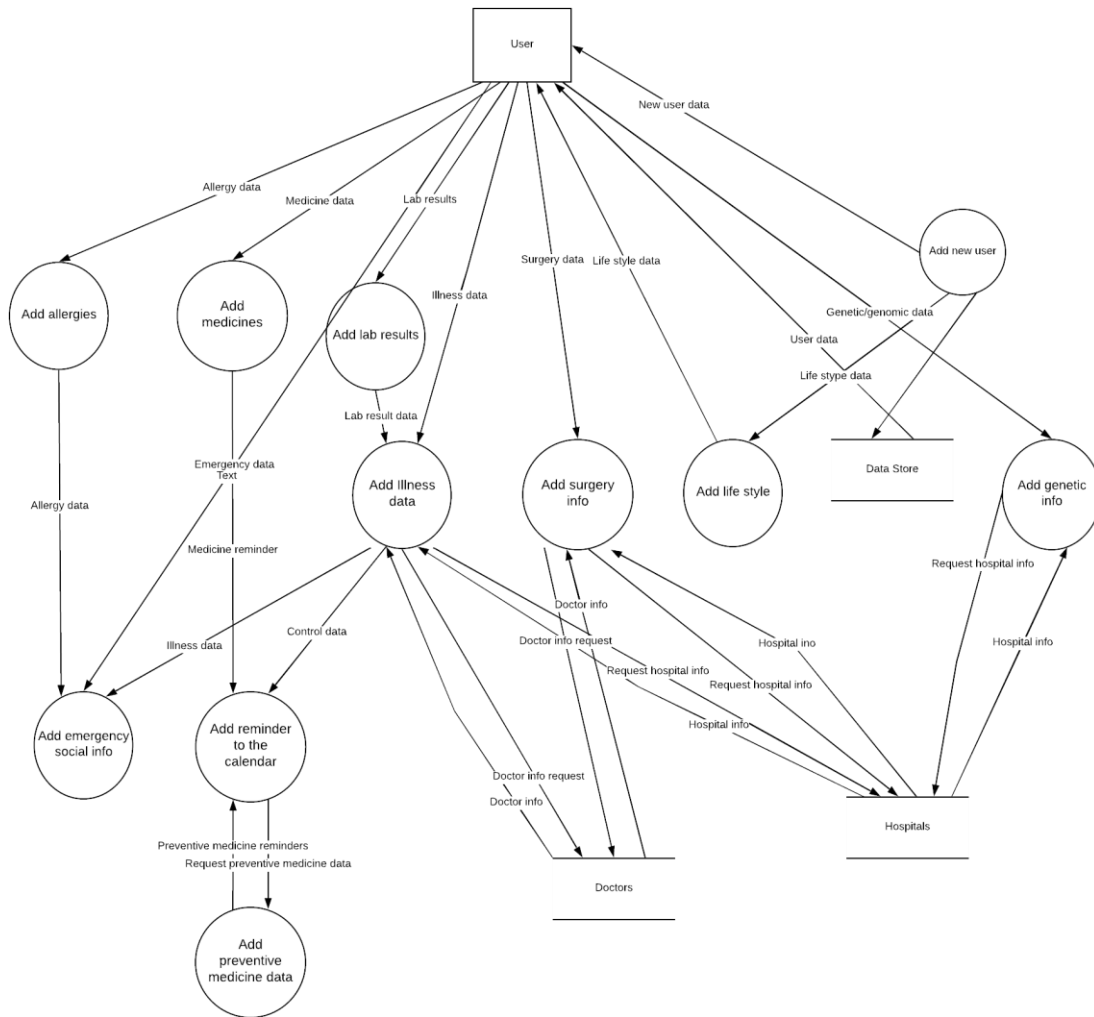


Figure 8 Dataflow Diagram

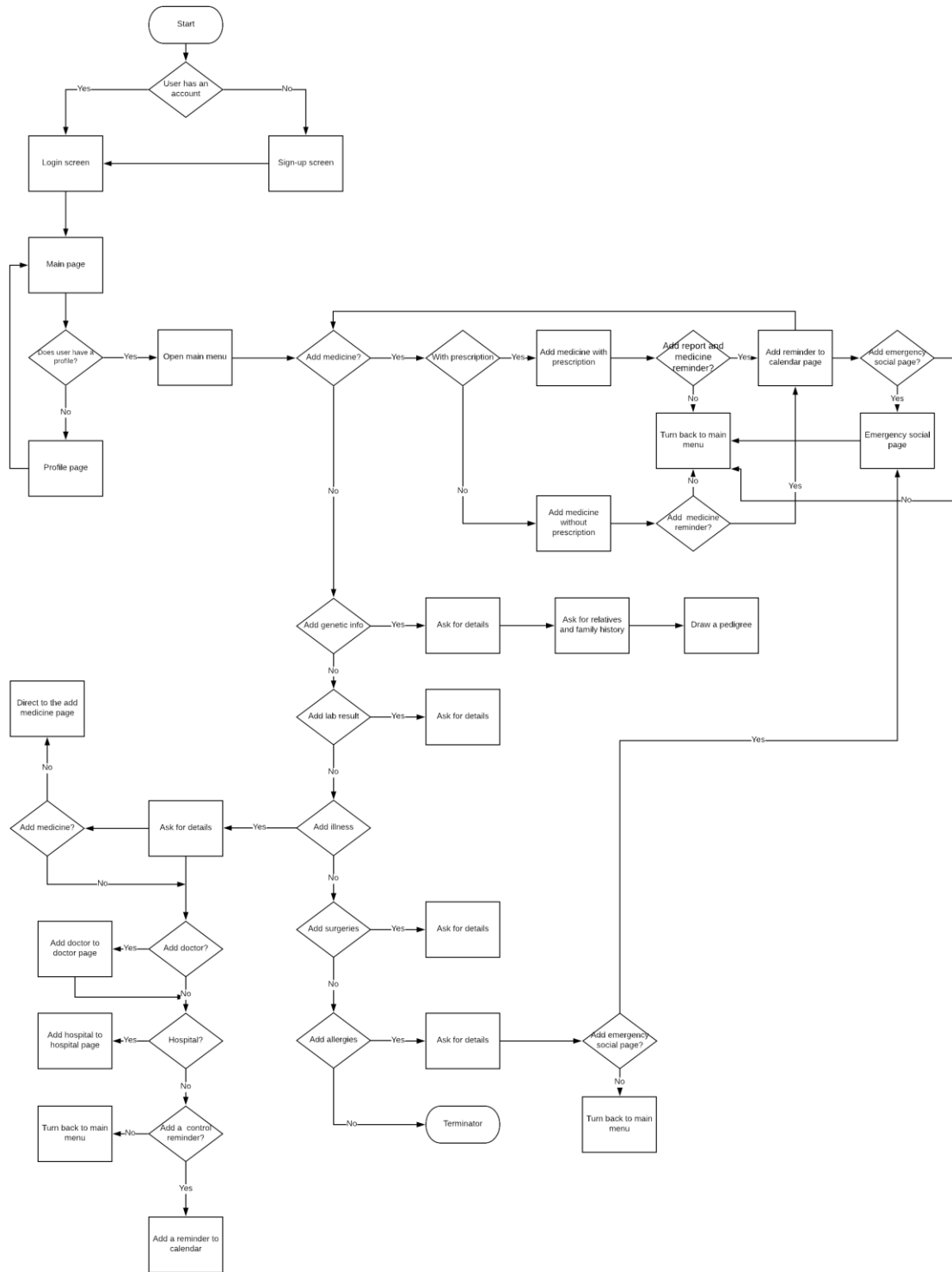


Figure 9 Workflow diagram

## 4.4. Analysis of Focus Group Meetings

Our analysis revealed four thematic areas:

- Lack of access and usage regulations for medical data, E-Nabız
- Management of genetic information in electronic health records
- Governmental business culture
- Public perception of risks, government failure, mishandling of data

### 4.5.1. Lack of Access and Usage Regulations for Medical Data, E-Nabız

#### *Health data should be collected*

As we mentioned previously, the first group discussions were mostly focused on the new data privacy law and regulations of Turkey. In both sessions, none of the participants were against the collection of health data; on the contrary they believed that this collection is necessary. Nevertheless, they had some concerns, and many criticized the current situation. Participants accepted that data collection was an obligation and it was beneficial for public health and economy. However, they were mostly against collecting the entire data in one center because of concerns regarding privacy, security, and anonymity of the data.

*NH: "...as an NGO, we have no objection to the collection of health information ... we have no objection to the collection of these data in the place where it was collected. ... Nevertheless, what we strongly oppose is the gathering of these data from hospitals, health departments, examinations, private places, etc. in one single center. Moreover, when these are gathered without anonymization, it is not possible to talk about confidentiality, security, or anonymity."*

*ZB: "The main goal is to reduce costs, reduce risks, diagnose, be beneficial to patients and the society, but when it is not done with the right methods, the concerns and the issues we are discussing here arise."*

One participant also stated that this data is already stored by the Ministry of Health; however, the important questions are with whom, when, and under which conditions this data will be shared:

*UU: "...beyond the storage of the data, it should be talked about how to share the data, with whom and under which rules. However, when it comes to confidential information such as patient data, I think that it can provide a lot of help to find and propose rules and mechanisms such as security mechanisms, rules for sharing and evaluating, etc."*

The concerns arose on the issue of central storage; however, as UU stated, the current system of the Ministry of Health was also central, so she emphasised the importance of regulations and laws on data privacy.

#### *The law legalized data sharing*



Participants viewed the law so unfavorably that they thought it would have been even better if it had not been issued in the first place. NH, a lawyer, thought that the situation had been better before the PDP law was passed:

*NH: "... I am saying this in quotes: it would have been better if the law had not been enacted. That's because [unauthorized data collection] was a crime before the law came out but now it is legalized. For the law makes it easy to capture and collect personal data, not to protect it; we have hesitations. "*

Another participant, from the second focus group, stated that the PDP law legalized unauthorized access in some way.

*OB: "Hacking is a crime, if a man is caught in the act, he has committed a crime. Nevertheless, on the other hand, the law is the main problem when it says, 'this is my right, I can share it or anybody else I decide can'."*

There are two general problems with the law: an excessive amount of exceptions and data collection without consent in article 6, paragraph 3. Our participants pointed out that even data about patients' sexual life can be processed without the consent of the data owner according to that paragraph.

*NH: "Exceptions are very wide; there are too many exceptions. The bowl is uncovered and the umbrella that protects it is too narrow. Hence the number of data sub-categories unprotected by the law is more than the ones being protected."*

The reference is to article 6 paragraph 3 PDP law because it gives the right to collect and process some sensitive data to individuals and institutions that are assigned by the law and are under the obligation to keep secrets, but without the consent of the data owner. In article 6, paragraph 1 defines sexual life and genetic data as special categories of personal data and gives some privileges to them. Paragraph 2 states the necessity of explicit consent, but in paragraph 3, exceptions are listed that allow processing data categorized as special without explicit consent.

NH also pointed out that the PDP law gives this right to the Ministry of Health as well:

*NH: "... Within the same law, the Ministry of Health is also assigned the task related to the collection of this data for certain purposes, like protecting public health etc."*

According to NH's claim, this part is added to the PDP law in order to legalize data collection by the e-Nabız system. The passage mentioned is article 47, which is amended by the PDP law from the Decree Law No. 663 dated Oct. 11, 2011 on the Organization and Duties of the Ministry of Health and its Affiliates:

*ARTICLE 47- (1) those who present to public or private health institutions and health professions in order to obtain health services, and the personal data they gave as a requirement to receive health service or personal data related to the services given to them can be processed.*

(2) In order to provide health services, to protect public health, for preventive medicine, to carry out medical diagnosis, treatment and care services and to plan health services and to calculate costs, the Ministry of Health may process the data obtained under the first paragraph.

HT had analogous thoughts about the law. She mentioned the topic of explicit consent in the law as one of the most problematic part:

*HT: "... it is stated in the item (Transitional Provisions, Temporary Item 1) that unless the data owner declared the opposite within one year, it is accepted that consent is given. It is not realistic for the data owner to remember whether she/he gave consent and when or where she/he gave it."*

The item of the law she mentioned is a sentence written in the third paragraph of Transitional Provisions, Temporary Item 1:

TRANSITIONAL PROVISIONS TEMPORARY ITEM 1 - (3) ... Consent in accordance with the law received before the date of publication of the PDP law is accepted as given unless a declaration of the opposite intent is made within a year.

Exceptions and various other parts of the law were criticized by the participants, even though the law was prepared based upon the directive of the European Union with high sensitivity to data confidentiality. However, the translation is a controversial topic, as well.

*Is the law a one-to-one translation of the EU Directive?*

Many negative opinions and criticisms about the law were expressed. Actually, the law is based on EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of data, which has been in effect since 1995. The lawyer referred to this situation in the second meeting and claimed that the law is almost a one-to-one translation of the directive.

*BF: "... It is almost a one-to-one translation of the European Union directive numbered 95/46. There are even thirty items in both of them. ..."*

*Particularly, personal data is organized in the 8<sup>th</sup> article. In its 3<sup>rd</sup> paragraph, exceptions to the special categories of data to be processed without explicit consent are given, namely the protection of public health, the purpose of preventive medicine, medical diagnosis, etc., almost a one-to-one translation ..."*

The items mentioned here are listed in section 3 of EU Directive 95/46/EC, under the rubric special categories of processing (see Article 8):

ARTICLE 8 – (1) Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

...

(3) Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject to the obligation of professional secrecy under national law or rules established by national competent bodies or by any other person also subject to an equivalent obligation of secrecy.

Paragraph 1 is quite similar to Article 6 (1), except that in the PDP law appearance-dressing, criminal convictions, and security measures, biometrics and genetics are added to the list of special categories of personal data. Some parts of paragraph 3 were updated as well when the PDP law was prepared. The Directive allows exceptions for all the data listed in the first paragraph; however, in the PDP law, health and sexual life data are separated from the list and different exceptions are defined for them. Health and sexual life data can only be processed without obtaining the explicit consent of the data subject for purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment, and care services, planning and management of health services, and financing by people under the obligation of secrecy or authorized institutions and organizations. The rest of the data, which is relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dressing, membership of association, foundation or trade-union, criminal conviction and security measures, and biometrics and genetics are special categories of personal data that can be processed if permitted by a law.

The lawyer's remarks do not completely reflect the truth about the issue of one-to-one translation. Besides, she added a reflection about the risk of implementation differences in Turkey:

*BF: "... Even if our law is the same as that of the European Union, the issue that needs to be discussed here about our law is the differences that may occur in its implementation."*

"The way of implementation" of the law and trust in the government were discussed for various subjects throughout the meetings. The Personal Data Protection Board (PDPB) is another subject raising these issues.

*"There is no autonomy, independence or diversity on the board"*

The election of nine members of the Personal Data Protection Board (PDPB) was completed on January 5, 2017 ("Kişisel verileri koruma kurumu başkanlığı," 2017). According to the latest regulation, the chairman and one other member of the board were elected by the President, two members by the Turkish Grand National Assembly, two from the two opposition parties in the parliament (CHP and HDP), and the remaining three from the ruling Justice and Development Party (AKP).

The way of appointing the PDPB was also criticized by the participants, as there were no autonomy, independence, or diversity. They claimed that the majority of the board was elected under the control of the ruling party; hence the board cannot be autonomous or independent. The diversity of the members was seen as another problem. According to

the views of the participants, the law does not provide any diversity when determining the background of the members.

*ZB: "There is no diversity, one of the members may be an engineer and the other may be a lawyer."*

*NH: "Of course, one may be a faculty member or a lawyer... Both the quality of the elected and the electoral procedure are problematic... How do we manage our autonomy and how to maintain a healthy independence?"*

*FB: "... There was a meeting a few weeks ago about this law and there was not a single technology-related person involved in the board as far as I know. In general, [they were all] political people... The board will be trust-based. There won't be any technological thing in it."*

According to article 21, background prerequisites for being board members are only having graduated after at least four years' study at undergraduate level and to have worked for at least ten years in public institutions and organizations, in international organizations, non-governmental organizations, or public institutions or professional organizations.

The participants presented reasons for their distrust and their thoughts on "the implementation way of the law" to the ministry.

#### *Unlawful acts done by the Ministry of Health*

The NGO lawyers mentioned that the Ministry of Health does not obey the court decision, citing the case of e-Nabız as an example ("e-Nabız Projesinin yürütmesi durduruldu," 2016). The NGO lawyers stated that even though the court stopped the implementation of the application, it is still active.

*NH: "When we look at health and safety, a very critical issue emerges. We say that it should never be done before the legal infrastructure is established. ... After NGOs won the cases, they [e-Nabız, SağlıkNet2, etc.] were all stopped by the court but actually continued. They never stopped completely."*

They mentioned the importance of the establishment of a legal infrastructure; however, the unlawful acts were not stopped after the passing of the law, either. The regulation of the protection of personal health information (numbered 29863) was published by the Ministry of Health, and with the circular numbered 2016-6 about e-Nabız (Genelge 2016/6 2016), the Ministry of Health started to collect health data again. The lawyers mentioned two main problems of the regulation for the protection of personal health information, too. The first problem regards limitations of data collection. According to claims made by the NGO lawyers, with this regulation every type of data can be collected and processed by government agencies.

*NH: "...There is no criterion of restricting by purpose, so the new regulation does not say that I want the following data for the following purposes. It says that when someone*

*comes to you, you have to send me all of the data you have obtained from him. This includes the story I told about my girlfriend, as well as my home address.”*

The second problem is data collection without waiting for establishment of the personal data protection board:

*NH: “... the law stated that you can collect data only if you take the safety precautions prescribed by the personal data protection board (Article 47- Paragraph 4). However, according to the regulation, the Ministry of Health would like to collect the data while the board has not yet been established.”*

The article mentioned here is article 47(4):

ARTICLE 47- (4) Standards relating to the safety and reliability of systems will be determined by the Ministry, in accordance with the principles determined by the Personal Data Protection Board. The Ministry shall take the necessary measures to ensure the safety of personal health data obtained pursuant to this Law. For this purpose, it establishes a security system that allows controlling for what purpose the registered information is used by which officer.

As NGO lawyers stated, the article mentioned the principles determined by the PDPB. The election of PDPB members (“Kişisel verileri koruma kurumu başkanlığı,” 2017) was completed on January 5, 2017, about two and a half months later than the regulation of the protection of personal health information had been published (October 20, 2016).

The lawyer accepted the existence of the problems in the regulations and indicated that the changes will be done soon.

*BF: “Changes in the regulation will be made in the near future; in fact, we have seen problems in the implementation as soon as the regulations went into effect, but we were waiting for the opinion of this board to make changes. ...”*

The changes were made in the regulation from November 24, 2017, which is almost five months later than BF stated (“Kişisel sağlık verilerinin işlenmesi ve mahremiyetinin sağlanması hakkında yönetmelikte değişiklik yapılmasına dair yönetmelik”, 2017). In the modified regulation, many of the contradictory paragraphs are updated or removed from the regulation. Article 7 was one of the modified ones, and its most contradictory paragraphs 1 and 2 were modified as well.

*ARTICLE 7 - (1) Personal health data; for the purpose of public health protection, preventive medicine, medical diagnosis, treatment and maintenance services, planning and management of health services and financing, can be processed by authorized institutions and organizations under the obligation to keep secrets without the explicit consent of the subjects.*

*(2) In order for personal health data to be processed non-anonymously, except for the purposes listed in the first paragraph, the relevant person must be informed in detail regarding the reason for the disposal, the written consent of the person must be taken, and the consent must be stored.*

*MODIFIED ARTICLE 7 - (1) No explicit consent of the person is sought, in order for the personal health data to be processed under the exceptional purposes and conditions set out in the third paragraph of Article 6 of the Law.*

*(2) In order to process personal health data within the scope of these purposes, the person must be informed, and consent must be taken in accordance with the information provided for in Article 10 of the Law.*

#### *4.5.2. Management of Genetic Information in Electronic Health Records*

Regulations and management of genetic data were the main topics at both meetings. Especially in the second meeting, handling genetic data was the main subject. The reasons that make genetic data different from other types of data are their unique features. Our participants addressed the issue that genetic data cannot be anonymized, it is related with the family rather than the gene owner alone, and it has the potential to generate more data about the owner in the near future. These special features of genetic data were discussed along with new legal developments. The participants generally criticized the current situation in Turkey, gave examples from all over the world, and had some disagreements during the meeting about usage of genetic information in the insurance sector.

##### *Anonymization does not work for genetic data*

In the PDP law, genetic data is only listed under the special categories of personal data, but there is no article particularly dedicated to genetic data in the law. However, FB, who has several academic publications and research on privacy and security of genetic data, thought that standard anonymization techniques will not be enough to protect the privacy for genetic information.

*FB: "...in order to anonymize data, you should extract the personal identifier from it, but genetic data is a personal identifier itself. It is ridiculous to try to anonymize it since you cannot do it; just as you cannot anonymize your name."*

ZB, an academic in the field of bioinformatics, also mentioned the same problem and added that only pseudonymization techniques can be used for genetic data.

*ZB: "... genomic data cannot be anonymized; that is a generally accepted knowledge. It can only be pseudonymous."*

There are many sources in the literature that support FB's and ZB's opinions (Gymrek, McGuire, Golan, Halperin, & Erlich, 2013; Malin, 2005; Sweeney, Abu, & Winn, 2013); thus we can say that it is generally accepted in the literature that genetic data is a personal identifier and cannot be anonymized.

The lawyer BF expressed thoughts similar to the academics' and added that while the law was prepared, they, as the Ministry of Health, presented their opinion that the law must include pseudonymization for genetic data.

*BF: "When the law was under construction, we sent our opinions [as the Ministry of Health] that pseudonymization must be found in the law. ... Pseudonymization is*

*absolutely essential for conducting clinical studies of scientific preparations or studies on genetic data because it is not possible to create anonymity.”*

However, this technique is not mentioned in the law, although pseudonymization was newly added and highly recommended by the General Data Protection Regulation (GDPR) (European Commission, 2017).

The unique properties of genetic data mean that it is related with more than one person; hence, the privacy of the data of a patient’s family members should be considered while regulating the law.

*Individual consent may not be enough*

According to the participants, taking consent from the patient only is not enough since family members will be affected by the results.

*OB: “Why genetic data is different? Because genetic diseases are not just about that individual. When you identify a certain genetic variation in a person, you are starting to get some information related with the entire family.”*

*ZB: “Yes, this genomic data belongs to the person but also contains information about the person’s family, relatives, past, even future generations. If you define a person as a patient with a hereditary incurable disease, if you reveal this to society, that person and the whole family will be exposed to it. Discrimination can have very different effects at every level in society. And genomic knowledge is permanent knowledge, I have to emphasize that a lot. ... So, if you do something [with the genetic code], you should take consent from the person’s relatives as well.”*

The genetic data is permanent as we cannot change who we are. We also do not know what may happen in the near future because genetic research is still very new. It is very difficult to predict what else can be found in the genes, so the risk may be much greater than we imagine. Nevertheless, there is no law or regulation dedicated to genetic data in Turkey.

*ZB: “By thinking about where we will be in a few decades, and perhaps even twenty years on; we just need to evaluate what can be done with today's situation in the future, not what we do today! The genetic code may be our financial problem, it may become our credit score, we cannot know that now. Society does not know how to evaluate this data. Things can go beyond health.*

*... The risk of someone testing the family is my risk. What if I do not want to know what will happen then. ... We do not have any law or regulation currently [on genetic data handling].”*

These are the important and still controversial issues of genetic data in other countries, as well. However, the basic issue of separation of genetic data from health data was still being discussed in the meetings about the PDP law.

*An important question arises: How do we distinguish genetic data from health data?*

The lawyer indicated that even though there is no article dedicated to it, there is no exception made for genetic data either, so it can be said that genetic data is under protection by the law.

*BF: "... In the first paragraph of Article 6, apart from health data, biometric data and genetic data are counted separately. However, in the third paragraph, only sexual life and health-related data are mentioned as being exceptional. Therefore, it is obvious that genetic data cannot be processed [without consent] under 6/3."*

She also added that this is her interpretation; the final decision will be provided by the PDP Board.

*The NGO lawyers agreed with this view and added that according to the PDP law, genetic data cannot be processed without the consent of the subject. However, if genetic data is seen as health data, it is possible to process it.*

*NH: "... Now, it is possible for genetic data to be processed without any consent only if it is seen as health data. "*

Genetic and health data are much intertwined. Medical diagnostics center representative TD stated that she does not know how to distinguish the two data types from each other.

*TD: "It is important to understand what is called genetic data. So clinically I make the FMF diagnosis for a child. Does that health data become genetic data when I find the mutation? When will they be separated? Because apart from infectious diseases, 85% - 90% of the remaining diseases are genetics-based. The discussion is so complicated at that point, so we should define very well what is genetic data and what is not."*

Apparently, the Turkish Social Insurance Institution (SGK) does not define any differences between genetic and health data while they are asking information from clinics, either. A university medical genetics laboratory academic, MH, told that in practice SGK acting against the law.

*MH: "In practice, we are producing the report; we are sending the bill to the SGK. The SGK tells us, 'what did you do to this patient and send me 90 pages of the sanger sequence. Put your signature on the detailed report below, send them to me, then I will put them in the patient file and then I will pay you the money'. When it comes to this point, then encapsulation or something seems very utopian."*

TD also reported that three members of the Medical Genetics Association have been investigated since the PDP law was published because they refused to share genetic data with the SGK.

Genetic data can be as large as a whole genome or a single genetic test result. Furthermore, there are two types of consequences of genetic test results: they may either give a possibility or an exact diagnosis. Most of the times, test results give only possibilities, and it is a controversial topic if to share these possibilities even with patients. If these results were in an insurance company's hands, they could cause very serious and irreversible consequences.



### *Insurance problems*

As is known, insurance companies want to be informed about the health status of their customers. In Turkey, this information is received on the basis of personal statements rather than looking directly into the health records. Despite the intense debate in this regard (Klitzman, Appelbaum, & Chung, 2014), insurers desire to access all health information, including genetic data from all available channels. Although genetic information is not currently used, the insurance company representative, FL, said that genetic information will be very useful for statistical analysis of insurance risk.

*FL: "We are in a sector that has to know the health information of people in order to sustain our business. As an insurance company, we want to access health information from all the channels we can get. My personal opinion is that genetic information should be used in the insurance sector because this is a risk analysis. We will determine premiums accordingly. We are collecting premiums in a pool and spending for sick people."*

FB opposed this idea and cited the GINA law as an example:

*FB: "That's not very understandable. There is a law against this in the US called GINA law which says that genetic data cannot be used in the insurance industry... Discrimination cannot be done by using genetic data by insurers and employers."*

As FB stated, there are legal regulations on this subject in other parts of the world, such as GINA. Nevertheless, the participants indicated that there is a lack of legislation on this issue in Turkey.

*FB: "Is there a Turkish law against genetic discrimination?"*

*NH: "No, there are EU regulations but no regulation in Turkey."*

### *4.5.3. Government's Business Culture*

Participants criticized how the government does business. According to their opinions, the government's consultation and discussion culture is weak. The participants stated that even though they are the experts on the privacy and security of personal health data, they have not been consulted while the government was conducting large scale health IT projects or preparing new regulations.

*HT: "While preparing this important, 35-year-old law, you should have been asked as an expert (pointed to the participants), I should have been asked, at least someone should..."*

*Temporary workers and contractors are one of the potential sources for privacy leaks in the system*

Temporary workers and contractors are seen as important risk factors for privacy leaks. The participants thought that officers should be assigned from among ministerial staff.

*HT: "... When a software vendor installs software, sending unauthorized employees when installing it, this disturbs me. The government does not monitor what the*

*unauthorized agent is doing, and no precautions are taken against copying the retrieved data.”*

*UU: “... Is this data protected enough? No. Because they have a serious problem with the background of personnel. You will see when you are searching on the internet now, consultant job offers for 55-60 people have been published recently. Therefore, it is outsourced continuously. These people are not ministerial staff; they are from private companies and other companies. Hence, I am saying this for those who do not know, any information specialist who is responsible for that database can access this data very easily, including identity, relationship, gene map, medical histories, etc.. It’s that simple.”*

#### *Audit of private companies on data privacy: Is it enough?*

Participants saw private companies as another problem for privacy of information. HV, as mentioned previously, is a co-founder of an activity tracker, and he thinks that companies in the sector leave security behind because of the financial burden.

*HV: “The security of devices, especially in the field of wearable technology, is a matter of serious competition and prices are starting to go down drastically. New products must be marketed very quickly. In order to be able to do this, they have to be able to reduce prices in some way, and some companies are giving up a bit on security to achieve this.”*

He also stated that companies which are working with personal data are inclined to sell the data, especially when they go bankrupt.

*HV: “Yes, you trust the company today but when the company goes down, those things are in the cloud. When RadioShack went bankrupt, they tried to sell collective data saying that we would not share it.”*

In 2015, RadioShack was bankrupt, and the company auctioned off 17 million customer data sets includes names, phone numbers, addresses, e-mail addresses, and in some cases purchase history (Isidore, 2015).

There is also a commercial risk of unauthorized information sharing as HV indicated:

*HV: “From the point of view of the end user, this may be a disadvantage, of course, as producers like us can share this data with third parties. Especially when it is shared with insurance companies, even if you do not give permission to share, your health insurance premiums may increase. Or we have the knowledge of your eating habits and when we sell it to an online food order company, you may receive various e-mails directly parallel to your eating habits.”*

Another lawyer from an NGO, PF, informed the participants about the latest decision of the Standing Committee of European Doctors (CPME) on wearable devices:

*PF: “Last year, the Standing Committee for European Doctors took these wearable technologies etc. as a topic and decided that we should create an ethical code for what the role of the physician should be. We should deal with the matter of what is and what*

*should be the doctor's role in these technology processes because there is a manipulation and commercialization of a patient privacy issue here."*

#### 4.5.4. Public Perception of Risks, Government Failure, Mishandling of Data

*The government is acting imperviously about data privacy*

NGO lawyers blame the government to be impervious to public health and security issues. They also claimed that the government is not acting under the maxim "Citizen first" in Turkey. According to them, it is an ethical problem and a great health risk to collect all kinds of personal health data including sensitive ones.

*NH: "The government is making an effort to collect all the data without leaving anything out. In the end, it may result in a situation where people may avoid going to the hospital because their data may be disclosed. In other words, avoidance of treatment may occur because it would be recorded. This is a very important violation of the patient's right. ... Here is not a system to prioritize treatment but a whole system has been established to identify what happened to whom. ... We know this part very well that this hurts the trust between the patient and the doctor. Because the patient and the doctor will pull a curtain in order to stay alone. But now the patients will know that someone is looking from behind the curtain. It does not matter if this someone is the government."*

The participants claimed that the government ignores the importance of data privacy. They mentioned the attitudes of government authorities in two incidents as examples for this claim: An illegal sale of health data by the Social Security Institution (SGK) in 2012 ("SGK plan to sell health data to global pharma creates controversy", 2012; Kaya, 2018) and a leak of personal details from 50 million Turkish citizens in April 2016 (Tait, 2016). According to what is known about data sale, a private company, called DataMed, bought the health records that were recorded in the SGK system ("SGK plan to sell health data to global pharma creates controversy", 2012). DataMed will also have the right to sell these records to national and international pharmaceutical companies in Turkey (ibid.). SGK officials argued that workers in the institution are selling these data illegally anyway. They also argued that the sale of medical data should be legitimate (ibid.).

*NH: "When we asked the SGK about why they sold the records, they said that officers were already doing it, everybody can obtain them informally, so we would close our deficit spending by this sale at least. Now, in a Turkey where work is done like this, we should think about this system more carefully. If the data collected in a hospital is disclosed, only the data of that hospital becomes the issue. Now, if this is stolen, 80 million data sets from calligraphy to genetics to physiology will be disclosed. When they are stolen, we have no way of turning the situation back, since I cannot change who I am."*

The Communications Minister of the time, Binali Yıldırım, spoke to the media about the data breach news and said that "[t]his is a very old story. A similar allegation was made in 2010. That kind of reports is brought to the agenda on social media from time to time.

These outdated reports are not newsworthy.” (“Communication Minister denies massive data leak”, 2016)

*HT: “According to my assessment, this country cannot understand the meaning of the data in its hands. The minister of communications said the data leaked was old and that’s all. I expect to hear something like that, even though they are old data, we are starting to investigate immediately, and we will understand where they came from. He should have said something like that, but he didn’t say this. It’s a very scary thing.”*

HT also claimed that this breach can be decrypted, and family trees can be generated easily, so the situation is more serious than what the government thinks.

*HT: “That means that you can reach family names; if you make such an effort, family trees can be created. Because the data is encrypted with bit shifting. Bit shifting means that, while identifying these Mernis records in 2000, the first time you give a number to you while giving your ID, family numbers, you know the father at the top, mother, kids. I will give examples with numbers. When it is 100 the father, last digit increased by 1 and the second digit is increased by 3 for the rest. So, 100 is going to go to 131 then 162. It’s the issue that you can create family trees with these numbers.”*

“All data can be de-anonymized”

On the other hand, FB claimed that all data can be identified, so in order to provide data security, he suggested a system that gives only the person who needs to see the data access authority.

*FB: “In security, it is said that depending on how much background information the attacker has, he/she can de-anonymize every dataset theoretically.”*

*“... In our work, our main goal is how to store this data so that even the government cannot see it, no one can see it. Europe is now trying to get new legislation called GDPR and they are trying to put a little bit more on this old data protection directive and tighten it a little bit further. What they are trying to do is data minimization. The data should be seen by as few people as possible, it should be seen only by the person who needs to see it. There is no need for showing this data to everyone in the government.”*

Other participants presented their suggestions in addition to their criticisms. They mentioned the need for discussing issues among stakeholders, preparing a national health data dictionary by taking America and Europe as examples, and preparing a tender specification with data privacy-security experts.

*HT: “In terms of how to be protected, it is necessary to form a common mind and to discuss it more.”*

*“... There are some things happening in the European Union, America. There’s a guideline too, it is not too far. On top of that, we can build our own practice. That’s all I have to say.”*

*PF: "Could we prepare a tender specification by translating the national health data dictionary and bringing together the people who know the technical part and the things which should be in the legislation?"*

UU suggested improving security features by using biometric data which will be stored in smart identity cards:

*UU: "Because in the coming days our life will get a new identity card. I have worked with a private company on this part of the project. Three biometric features will be collected: fingerprint, palm print, and print of blood vessels under the skin. ... Therefore, the verifications can be done in a more appropriate way with this biometric data rather than with the SMS verification mechanism, etc."*

#### **4.5. Summary and Conclusion of the Results**

In this chapter, the results of four sub studies are presented. The first study is the mPHR analysis. English and Turkish keywords were used to search in Google Play and inApp Store markets in order to answer the questions: What features are the currently available applications using? What kind of information are they recording? Do they have any area to record genetics-related data? Twenty applications (one in Turkish) were evaluated by predefined criteria as determined by Kharrazi et al. (2012).

Secondly, a questionnaire was developed with the help of the results of this analysis and administered to the public. Half of the participants were familiar with genetic tests, either done for himself/herself or for a family member. The questionnaire contained questions related to privacy and security of health and genetic records. Security protections used in online banking were explained to the participants in order to understand whether these high-level protection measures helped the participants to feel more secure about the privacy of their genetic and health data. The results of the survey revealed that people had negative experiences and prejudices; hence, they had concerns about the privacy and security of their health and genetic data. They would like to see security measurements and regulations to protect their privacy before starting to use any application to keep track of their health/genetic data. They would also like to have sole control over these applications.

Thirdly, with the participatory design method, the appearance and the content of the application were discussed with five participants chosen from among health application designers and potential users. As a result of 11 meetings, a sample paper prototype was prepared for a genetic data-enabled PHR application as a concrete product of the dissertation. The prototype is presented as an example of the possible solutions. It demonstrates a sample of an mPHR including genetic data with the necessary pages and subpages. Even some suggestions for security protection were discussed in the meetings.

The last substudy consisted of two focus group meetings on the requirements for the compatibility of a health record system including genetic data with the current health system and data privacy laws. Eighteen participants came together to discuss this topic for the first time, and the report created by their contributions is an entirely novel and

valuable contribution to the literature on the ethics of medical informatics. In this way, two main questions were answered: what are the requirements for developing a legal compliance system and what are the problems of the current situation? As a result, the meetings proved the importance of legal compliance for the applications. Moreover, experts supported the idea that genetic data is of special importance compared to other types of data.

## CHAPTER 5

### DISCUSSION

In this chapter, discussions of the study are presented under four subheadings: mPHR analysis, the survey, PD workgroup, and focus group meetings.

#### 5.1. mPHR Analysis

According to the results of our mPHR analysis, we chose 19 finalist applications. Although this number is the same as in the guidance paper (Kharrazi et al., 2012), in contrast to our study, Kharrazi et al. included paid applications into their research, though in their results, there were 9 free applications as well.

There is a column in Table 7 and Table 8 called “Average data elements covered by each mPHR” that shows an average of 10 data elements; *Problems/conditions, Procedures, Medications, Providers, Allergies, Lab Results, Immunizations, Family history, Emergency contact, and Insurance*. The highest coverage was 80% and the lowest one 10%. In the reference paper (Kharrazi et al., 2012), the four applications that covered all these ten data elements were paid applications. E-Nabiz was added to the results later; it has a 70% coverage of the data elements and three out of four features.

The results identified the most common data elements found in the markets (*Problems/conditions, Medications, Providers, Allergies, Lab Results and Immunizations*) and the features used in these applications; thus, we could use them as a starting point for the next analysis. A more recent study by Roehrs et al. (2017) that aimed to explore the recent literature related to PHRs listed the most common data types in PHRs as “allergies, immunizations, laboratory results, medications, scheduling”. Except for scheduling, the results are similar to ours.

Moreover, the analysis showed that apart from one application, every application in the markets had at least one security protection feature. According to the result of an earlier study on PHR safety (Señor et al., 2012), this number is 15 (out of 24 PHRs). However, except for e-Nabiz, the applications did not use many of the advanced security features.

Even though e-Nabiz has many good features and high security measures, there are some fundamental problems. E-Nabiz uses an opt-out-based participation system, so the users are automatically included in the system without being asked to consent. Unless they close their accounts, they remain in the system. Moreover, even after they closed

their e-Nabız accounts, the system continues to keep a large amount information except for the history of blood pressure, step, sensor data, etc. (“E-nabız,” 2015).

This is in contradiction with the EU General Data Protection Regulation (GDPR), which states that explicit consent is necessary for organizations that want to legitimate the use of special category (sensitive) data. Health information, Biometric data and Genetic data are included in the definition of sensitive data in GDPR as well (“General Data Protection Regulation ”, 2017). The explicit consent should also be a “freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”. These rules are ignored by the e-Nabız system as it is opt-out based. The rights of the patient to receive his or her own knowledge and the right to hide or to delete data are blocked by the system.

The scope of this mPHR analysis was limited to the data elements and features in the mobile markets. With the help of the results, we could define the basics of an mPHR application that were then used as a starting point for the further analysis as is mentioned in the following chapters. However, the study also indicated the importance of laws and regulations for the processing of such sensitive data (health and genetic) and a need for their critical evaluation.

## **5.2. The Survey**

Our results showed the respondents’ sensitivity about sharing health/genetic data with third parties. They wanted to see regulations and security measures for the protection of their data. The participants chose to trust only their doctors regarding the privacy of their health and genetic data. On the other hand, they chose to limit even their doctors’ access to their genetic/health records. Although most participants did not oppose keeping their health and genetic data in a mobile data management application, significantly more participants thought that their genetic data was at a higher security risk in such applications. We also found that privacy concerns were greater among the young, female, and higher educated respondents.

We also asked the participants several questions to understand their concerns about the current health record system. Three questions (Q17-Q19) relating to the participants’ experience had been used in a previous survey conducted in 2011 in Turkey (Özkan, 2011). Although that survey had a higher number of participants (596), the participant profile was very similar in terms of age (average: 28.6) and educational level (university or above: 87.3%). There was a noticeable difference between the two surveys in the percentages of ‘yes’ responses to the three questions listed (the results of the current survey are given in parenthesis): 0.8% (9.7%) reported that either their or one of their family member’s medical records had been inappropriately used or released without their consent, 12.5% (15.1%) avoided being tested in case someone might see their results, and 1.5% (3.5%) asked their doctors to include a less embarrassing alternative in their medical records rather than their actual condition. We find these results alarming since they support the idea that patients are inclined to postpone or give up treatment or



change the circumstances in which their illness occurred or withhold certain details because they have concerns about confidentiality. An urgent action plan is needed to establish greater public confidence about the confidentiality and privacy of health, genetic, and other records.

Another important finding of the survey was the observation that only a small number of participants had comprehensive knowledge regarding the rights of access to their health records. Unfortunately, the remaining participants either had no relevant knowledge at all or were in doubt about the issue. When asked about their preferences for access rights, most believed that they should be the only people with full access to their medical and genetic data. These results indicate that people would like to have exclusive control over the use of their data and favor a self-controlled rather than a centralized, multi-user system. An exploratory survey conducted in Saudi Arabia (Alahmad et al., 2016) contained similar questions about access rights. Although there was no limited access option in the Saudi questionnaire, the results were parallel to ours. The Saudi participants preferred to give their doctors and themselves access to their medical data while they were refusing to do the same for insurance companies. The health systems, policies, and regulatory frameworks of both countries should be discussed to see the reasons behind the similarity of the results obtained from these two countries.

Most of the participants in this study (79.8%) also wanted to have the option to see when and by whom their records were retrieved. Similarly, Atienza et al. (2015) reported that the participants' concerns about privacy and security of mobile health data were connected with uncertainty about when and by whom the information was accessed and seen. Our overall results suggest that the system should allow tracking access and ask for the patient's permission prior to releasing or distributing their medical data or sharing anonymous information that does not contain any personal details. Furthermore, an effective health information system should allow the user to hide sensitive information from users that are not authorized by the data owner.

According to the results, significantly more husbands preferred to give their wives full access to their genetic and medical data. This may have several reasons. Some related studies have shown that women are less willing to participate in genetic studies or allow storage of their genetic data than men (Espeland et al., 2006; Matsui, Kita, & Ueshima, 2005). One reason may be the privacy concerns of women regarding genetic tests. However, the results are not consistent (Khan, Capps, Sum, Kuswanto, & Sim, 2014): while some of the studies could not find any relation (Mezuk, Eaton, & Zandi, 2008), another one reported men's higher concern levels (Green et al., 2006).

Another reason behind women being less willing to share their medical data could be that they have more information in their medical records than men since they are admitted to healthcare facilities more often (Ashley, 2010; Brett & Burt, 2001; Goldstein, 2010). Excluding prenatal examinations, statistically more women visit hospitals for psychiatric and chronic diseases (Ashley, 2010; Bates, 2011; Goldstein, 2010). Thus, one justification for our observation could be men having a lower level of concern about their health or health records since they experience fewer medical conditions. Lastly, there can be cultural or country-specific reasons for the differences of

view between genders. In many countries, women still cannot express themselves freely since they are under the pressure of men and society in the majority of areas from business and economy to family (Kandiyoti, 1977, 1988). The discrimination between men and women may result in the latter feeling less comfortable sharing their private information with their spouses.

The literature contains parallel results on the association of younger age and greater privacy concerns about genetic/genomic data (Khan A et al., 2014). According to Oliver et al., (2012), the reason behind this could be older people's beliefs that their remaining lifetime might not be long enough to experience any negative results of DNA data leaks or disclosures. Despite being an unusual explanation, this may also be the underlying reason for our results.

The situation was similar for educational level. University degree holders tended to have more concerns (McGuire et al., 2011). Our study also showed that different groups had varying perceptions and views which should be taken into consideration when designing genetic-health data systems. As Aro et al. (1997) also suggested, "age, education and gender related differences in acceptance of genetic testing [...] need to be taken into account when considering screening programs and informing the public".

Our findings showed that the level of trust in terms of ensuring the confidentiality of genetic and medical data ranged from most to least trusted as follows; doctors, pharmacists, nurses and other hospital staff, the government, information technology specialists, and finally insurance companies. In general, the participants tended to trust people who were directly involved in their treatment more than the government, insurance companies, or information technology staff. Moreover, the results showed that people trusted only their doctor with their health and genetic data, which is promising as no quality healthcare service can be provided when there is no trust in the provider. The analysis of the same question showed that information technology specialists are one of the least trusted groups in the eyes of the participants. However, health information technology professionals have a key role in protecting the security of genetic data and minimizing breach risks when designing related systems (Shoenbill et al., 2014). Very recently, many significant steps have been taken in personal data privacy legislation in Turkey. The first Turkish Personal Data Protection Law (numbered 6693) was published on March 24, 2016 ("Kişisel verilerin korunması kanunu," 2016), which introduces new sanctions and punishments for those who do not protect the privacy of data. This may still not be enough to reduce people's concerns on this issue; however, considering that the law is relatively new, the actual outcomes will only be observed over time.

Nearly half of the participants or at least one of their family members had been genetically tested before the study, and the majority of the remaining participants stated that they would take a genetic test if necessary. This result is valuable since the questions about sharing, storing, and protecting genetic information provided an insight into the participants' views based on their actual experience in addition to a hypothetical scenario. The responses also revealed that the participants had a different attitude towards their genetic information compared to other medical information, with more people finding it risky to store their genetic information in mobile applications. Even

though the number of “not sure” responses is quite noticeable (14%), this can be a reflection of a low level of knowledge about genetic science. As in other types of health-related data, the participants were also not very willing to keep information about inherited diseases in an application. In contrast, Alahmad et al. (2016) found no significant difference in giving access to medical or genetic records. Our participants compared the value of genetic information to their identity and personal information, such as address and phone numbers. Many people also stated that a mobile health record application should have similar security protections such as OTP and mobile signature to keep their health and genetic information secure. This indicates that a mobile health record application with sufficient security protections has a potential for adoption by mobile users. Otherwise, as discussed by Heath et al. (2016), “privacy concerns will have a negative influence on behavioral intentions to share genetic information”.

In conclusion, the results of our study show that people would like to have a system that will give them full control over their health and genetic data and makes them feel safe and secure about sharing, hiding or even deleting their information. The system should also be flexible in terms of being adaptable to user preferences. All of these requests are pointing to a personal, self-controlled health application. A well-designed, patient-oriented, and secure mobile personal health record application has a potential to be adopted and used for health and genetic data management.

### **5.3. PD Workgroup**

The MPHR analysis study showed which features are currently used in the application markets. Problems & Conditions/Medical history, Medications, Providers/Doctors, Allergies, Lab results and Immunizations/Vaccines were used by at least half of the mPHR applications. The results of the survey revealed that Inherited disease/Genetic illnesses/Family history, In case of emergency (ICE) number, Surgeries/Procedures and X-rays/Images should be added to this list since they were selected by more than half of the participants. However, another set of data elements was defined by the participatory design meetings: Terms and data policy, Main Page, Login and Sign up Pages, Profile Page, Calendar, Emergency Social Page, Preventive Medicine Pages were all designed in the meetings. During the discussions and while working to prepare a sample prototype, the group realized these details which had not been thought of before. Figure 10 gives a summary of the distribution of these features in mPHRs.

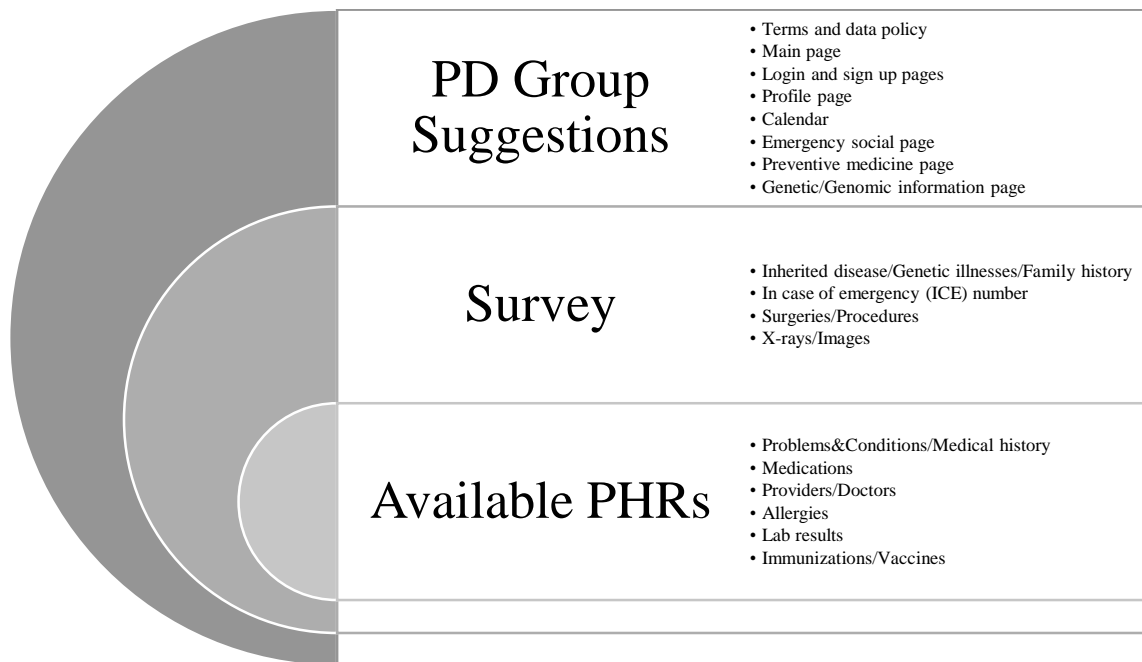


Figure 10 Summary of the data elements determined in PD Group, Survey, and mPHR analysis

Genetic/Genomic information and Preventive medicine pages had helped to expand the literature as new PHR features. Roehrs et al. (2017) stated the emergence of the same data types in PHRs: “new data types have emerged, including genetic information, medical advice (recommendations), and prevention concerning the patient’s health, as well as data types with recommendations for prevention...”. These data types are pointing Genomic Information and Preventive medicine pages proposed by the PD group members. Even though three finalist applications had a Family history feature in the mPHR analysis study, none of them has a special design for genetic data records or a pedigree tool to track family diseases. The Preventive medicine page was not one of the features of the mPHR analysis study; it emerged as a result of the PD group discussions. With the guidance of the doctor participant (P3), the necessity and importance of the page was understood. With the help of the Preventive medicine page, necessary alerts for routine controls and required vaccines and tests would be presented specifically tailored to the health history of the person.

Working on the application from scratch helped us to see every detail of the application and to understand how important these are. Which user name should be used? How many questions are needed for a user profile? What does a doctor want to see in such an application? In which way should a reminder or medicine or disease or genetic illness be recorded in the system? ... etc. The group did brainstorming for each question and came up with various ideas for solutions. In addition, with the help of the participatory design method, these solutions were owned by both the users (chronically ill patients, a genetics lab worker and a doctor) and the system designers (mobile health application developers).

The basic design rules, features, and security protections were defined in the meetings while some parts were created entirely from scratch. The National Committee on Vital and Health Statistics (2006) offers terms and conditions of use, controls to see who has access to a person's records, and industry-standard security and privacy schemes with the ability to change the accessibility of one's records for PHR security. These recommendations were covered in the PD meetings. An up-to-date terms and condition page and the use of at least one security measure was proposed; the ability to see last logins and the ability to share data with the doctor or other professional groups were discussed.

#### **5.4. Focus Group Meetings**

Recently, more and more people have been concerned about the privacy of their information (Madden & Rainie, 2015). Nevertheless, many experts think that in the future, with the help of technical and regulatory changes, the problem of public concern about security and privacy can be overcome (Rainie & Anderson, 2017). Surprisingly, the participants' opinions about new legal actions in Turkey were quite contrary to this view. Some of the participants even said that the situation had become still worse after the law. None of the participants in either meeting was opposed to data collection; however, they did not support the current way, either. They had many critiques due to an absence of legality, while they were also dissatisfied about the current law and regulations.

The participants claimed that the system in Turkey aims to collect data in one center (such as e-Nabız) and the PDP law was designed to support this aim. According to their views, this is not acceptable since it is not in accordance with human rights and it is detrimental to data privacy mainly because of the huge data leak risks. Diamond, Mostashari and Shirky (2009) present a parallel analysis to this view, stating that results of data leaks are dangerous when collecting large-scale data. They also added that mostly because of data owners' privacy concerns the success of large-scale data collection in the public sector is very rare. The source of this failure may be either overpayments due to legal obligations (Diamond et al., 2009) or being stopped by the courts for infringing legal obligations, as in Turkey. In the near history of Turkey, two big and very expensive public health IT projects were suspended as they did not obey personal data privacy laws: SağlıkNet2 and e-Nabız ("Danıştay: Kişisel verileri toplamak hukuka aykırı," 2014; "e-Nabız Projesinin yürütmesi durduruldu," 2016). Besides the breach risks, there is a lack of trust in the government about selling personal data on purpose, after a government institute, SGK, has received a bad reputation about this issue in the past ("SGK plan to sell health data to global pharma creates controversy," 2012). Breach risks exist for many projects in some ways; however, trust is something which can be improved by regulation through strong laws, especially for privacy issues. The government needs to take constructive steps such as increasing the penalties for data abuse, giving the subject all rights over his/her data, etc.

Some articles of the new law were found to be dangerous for personal privacy. The EU was given as a good example many times. Even though the Turkish PDP law was written based on EU Directive number 95/46/EC, it is not an exact translation. Recently, in the Turkey report of the EU Commission, the PDP law was also criticized, and it was stated that “it is not yet in line with European standards” (EU Turkey 2018 Report, 2018, p. 42). Moreover, the Data Protection Directive 95/46/EC was replaced with the EU General Data Protection Regulation (GDPR) on May 25, 2018. The regulatory policies of the new directive have been changed significantly (“Key Changes with the General Data Protection Regulation,” 2017). To update the law according to GDPR may become a solution for some of the critics of the PDP law.

Data collection and processing without consent, especially with the exceptions made for sexual life data, are the most criticized part of the PDP law. Contrary to the situation in Turkey, the GDPR strengthens the issue of explicit consent. Moreover, the sentence “It must be as easy to withdraw consent as it is to give it” is added to the GDPR (ibid.). However, Transitional Provisions Temporary Item 1 makes giving and withdrawing consent even more complicated.

The article that defines the PDPB is one of the most criticized ones since the board has no diversity and independence. Actually, having such a board is not a necessity for data protection laws; there are other countries that have no data protection board, e.g. Germany. Nevertheless, there are other examples for the preference to have a board like in Turkey. There are national data protection authorities with different names, such as the Data Protection Authority in Norway, Federal Data Protection and Information Commissioner in Switzerland, Commission for the Protection of Privacy in Belgium, Information Commissioner’s Office in UK, etc. Finland has a board with the same name, Personal Data Protection Board, as an independent decision-making agency in personal data matters (“Data Protection Ombudsman,” 2014). It has also implemented the EU Data Protection Directive 95/46/EC as the Personal Data Act 523/1999 since June 1999. The board is appointed by the Council of State every three years and consists of a chair, deputy chair and five members, who are required to be familiar with register operations (“Data Protection Ombudsman,” 2014). There is also the Data Protection Ombudsman who is an independent authority operating in connection with the Ministry of Justice. To sum up, the way of selection of board members and the government agency that it is affiliated with are different than Turkey’s. In Turkey, five members of the Board are selected by the Turkish Grand National Assembly, two members by the President, and two members by the Council of Ministers, and the rest is chosen according to the parliamentary representation of the political parties. Therefore, in the current situation, on Turkish board only two of the nine board members were chosen by the opposition parties of the parliament. However, the board has not given any decision yet, so it is too early to talk about its independence.

The members of the board were chosen from the areas of law, electrical engineering, provincial population and citizenship, theology, public administration, medicine, and journalism. Even though there is no female representation in the group, it can be said that there is diversity regarding the background; however, the relevance of the board

members' training for data privacy is still debatable. The attitudes of the board towards controversial issues will provide more reliable ideas in this regard.

As previously stated, the regulation of the protection of personal health information was revised after a discussion in which the lawyer (BF) pointed out the regulation's mistakes and counterproductive aspects with the law. Since the changes have occurred after the meeting, it was not possible to explore the focus group members' ideas about these changes. However, the NGOs have not yet filed suits against these changes.

When it comes to genetic data, in general, the discussants complained that the government does not give the necessary attention to it under legal aspects. Many features specific to genetic data should be thought about before any action is taken. For instance, since genetic data cannot be anonymized, the use of a pseudonymization technique was proposed in the meetings. However, the PDP law does not include pseudonymization. Pseudonymization has also been added to GDPR ("Key Changes with the General Data Protection Regulation," 2017), so it should be in the PDP law, too. A family consent option needs to be discussed further within the scope of the law. Since it is difficult to predict what genetic science will bring us in the future, preventing genetic data from being stored in unsafe environments is crucial.

Health and genetic data are listed in the law as special categories of data. Besides, no exception is defined for the processing of genetic data. However, as was mentioned in the meetings, government agencies request genetic data within health records. Furthermore, investigations were conducted against some clinicians who refused to share this data. There may be many other clinicians who accepted to share genetic data with these agencies. Although genetic data and health data are mentioned separately in the law, there is obviously a disagreement in the current situation. It is necessary to emphasize this distinction within the law more clearly. Moreover, the law addresses only genetic data, but genomic data needs to be mentioned, too.

The absence of a special act on genetic data is seen as the major shortcoming in Turkey. According to the participants' opinions, just listing genetic data in the special category will not be enough. As the analysis by Joly, Feze and Simard (Joly et al., 2013) showed, genetic discrimination exists and people are concerned about it. Therefore, more detailed and constructive regulations are needed in this area. A special act, like GINA, to prevent genetic data from being abused in the insurance sector should be discussed in Turkey, as well. The same study also reported that the identification of the genome can cause discrimination especially by insurance companies (ibid.). Actually, the Turkish constitution was based essentially on the prevention of discrimination. No addition to the constitution may be needed, but a special act might guarantee that misuse will be avoided.





## CHAPTER 6

### CONCLUSION

The dissertation has generated many important secondary products, since it consists of four sub-studies on popular research topics in the area of medical informatics. Even though each sub-study was conducted independently, they are closely related with one another. Firstly, through an application market analysis, we could identify the shortcomings and limitations of the current personal health record applications. Moreover, basic data elements and features of an mPHR were defined as a starting point for the dissertation. Thus, we could also figure out what we should ask the public about design elements of a mobile PHR in the survey. Afterwards, the results of the analysis were expanded with a public survey. The preliminary results of the survey and the results of the mPHR analysis were used in the first meetings of the participatory design study. In this way, a paper prototype sample of an mPHR including genetic/genomic data was created in these meetings. For a last study, we evaluated the ethical and legal problems of the current situation in Turkey and determined the requirements for developing a legal compliance system, since there is no meaning in developing a perfectly designed system unless it obeys the data protection laws and regulations or in developing the most secure system unless the data is protected by laws.

In the scope of the dissertation, our initial research questions were answered and reported: essential characteristics of a health record application with inclusion of genetic/genomic data were defined, the opinions of ordinary users, stakeholders, and experts on design issues regarding the application were taken, ethical and legal problems of the Turkish electronic health system concerning the exchange of health and genetic data were discussed, and we established what type of security protections and regulations are needed in order to reduce public concerns about security and confidentiality.

Three essential characteristics of mPHRs including genetic data were defined. First, it should provide a high standard of security and privacy. Security and privacy issues of the application should be solved before handling any sensitive data. mPHR analysis showed that applications in the market have limited security features. According to the survey results, people tended to want more than one security protection, and online banking security solutions can be implemented in the application to increase users' trust. In parallel with these preferences, the participants in the PD group discussions agreed on adding a Terms and conditions section covering Turkish data privacy issues, setting up security measures for the system login, and using a less sensitive ID for signing up to the application.

Second, the user should have exclusive control over his or her genetic/health data. Hence, the importance of PHRs was emphasized for storing and processing genetic data. Participants of the survey would like to have exclusive control over their data, insisting that no one should have access to their data without their consent. Their opinions on this subject were so strong that they said they would prefer to limit the access right even to their doctors, while they had previously defined doctors as the only professional group they would trust with the privacy of their health/genetic data. Experts in both focus group studies thought that collecting health and genetic information was not a problem; nevertheless, collecting them in a single center and process them without the consent of the data owner were considered important problems. The the focus group suggested that the data should not be collected in a single center, since this is not only against human rights but also entails a big threat of data being leaked. Since the PHRs give undivided control to the users, it is easier to get consent for collecting data with a PHR. Moreover, with PHRs data is not collected in one center; it is distributed between the users. Hence, these results support the importance of PHRs for handling genetic/genomic data.

Third, the application should definitely be developed in accordance with the provisions of the data privacy laws and regulations. The mPHR analysis indicated that even the most secure application evaluated in our sample had deficiencies in data privacy issues. Moreover, the laws and regulations for the protection of the personal data privacy should be tightened. Necessary actions should be taken in order to reduce public concerns that were referred to many times in the survey and focus group studies. The survey results showed that people have prejudices and concerns about their health data. Moreover, an important number of people had been faced with disclosures and breach of their health data security. In the focus group meetings, these concerns and the importance of legal protection were emphasized repeatedly. Negative consequences, such as avoiding to see a doctor, go for testing, or ask for treatment, were mentioned. In order to reduce these worries, laws (PDP) and regulations should be redesigned, and the punishments should be more daunting to reduce these concerns. Otherwise, people may refuse to use even the most secure, perfectly designed systems.

The opinions of ordinary users, stakeholders, and experts on design issues about the application were included in the scope of the dissertation. First of all, our studies indicated that the design of a genetic data record system should be different from a regular health record system. The results of the survey pointed out that people were not opposed to keeping genetic data in a mobile application; however, they thought that genetic data was significantly more sensitive than any other health-related data. This was a very important result because in this way, we could see that people are aware that genetic data is different, even more sensitive than general health data. Since we conducted the onsite survey in genetic test centers and half of our participants were familiar with genetic tests, this information was rather more meaningful.

Experts and stakeholders, too, stressed the sensitivity and specialty of genetic information several times in the focus group meetings. It was emphasized that the genetic data might even be the most sensitive data type in the world. Hence, if any breach or disclosure incident occurs in a genetic/genomic data storage, the consequences

cannot be reversed. Even though the Turkish personal data protection law (PDP) has recently come into effect, there is still a deficiency in genetic/genomic data protection in Turkey's legal system. Hence, both experts and public opinion hold that genetic/genomic data is of special importance and necessitates a better protection through a law or an act. With the help of the PD group study, an example of how to add genetic data to this system was shown in a prototype, to which a small questionnaire about family history and a pedigree tool were added.

Privacy and legal problems of the Turkish electronic health system regarding health and genetic data exchange were mostly discussed in the focus group meetings. As a result, problems of the current legal status of health and genetic data were reported. They were not only criticized but also suggestions were presented for a better legal grounding. This topic was very important since there is no point in designing a perfect and most secure system as long as the security and privacy of the products are not guaranteed by law.

According to the discussions, there were problems with the new Turkish personal data protection law: the frame of collectable data was too wide, and the exceptions were large. Furthermore, exceptions defined in the law on consent issues are very broad, even for the most sensitive types of data. However, consent was recently strengthened in the GDPR. The consent topic is a very important issue and should be treated much more carefully when defining any exceptions in this regard. For any sensitive information such as sexual health and genetic data, there should be no exception other than in urgent or judicial cases.

Furthermore, the importance of genetic data was not emphasized enough. Genetic data have many properties that should be considered when drafting laws and regulations, given that there is no possible way to restore the situation after a breach of genetic data security since people's genetic codes cannot be changed. Therefore, preventive actions must be taken much more rigorously before genetic data is collected. There should be a specific law or at least individual articles dedicated to genetic data which also include the dimension of discrimination based on genetic differences in Turkey.

Another topic of this dissertation was the type of security protection and regulations that are needed in order to reduce public concerns about security and confidentiality. In the PD analysis, it was found that there was a highly protected mobile PHR application in the market, whose design had even won international awards ("e-Nabız'a dünya çapında ödül", 2017). However, there is a big fundamental privacy problem with this application, because it uses an opt-out system. As opt-out systems bypass the task of getting consent from users, they are in conflict with data protection laws and regulations. A legally appropriate system must definitely be opt-in based.

The mPHR analysis indicated that the majority of the applications had limited security features (mostly only ID-Password logins). By contrast, the results of the survey showed that people want to see more than an ID-password login protection in a mobile health/genetic data record system. According to the results, especially a One Time SMS Password feature could be implemented in the application to increase users' trust.

Experts and stakeholders of the focus group studies emphasized the need for special laws and regulations for genetic/genomic data handling. The genetic data is only listed in the category of special data in the PDP law. Besides, although the genetic code is unique for every person, genetic illnesses are related with all the family members. In other words, besides the personal risks, a disclosure affects relatives beyond the patient. Therefore, in addition to the importance of consent even before taking the test, participants suggested to include family consent options.

In the meetings, focus group participants highly recommended the use of pseudonymization as a technique instead of the unachievable anonymization of genetic/genomic data. Even though this technique has been added to GDPR recently, it is not mentioned in the PDP law.

As a result, the dissertation answered the question about the characteristics of a personal health record application for inclusion of genetic/genomic data. Furthermore, the necessary security protection measures and desirable laws and regulations to reduce the public concerns about security and privacy were identified and security, privacy, and legal problems of the Turkish electronic health system regarding health and genetic data exchange were listed. In the end, a sample paper-prototype for interface design was suggested. Thus, the system elements for genetic/genomic data inclusion were discussed and determined in all aspects.

## **6.1. Limitation and Future Work**

In this section, some limitations are listed, and future studies are suggested:

- In the survey, collecting data from genetically tested patients was challenging since most people in the diagnostic centers either refused to participate in the study or did not fully complete the questionnaire. In addition, approximately 85% of the incomplete questionnaires belonged to respondents with a high school or a lower level of education. In the online version of the questionnaire, only 5.7% of the participants who responded to all questions had a lower educational background. Therefore, it was not possible to analyze the overall difference between the results according to the education levels of the participants.
- A sample prototype was drawn by the participatory design group. However, an evaluation of the paper prototype was missing. The evaluation part can be done as a future study. The participant representation was also limited, as there was no handicapped or elderly participant in the design group.
- There is no established legal system in Turkey regarding data privacy; the law and regulations were brand new when the focus groups met. Many issues were newly constituted, and some rules were modified after being criticized by the groups. Therefore, the issue of how laws will be enforced is based on

assumptions only. After a certain period of time, these issues can be discussed again based upon actual events in a future research project.

- The infrastructure of data storage and data encryption options were not in the scope of the design studies, so where the actual data would be stored (i.e. in a cloud system or on a server) and what kind of encryption methods should be applied to the system are to be discussed in the design. It was assumed that these methods would be adapted to the system in the most appropriate manner. For future research, these issues can be discussed with cyber security and data infrastructure experts.
- Lastly, a mobile PHR application can be designed conforming to the rules and concerns laid out in the study, and then a usability analysis can be implemented with various user groups and their opinions can be compared.



## REFERENCES

- Akgün, M., Bayrak, A. O., Ozer, B., & Sağıroğlu, M. Ş. (2015). Privacy preserving processing of genomic data: A survey. *Journal of Biomedical Informatics*, 56, 103-111. <https://doi.org/10.1016/j.jbi.2015.05.022>
- Akpınar, A. (2010). *Ethics in using genetic information: attitudes and preferences of physicians and testees*. (Doctoral dissertation). Retrieved from Council of Higher Education Thesis Center. (Accession No. 288988)
- Alahmad, G., Hifnawy, T., Abbasi, B., & Dierickx, K. (2016). Attitudes toward medical and genetic confidentiality in the Saudi research biobank: An exploratory survey. *International Journal of Medical Informatics*, 87, 84-90. <https://doi.org/10.1016/j.ijmedinf.2015.12.015>
- Almadani, Y. A. A. (2016). *Usability of phr systems*. (Master's thesis). Retrieved from Council of Higher Education Thesis Center. (Accession No. 444373)
- Anayasa Mahkemesinin 28/9/2017 Tarihli ve E: 2016/125, K: 2017/143 Sayılı Kararı. (2018). Retrieved April 15, 2018, from <http://www.resmigazete.gov.tr/eskiler/2018/01/20180123-15.pdf>
- Andrews, E. L. (1998, October 26). European Law Aims to Protect Privacy of Data. *The New York Times*. Retrieved from <http://www.nytimes.com/1998/10/26/business/european-law-aims-to-protect-privacy-of-data.html>
- Andrews, L. B., & Jaeger, A. S. (1991). Confidentiality of genetic information in the workplace. *American Journal of Law and Medicine*, 17(1-2), 75-108.
- Aro, A. R., Hakonen, A., Hietala, M., Lönnqvist, J., Niemelä, P., Peltonen, L., & Aula, P. (1997). Acceptance of genetic testing in a general population: Age, education and gender differences. *Patient Education and Counseling*, 32(1-2), 41-49. [https://doi.org/10.1016/S0738-3991\(97\)00061-X](https://doi.org/10.1016/S0738-3991(97)00061-X)
- Arora, S., Yttri, J., & Nilse, W. (2014). Privacy and Security in Mobile Health (mHealth) Research. *Alcohol Research : Current Reviews*, 36(1), 143-51. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/26259009>
- Ashley, J. (2010, April 26). BBC News - Women “more likely to report ill health than men.” *Bbc*. Retrieved from <http://news.bbc.co.uk/2/hi/health/8588686.stm>
- Atienza, A. A., Zarcadoolas, C., Vaughon, W., Hughes, P., Patel, V., Chou, W.-Y. S., & Pritts, J. (2015). Consumer Attitudes and Perceptions on mHealth Privacy and

- Security: Findings From a Mixed-Methods Study. *Journal of Health Communication*, 20(6), 673-679. <https://doi.org/10.1080/10810730.2015.1018560>
- Ayday, E., De Cristofaro, E., Hubaux, J.-P., & Tsudik, G. (2015). The Chills and Thrills of Whole Genome Sequencing. *Computer*, (iv), 1-1. <https://doi.org/10.1109/MC.2013.333>
- Ayday, E., Raisaro, J. L., Hubaux, J.-P., & Rougemont, J. (2013). Protecting and evaluating genomic privacy in medical tests and personalized medicine. *Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society - WPES '13*, 95-106. <https://doi.org/10.1145/2517840.2517843>
- Baig, M. M., GholamHosseini, H., & Connolly, M. J. (2015). Mobile healthcare applications: system design review, critical issues and challenges. *Australasian Physical & Engineering Sciences in Medicine*, 38(1), 23-38. <https://doi.org/10.1007/s13246-014-0315-4>
- Baird, A., North, F., & Raghu, T. (2011). Personal Health Records (PHR) and the future of the physician-patient relationship. *Proceedings Of The 2011 Iconference On - Iconference '11*. doi:10.1145/1940761.1940800
- Bates, C. (2011, December 30). Women pop to the doctor more than men “because they really ARE the sicker sex” | Daily Mail Online. Retrieved April 4, 2017, from <http://www.dailymail.co.uk/health/article-2080238/Women-pop-doctor-men-really-ARE-sicker-sex.html>
- Belmont, J., & McGuire, A. L. (2009). The futility of genomic counseling: essential role of electronic health records. *Genome Medicine*, 1(5), 48. <https://doi.org/10.1186/gm48>
- Bennett, R. L., French, K. S., Resta, R. G., & Doyle, D. L. (2008). *Standardized human pedigree nomenclature: Update and assessment of the recommendations of the national society of genetic counselors*. *Journal of Genetic Counseling*, 17(5), 424-433. <https://doi.org/10.1007/s10897-008-9169-9>
- Bernard, H. R. (2017). *Research methods in anthropology: Qualitative and quantitative approaches*. Rowman & Littlefield.
- Beyan, T. (2014). *Single nucleotide polymorphism (snp) data integrated electronic health record (ehr) for personalized medicine*. (Doctoral dissertation). Retrieved from Council of Higher Education Thesis Center. (Accession No. 379859)
- Botts, N. E., Horan, T. A., & Thoms, B. P. (2011). HealthATM: Personal health cyberinfrastructure for underserved populations. *American Journal of Preventive Medicine*, 40(5 SUPPL. 2), 115-122. <https://doi.org/10.1016/j.amepre.2011.01.016>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101. <https://doi.org/10.1191/1478088706qp063oa>
- Brett, K. M., & Burt, C. W. (2001). Utilization of ambulatory medical care by women: United States, 1997-98. *Vital and Health Statistics. Series 13, Data from the*



- National Health Survey*, (149), 1-46. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/11478128>
- Burns, C., Cottam, H., Vanstone, C., & Winhall, J. (2006). RED Paper 02: Transformation Design. *Design Council*. Retrieved from [www.designcouncil.org.uk/red](http://www.designcouncil.org.uk/red).
- Canada Health Infoway, & EKOS Research Associates. (2007). Electronic health information and privacy survey: What Canadians think — 2007. *Health (San Francisco)*.
- Canbay, P. (2014). *Anonymity in healthcare systems: An ideal data sharing model for distributed structures*. (Master's thesis). Retrieved from Council of Higher Education Thesis Center. (Accession No. 379628)
- Carman, D., & Britten, N. (1995). Confidentiality of medical records: The patient's perspective. *British Journal of General Practice*, 45(398), 485-488.
- Carrión Señor I., Fernández-Alemán J.L, & Toval A. (2012). Are Personal Health Records Safe? A Review of Free Web-Accessible Personal Health Record Privacy Policies. *Journal of Medical Internet Research*, 2012;14(4):e114 DOI: 10.2196/jmir.1904, PMID: 22917868, PMCID: PMC3510685
- Chen, H. M., Liou, Y. Z., Chen, S. Y., & Li, J. S. (2013). Design of mobile healthcare service with health records format evaluation. In *2013 IEEE International Symposium on Consumer Electronics (ISCE)* (pp. 257-258). IEEE. <https://doi.org/10.1109/ISCE.2013.6570215>
- Chiu, P. P. K., Lee, T. K. S., & Cheng, J. M. F. (2011). Health guard system with emergency call based on smartphone. In *IET International Communication Conference on Wireless Mobile and Computing (CCWMC 2011)* (Vol. 2011, pp. 443-446). IET. <https://doi.org/10.1049/cp.2011.0926>
- CHP kişisel verilerin korunması kanununun iptali için AYM'ye başvurdu. (2016, June 3). *Sözcü*.
- Communication Minister denies massive data leak. (2016). Retrieved March 3, 2018, from <http://www.milliyet.com.tr/communication-minister-denies-en-2222088/en.htm>
- Danıştay: Kişisel verileri toplamak hukuka aykırı. (2014). Retrieved March 3, 2018, from <http://haber.sol.org.tr/devlet-ve-siyaset/danistay-kisisel-verileri-toplamak-hukuka-aykiri-haberi-97773>
- Danıştay Sağlık Net 2 Veri Gönderiminin Yürütmesini Durdurdu. (2014). Retrieved April 21, 2018, from [https://ttb.org.tr/haberarsiv\\_goster.php?Guid=675640fe-9232-11e7-b66d-1540034f819c&1534-D83A\\_1933715A=170329c1a3a1e49803a269ca4a0db95b0e762496](https://ttb.org.tr/haberarsiv_goster.php?Guid=675640fe-9232-11e7-b66d-1540034f819c&1534-D83A_1933715A=170329c1a3a1e49803a269ca4a0db95b0e762496)
- Data Protection Ombudsman. (2014). Retrieved March 3, 2018, from <http://www.tietosuoja.fi/en/index/tietosuojavaaltuutetuntoimisto.html>

- Diamond, C. C., Mostashari, F., & Shirky, C. (2009). Collecting and sharing data for population health: A new paradigm. *Health Affairs*, 28(2), 454-466. <https://doi.org/10.1377/hlthaff.28.2.454>
- Dollar, N. J., & Merrigan, G. M. (2002). *New Directions in Group Communication*. In *New Directions in Group Communication* (pp. 52-78). SAGE PUBLICATIONS.
- Dust, F., & Jonsdatter, G. (2008). Participatory design. In M. Erlhoff & T. Marshall (Eds.), *Design dictionary: Perspectives on design terminology* (290-292). Boston, MA: Birkhauser Verlag AG.
- Erdfelder, E., Faul, F., & Buchner, A. (1996). GPOWER: A general power analysis program. *Behavior Research Methods, Instruments, & Computers*, 28(1), 1-11. <https://doi.org/10.3758/BF03203630>
- E-nabiz. (2015). Retrieved February 22, 2018, from <https://enabiz.gov.tr/Yardim/Index>
- e-Nabız'a dünya çapında ödül. (2017). Retrieved July 20, 2018, from <http://www.ensonhaber.com/e-nabiza-dunya-capinda-odul-2017-03-21.html>
- e-Nabız Projesinin yürütmesi durduruldu. (2016). Retrieved February 22, 2018, from [https://www.ttb.org.tr/haber\\_goster.php?Guid=67aba954-9232-11e7-b66d-1540034f819c&1534-D83A\\_1933715A=11be176a2b2e05b25eda69109c875503d8cca463](https://www.ttb.org.tr/haber_goster.php?Guid=67aba954-9232-11e7-b66d-1540034f819c&1534-D83A_1933715A=11be176a2b2e05b25eda69109c875503d8cca463)
- Espeland, M. A., Dotson, K., Jaramillo, S. A., Kahn, S. E., Harrison, B., Montez, M., ... Look AHEAD Research Group, L. A. R. (2006). Consent for genetics studies among clinical trial participants: findings from Action for Health in Diabetes (Look AHEAD). *Clinical Trials (London, England)*, 3(5), 443-56. <https://doi.org/10.1177/1740774506070727>
- Etikan, I., Abubakar Musa, S., & Sunusi Alkassim, R. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1-4. <https://doi.org/10.11648/j.ajtas.20160501.11>
- EU 2016 Press release. (2016). EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield. *European Commission - Press Release*, (February). Retrieved from [http://europa.eu/rapid/press-release\\_IP-16-216\\_en.htm](http://europa.eu/rapid/press-release_IP-16-216_en.htm)
- EU Turkey 2018 Report. (2018). Strasbourg. Retrieved from <https://ec.europa.eu/neighbourhood-enlargement/sites/near/files/20180417-turkey-report.pdf>
- Floyd, C., Mehl, W.-M., Resin, F.-M., Schmidt, G., & Wolf, G. (1989). Out of Scandinavia: Alternative Approaches to Software Design and System Development. *Human-Computer Interaction*, 4(4), 253-350. [https://doi.org/10.1207/s15327051hci0404\\_1](https://doi.org/10.1207/s15327051hci0404_1)
- Ford, E. W., Hesse, B. W., & Huerta, T. R. (2016). Personal Health Record Use in the United States: Forecasting Future Adoption Levels. *Journal of Medical Internet*

- Research*, 18(3), e73. <https://doi.org/10.2196/jmir.4973>
- Friedman, C. P., & Wyatt, J. C. (1997). *Evaluation Methods in Medical Informatics*. New York, NY: Springer New York. <https://doi.org/10.1007/978-1-4757-2685-5>
- Fromholz, J. M. (2000). The European Union data privacy directive. *Berkeley Technology Law Journal*, 15(418), 461-484. <https://doi.org/10.15779/Z383D48>
- Garets, D., & Mike, D. (2006). Electronic Medical Records vs . Electronic Health Records : Yes , There Is a Difference By Dave Garets and Mike Davis Updated January 26 , 2006 HIMSS Analytics , LLC 230 E . Ohio St ., Suite 600 Chicago , IL 60611-3270 EMR vs . EHR : Definitions The marke. *Health (San Francisco)*, 1-14. <https://doi.org/10.3233/978-1-60750-044-5-26>
- Geller, T. (2016). In privacy law, it's the U.S. vs. the world. *Communications of the ACM*, 59(2), 21-23. <https://doi.org/10.1145/2852233>
- General Data Protection Regulation (GDPR). (2017). Retrieved April 23, 2018, from <https://gdpr-info.eu/>
- Goldman, J. (1998). Protecting privacy to improve health care. *Health Affairs*, 17(6), 47-60. <https://doi.org/10.1377/hlthaff.17.6.47>
- Goldstein, J. (2010, March 26). Women admitted to hospitals more often than men. *Philly.Com*. Retrieved from [http://www.philly.com/philly/blogs/healthcare/Women\\_admitted\\_to\\_hospitals\\_more\\_often\\_than\\_men.html](http://www.philly.com/philly/blogs/healthcare/Women_admitted_to_hospitals_more_often_than_men.html)
- Green, D., Cushman, M., Dermond, N., Johnson, E. A., Castro, C., Arnett, D., ... Manolio, T. A. (2006). Obtaining Informed Consent for Genetic Studies. *American Journal of Epidemiology*, 164(9), 845-851. <https://doi.org/10.1093/aje/kwj286>
- Greenleaf, G. (2017). Countries with Data Privacy Laws – by Year 1973- - - 2016, 108, 2016-2017.
- Guttmacher, A. E., & Collins, F. S. (2003). Welcome to the Genomic Era. *New England Journal of Medicine*, 349(10), 996-998. <https://doi.org/10.1056/NEJMe038132>
- Gymrek, M., McGuire, A. L., Golan, D., Halperin, E., & Erlich, Y. (2013). Identifying Personal Genomes by Surname Inference. *Science*, 339(6117), 321-324. <https://doi.org/10.1126/science.1229566>
- Heath, D., Ardestani, A., & Nemati, H. (2016). Sharing personal genetic information: the impact of privacy concern and awareness of benefit. *Journal of Information, Communication and Ethics in Society*, 14(3), 288-308. <https://doi.org/10.1108/JICES-07-2015-0025>
- Henneman, L., Vermeulen, E., Van El, C. G., Claassen, L., Timmermans, D. R. M., & Cornel, M. C. (2013). Public attitudes towards genetic testing revisited: Comparing opinions between 2002 and 2010. *European Journal of Human Genetics*, 21(8), 793-799. <https://doi.org/10.1038/ejhg.2012.271>

- Hietala, M., Hakonen, a, Aro, a R., Niemelä, P., Peltonen, L., & Aula, P. (1995). Attitudes toward genetic testing among the general population and relatives of patients with a severe genetic disease: a survey from Finland. *American Journal of Human Genetics*, 56(6), 1493-500. Retrieved from <http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=1801087&tool=pmcentrez&rendertype=abstract>
- Hoffman, M. A. (2007). The genome-enabled electronic medical record. *Journal of Biomedical Informatics*, 40(1), 44-46. <https://doi.org/10.1016/J.JBI.2006.02.010>
- Hoffman, S. (2017, January 1). Big Data and the Americans with Disabilities Act: Amending the Law to Cover Discrimination Based on Data-Driven Predictions of Future Illnesses. Retrieved December 25, 2017, from [https://scholarlycommons.law.case.edu/faculty\\_publications/1990](https://scholarlycommons.law.case.edu/faculty_publications/1990)
- Isidore, C. (2015). RadioShack trying to sell data of 100 million customers - Mar. 25, 2015. Retrieved March 3, 2018, from <http://money.cnn.com/2015/03/25/news/companies/radioshack-customer-data/index.html>
- Jamal, L., Sapp, J. C., Lewis, K., Yanes, T., Facio, F. M., Biesecker, L. G., & Biesecker, B. B. (2014). Research participants' attitudes towards the confidentiality of genomic sequence information. *European Journal of Human Genetics*, 22(8), 964-968. <https://doi.org/10.1038/ejhg.2013.276>
- Joly, Y., Ngueng Feze, I., & Simard, J. (2013). Genetic discrimination and life insurance: a systematic review of the evidence. *BMC Medicine*, 11(1), 25. <https://doi.org/10.1186/1741-7015-11-25>
- Jonassen, D. H., & Driscoll, M. P. (2004). *Handbook of research on educational communications and technology*. Lawrence Erlbaum.
- Jones, B. (2012). Genetic Information Nondiscrimination Act of 2008, 2008, 881-922. Retrieved from <http://www.gpo.gov/fdsys/pkg/PLAW-110publ233/content-detail.html>
- Kandiyoti, D. (1977). Sex Roles and Social Change: A Comparative Appraisal of Turkey's Women. *Signs: Journal of Women in Culture and Society*, 3(1), 57-73. <https://doi.org/10.1086/493439>
- Kandiyoti, D. (1988). Bargaining with Patriarchy. *Gender & Society*, 2(3), 274-290. <https://doi.org/10.1177/089124388002003004>
- Kaya, B. (2018). Skandal! SGK hasta bilgilerini 65 bin TL'ye sattı. *Sözcü Gazetesi*. Retrieved August 6, 2018, from <https://www.sozcu.com.tr/2018/ekonomi/skandal-sgk-hasta-bilgilerini-65-bin-tlye-satti-2225264/>
- Keser Berber, L., Ülgü, M., & Er, C. (2010). *Elektronik Sağlık Kayıtları ve Özel Hayatın Gizliliği*. Roche.
- Key Changes with the General Data Protection Regulation. (2017). Retrieved March 3,

- 2018, from <https://www.eugdpr.org/the-regulation.html>
- Khan A, Capps BJ, Sum MY, Kuswanto CN, & Sim K. (2014). Informed consent for human genetic and genomic studies: a systematic review. *Clin Genet*, 86(86), 199-206. <https://doi.org/10.1111/cge.12384>
- Kharrazi, H., Chisholm, R., VanNasdale, D., & Thompson, B. (2012). Mobile personal health records: An evaluation of features and functionality. *International Journal of Medical Informatics*. <https://doi.org/10.1016/j.ijmedinf.2012.04.007>
- Kişisel sağlık verilerinin işlenmesi ve mahremiyetinin sağlanması hakkında yönetmelikte değişiklik yapılmasına dair yönetmelik. (2017). Retrieved February 25, 2018, from <http://www.resmigazete.gov.tr/eskiler/2017/11/20171124-1.htm>
- Kişisel verileri koruma kurumu başkanlığı. (2017). Retrieved February 25, 2018, from <http://www.kvkk.gov.tr/>
- Kişisel verilerin korunması kanunu. (2016). Retrieved April 4, 2017, from <http://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf>
- Klitzman R, Appelbaum PS, & Chung WK. (2014). Should life insurers have access to genetic test results? *Jama*, 312(18), 1855-1856. <https://doi.org/10.1001/jama.2014.13301>
- Knoppers, B. M., & Godard, B. (1998). Ethical and legal perspectives on inherited cancer susceptibility. Retrieved from <https://papyrus.bib.umontreal.ca/xmlui/handle/1866/72>
- Küzeci, E. (2010). *Kişisel Verilerin Korunması*. Ankara: Turhan Kitapevi. Retrieved from <http://www.kisiselsaglikverileri.org/51-kisisel-verilerin-korunmasi-dr-elif-kuzeci.html>
- Lafky, D. B., & Horan, T. A. (2011). Personal health records: Consumer attitudes toward privacy and security of their personal health information. *Health Informatics Journal*, 17(1), 63-71.
- Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. *IEEE transactions on parallel and distributed systems*, 24(1), 131-143.
- Liu, J., Huang, X., & Liu, J. (2015). Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption. *Future Generation Computer Systems*, 52, 67-76. doi:10.1016/j.future.2014.10.014
- Lunshof, J. E., Chadwick, R., Vorhaus, D. B., & Church, G. M. (2008). From genetic privacy to open consent. *Nature Reviews Genetics*, 9(5), 406-411. <https://doi.org/10.1038/nrg2360>
- Luxton, D. D., Kayl, R. A., & Mishkind, M. C. (2012). mHealth Data Security: The Need for HIPAA-Compliant Standardization. *Telemedicine and E-Health*, 18(4), 284-288. <https://doi.org/10.1089/tmj.2011.0180>

- Luxton, D. D., McCann, R. A., Bush, N. E., Mishkind, M. C., & Reger, G. M. (2011). MHealth for mental health: Integrating smartphone technology in behavioral healthcare. *Professional Psychology: Research and Practice*, 42(6), 505-512. <https://doi.org/10.1037/a0024485>
- Madden, M., & Rainie, L. (2015). Americans' Attitudes About Privacy, Security and Surveillance. *Pew Research Center, Washington D.C.* Retrieved from [www.pewresearch.org](http://www.pewresearch.org)
- Malin, B. (2005). An Evaluation of the Current State of Genomic Data Privacy Protection Technology and a Roadmap for the Future. *Journal of the American Medical Informatics Association*, 12, 28-34. <https://doi.org/10.1197/jamia.M1603>.The
- Maria Piras, E., & Zanutto, A. (2014). "One day it will be you who tells us doctors what to do!". Exploring the "Personal" of PHR in paediatric diabetes management. *Information Technology & People*, 27(4), 421-439. <https://doi.org/10.1108/ITP-02-2013-0030>
- Marr, B. (2015, September 30). Big Data: 20 Mind-Boggling Facts Everyone Must Read. *Forbes*. Retrieved from <https://www.forbes.com/sites/bernardmarr/2015/09/30/big-data-20-mind-boggling-facts-everyone-must-read/#2735d4f617b1>
- Martínez-Pérez, B., Torre-Díez, I. de la, & López-Coronado, M. (2015). Privacy and Security in Mobile Health Apps: A Review and Recommendations. *Journal of Medical Systems*, 39(1). <https://doi.org/10.1007/s10916-014-0181-3>
- Matsui, K., Kita, Y., & Ueshima, H. (2005). Informed consent, participation in, and withdrawal from a population based cohort study involving genetic analysis. *J Med Ethics*, 31, 385-392. <https://doi.org/10.1136/jme.2004.009530>
- McCusker, S. (2016). *Business law review. Business Law Review* (Vol. 37). Kluwer Law International. Retrieved from <https://www.kluwerlawonline.com/abstract.php?area=Journals&id=BULA2016017>
- McGrath, M. (2014, January 10). Target Data Breach Spilled Info On As Many As 70 Million Customers. *Forbes*. Retrieved April 4, 2017, from <https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/#3bb9bccce795>
- McGrenere, J., Davies, R., Findlater, L., Graf, P., Klawe, M., Moffatt, K., ... Yang, S. (2002). Insights from the aphasia project. *ACM SIGCAPH Computers and the Physically Handicapped*, (73-74), 112. <https://doi.org/10.1145/960201.957225>
- McGuire, A. L., Fisher, R., Cusenza, P., Hudson, K., Rothstein, M. A., McGraw, D., ... Henley, D. E. (2008). Confidentiality, privacy, and security of genetic and genomic test information in electronic health records: points to consider. *Genetics in Medicine*, 10(7), 495-499. <https://doi.org/10.1097/GIM.0b013e31817a8aaa>
- McGuire, A. L., Oliver, J. M., Slashinski, M. J., Graves, J. L., Wang, T., Kelly, P. A., ...

- Hilsenbeck, S. G. (2011). To share or not to share: a randomized trial of consent for data sharing in genome research. *Genetics in Medicine: Official Journal of the American College of Medical Genetics*, 13(11), 948-55. <https://doi.org/10.1097/GIM.0b013e3182227589>
- Mezuk, B., Eaton, W. W., & Zandi, P. (2008). Participant Characteristics That Influence Consent for Genetic Research in a Population-Based Survey: The Baltimore Epidemiologic Catchment Area Follow-Up. *Community Genet*, 11, 171-178. <https://doi.org/10.1159/000113880>
- Mohammed, S., Lim, Z., Dean, P. H., Potts, J. E., Tang, J. N. C., Etheridge, S. P., ... Sanatani, S. (2017). Genetic Insurance Discrimination in Sudden Arrhythmia Death Syndromes: Empirical Evidence From a Cross-Sectional Survey in North America. *Circulation. Cardiovascular Genetics*, 10(1), e001442. <https://doi.org/10.1161/CIRCGENETICS.116.001442>
- Muller, M. J. (1991). PICTIVE -An Exploration in Participatory Design. In *The SIGCHI Conference on Human Factors in Computing Systems Reaching through Technology - CHI '91* (pp. 225-231). <https://doi.org/http://doi.org/10.1145/108844.108896>
- National Committee on Vital and Health Statistics. (2006). *Personal Health Records and Personal Health Record Systems*. Retrieved from <https://ncvhs.hhs.gov/wp-content/uploads/2014/05/0602nhirpt.pdf>
- O'Brien, D. G., & Yasnoff, W. A. (1999). Privacy, confidentiality, and security in information systems of state health agencies. *American Journal of Preventive Medicine*, 16(4), 351-8. Retrieved from <http://www.ncbi.nlm.nih.gov/pubmed/10493295>
- Ocak 2015 Aclik ve Yoksulluk Siniri. (2015). Retrieved April 4, 2017, from <http://www.turkis.org.tr/OCAK-2015-ACLİK-ve-YOKSULLUK-SINIRI-d597>
- Oliver, J. M., Slashinski, M. J., Wang, T., Kelly, P. A., Hilsenbeck, S. G., & Mcguire, A. L. (2012). Balancing the Risks and Benefits of Genomic Data Sharing: Genome Research Participants' Perspectives. *Public Health Genomics*, 15, 106-114. <https://doi.org/10.1159/000334718>
- Ozok, A. A., Wu, H., Garrido, M., Pronovost, P. J., & Gurses, A. P. (2014). Usability and perceived usefulness of personal health records for preventive health care: A case study focusing on patients' and primary care providers' perspectives. *Applied ergonomics*, 45(3), 613-628.
- Özdemir, K. M. (2010). *A framework for authentication of medical reports based on keystroke dynamics*. (Master's thesis). Retrieved from Council of Higher Education Thesis Center. (Accession No. 291681)
- Özkan, Ö. (2011). *Attitudes and opinions of people who use medical services about privacy and confidentiality of health information in electronic environment*. (Master's thesis). Retrieved from Council of Higher Education Thesis Center.

(Accession No. 291671)

- Pala, E., & Kartal, B. (2010). Banka müşterilerinin internet bankacılığı ile ilgili tutumlarına yönelik bir pilot araştırma. *Yönetim ve Ekonomi: Celal Bayar Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 17(2), 43-61.
- Pallant, J. (2013). *Spss Survival Manual - Pallant, Julie*. McGraw-Hill Education. Retrieved from [https://books.google.de/books?hl=tr&lr=&id=fZZTBgAAQBAJ&oi=fnd&pg=PR7&ots=KVGxiQUZxR&sig=vewn7UmcvRKJpj2c36wbW1rGHeY&redir\\_esc=y#v=onepage&q&f=false](https://books.google.de/books?hl=tr&lr=&id=fZZTBgAAQBAJ&oi=fnd&pg=PR7&ots=KVGxiQUZxR&sig=vewn7UmcvRKJpj2c36wbW1rGHeY&redir_esc=y#v=onepage&q&f=false)
- Pohl, M. (2017). 325,000 mobile health apps available in 2017 – Android now the leading mHealth platform. Retrieved December 23, 2017, from <https://research2guidance.com/325000-mobile-health-apps-available-in-2017/>
- Postacı, Ş. (2012). *An advanced personal health record platform for patient empowerment*. (Master's thesis). Retrieved from Council of Higher Education Thesis Center. (Accession No. 318815)
- Presidential Commission for the Study of Bioethical Issues. (2012). *PRIVACY and PROGRESS in Whole Genome Sequencing*. Washington, D.C. Retrieved from [https://bioethicsarchive.georgetown.edu/pcsbi/sites/default/files/PrivacyProgress508\\_1.pdf](https://bioethicsarchive.georgetown.edu/pcsbi/sites/default/files/PrivacyProgress508_1.pdf)
- Princeton Survey Research Associates. (1999). *Medical Privacy and Confidentiality Survey*. California.
- Rainie, L., & Anderson, J. (2017). *The Fate of Online Trust in the Next Decade*.
- Raul, A. C., Manoranjan, T. D., & Mohan, V. (2015). *The Privacy , Data Protection and Cybersecurity Law Review*.
- Riley, C. (2015, February 6), "Insurance giant anthem hit by massive data breach", *CNN Money*, Retrieved April 4, 2017, from <http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/>
- Robinson, D. (2016, May 25). Facebook data transfers threatened by EU ruling. *Financial Times*. Retrieved from <https://www.ft.com/content/8fe7c850-226f-11e6-9d4d-c11776a5124d>
- Roehrs, A., da Costa, C. A., Righi, R. da R., & de Oliveira, K. S. F. (2017). Personal Health Records: A Systematic Literature Review. *Journal of Medical Internet Research*, 19(1), e13. <http://doi.org/10.2196/jmir.5876>
- Sanderson, S. C., Linderman, M. D., Suckiel, S. A., Diaz, G. A., Zinberg, R. E., Ferryman, K., ... Schadt, E. E. (2016). Motivations, concerns and preferences of personal genome sequencing research participants: Baseline findings from the HealthSeq project. *European Journal of Human Genetics*, 24(1), 14-20. <https://doi.org/10.1038/ejhg.2015.118>



- Sankar, P., Mora, S., Merz, J. F., & Jones, N. L. (2003). Patient perspectives of medical confidentiality: a review of the literature. *Journal of General Internal Medicine*, 18(8), 659-69. <https://doi.org/10.1046/j.1525-1497.2003.20823.x>
- Scheuner, M. T., de Vries, H., Kim, B., Meili, R. C., Olmstead, S. H., & Teleki, S. (2009). Are electronic health records ready for genomic medicine? *Genetics in Medicine*, 11(7), 510-517. <https://doi.org/10.1097/GIM.0b013e3181a53331>
- Schriver, R. R. (2001). You Cheated, You Lied: The Safe Harbor Agreement and its Enforcement by the Federal Trade Commission. *Fordham L. Rev.*, 70(6), 2777. Retrieved from [http://heinonlinebackup.com/hol-cgi-bin/get\\_pdf.cgi?handle=hein.journals/flr70&section=124](http://heinonlinebackup.com/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/flr70&section=124)
- Schwartz, P. M., & Reidenberg, J. R. (1996). *Data privacy law : a study of United States data protection*. Michie. Retrieved from <https://dl.acm.org/citation.cfm?id=547489>
- SGK plan to sell health data to global pharma creates controversy. (2012). *Cihan Haber Ajansi*. Retrieved from <https://www.cihan.com.tr/en/sgk-plan-to-sell-health-data-to-global-pharma-creates-controversy-863135.htm>
- Sherwin, S., & Simpson, C. (1999). Ethical Questions in the Pursuit of Genetic Information. In *Genetic Information* (pp. 121-128). Boston, MA: Springer US. [https://doi.org/10.1007/978-0-585-34586-4\\_11](https://doi.org/10.1007/978-0-585-34586-4_11)
- Shoenbill, K., Fost, N., Tachinardi, U., & Mendonca, E. A. (2014). Genetic data and electronic health records: a discussion of ethical, logistical and technological considerations. *Journal of the American Medical Informatics Association*, 21(1), 171-180. <https://doi.org/10.1136/amiajnl-2013-001694>
- Sikka, N., Carlin, K. N., Pines, J., Pirri, M., Strauss, R., & Rahimi, F. (2012). The use of mobile phones for acute wound care: Attitudes and opinions of emergency department patients. *Journal of Health Communication*, 17(SUPPL. 1), 37-43. <https://doi.org/10.1080/10810730.2011.649161>
- Smith, E., & Eloff, J. H. . (1999). Security in health-care information systems—current trends. *International Journal of Medical Informatics*, 54(1), 39-54. [https://doi.org/10.1016/S1386-5056\(98\)00168-3](https://doi.org/10.1016/S1386-5056(98)00168-3)
- Sommerville, A., & English, V. (1999). Genetic privacy: orthodoxy or oxymoron? *Journal of Medical Ethics*, 25, 144-150. <https://doi.org/10.1136/jme.25.2.144>
- Spradley, J. (1979). *The Ethnographic Interview*. New York, NY: Holt, Rinehart and Winston.
- Statista. (2017). *Projected total global mHealth devices and services revenue from 2014 to 2020 (in billion U.S. dollars)*. Statista - The Statistics Portal. Retrieved from <https://www.statista.com/statistics/628190/global-mhealth-devices-and-services-revenue-worldwide/>
- Sweeney, L., Abu, A., & Winn, J. (2013). Identifying Participants in the Personal Genome Project by Name (A Re-identification Experiment). Retrieved from

<http://arxiv.org/abs/1304.7605>

- T.C. Danistay Onbesinci Daire. Sağlık Bakanlığı'nın 05.02.2015 günlü e-Nabız Projesi konulu Genelgesinin iptali ve yürütmesinin durdurulması (2015). Retrieved from [http://www.ttb.org.tr/images/stories/haberler/file/danistay\\_10\\_daire\\_2015\\_karar.pdf](http://www.ttb.org.tr/images/stories/haberler/file/danistay_10_daire_2015_karar.pdf)
- Tait, R. (2016). Personal details of 50 million Turkish citizens leaked online, hackers claim. Retrieved from <http://www.telegraph.co.uk/news/2016/04/04/personal-details-of-50-million-turkish-citizens-leaked-online-ha/>
- Türk Dişhekimleri Birliği. (2016). Bakanlık Yine Sağlık Verilerini İstiyor; 'Hastalar bilgilendirilmeli, rıza göstermeyenlerin bilgileri sır kapsamında korunmalıdır'. Retrieved February 17, 2018, from [http://www.tdb.org.tr/icerik\\_yazdir.php?Id=2652](http://www.tdb.org.tr/icerik_yazdir.php?Id=2652)
- Williams, J. (2010, May). Social networking applications in health care: threats to the privacy and security of health information. In *Proceedings of the 2010 ICSE workshop on software engineering in health care* (pp. 39-49). ACM.
- Wingo, P., Higgins, J. E., Rubin, G. L., Zahniser, S. C., WHO Special Programme of Research, D. and R. T. in H. R., (U.S.), C. for D. C., & International, F. H. (1994). *An Epidemiologic approach to reproductive health / Centers for Disease Control, U.S.A., Family Health International, World Health Organization*. Geneva: World Health Organization.
- Wooten, R., Klink, R., Sinek, F., Bai, Y., & Sharma, M. (2012, May). Design and implementation of a secure healthcare social cloud system. In *Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (ccgrid 2012)* (pp. 805-810). IEEE Computer Society.
- Yoo, C., Kang, B. T., & Kim, H. K. (2015). Case study of the vulnerability of OTP implemented in internet banking systems of South Korea. *Multimedia Tools and Applications*, 74(10), 3289-3303.
- Zhang, R., & Liu, L. (2010). Security models and requirements for healthcare application clouds. *Proceedings - 2010 IEEE 3rd International Conference on Cloud Computing, CLOUD 2010*, 268-275. <https://doi.org/10.1109/CLOUD.2010.62>
- Beer, R. (2000). Dynamical approaches to cognitive science. *Trends in Cognitive Sciences*, 4(3), 91-99.
- Bernoulli, D. (1954). Exposition of a new theory on the measurement of risk - Originally published in 1738; translated by Dr. Louise Sommer. *Econometrica: Journal of the Econometric Society*, 23-36.
- Blais, A. R., & Weber, E. U. (2006). A Domain-specific risk-taking (DOSPERT) scale for adult populations. *Judgment and Decision Making*, 1, 33-47.

- Blakemore, S. J., & Robbins, T. W. (2012). Decision making in the adolescent brain. *Nature Neuroscience, 15*, 1184-1191.
- Bradley, M. M., Miccoli, L., Escrig, M. A., & Lang, P. J. (2008). The pupil as a measure of emotional arousal and autonomic activation. *Psychophysiology, 45*(4), 602-607.
- Breiter, H. C., Aharon, I., Kahneman, D., Dale, A., & Shizgal, P. (2001). Functional imaging of neural responses to expectancy and experience of monetary gains and losses. *Neuron, 30*(2), 619-639.
- Buelow, M. T., & Suhr, J. A. (2013). Personality characteristics and state mood influence individual deck selections on the Iowa Gambling Task. *Personality and Individual Differences, 54*(5), 593-597.
- Busemeyer, J. R., & Johnson, J. G. (2005). Computational models of decision making. In D. Koehler, & N. Harvey (Eds.), *Blackwell Handbook of Judgment and Decision Making* (pp. 133-154). London: Wiley-Blackwell.
- Camerer, C. (1999). Behavioral economics: Reunifying psychology and economics. *Proceedings of the National Academy of Sciences of the United States of America, 96*(19), 10575-10577.
- Camerer, C. F., & Loewenstein, G. (2004). Behavioral economics: past, present, future. In C. F. Camerer, G. Loewenstein, & M. Rabin (Eds.), *Advances in Behavioral Economics* (pp. 3-51). New York: Princeton University Press.
- Caplin, A., & Dean, M. (2009). Dopamine, reward prediction error, and economics. *Quarterly Journal of Economics, 123*(2), 663-701.
- Cavanagh, J. F., Wiecki, T. V., Kochar, A., & Frank, M. J. (2014). Eye tracking and pupillometry are indicators of dissociable latent decision processes. *Journal of Experimental Psychology: General, 143*(4), 1476-1488.
- Cessac, B. (2010). A view of neural networks as dynamical systems. *International Journal of Bifurcation and Chaos, 20*(6), 1585-1629.
- Chiu, Y. C., Lin, C. H., T, H. J., Lin, S., Lee, P. L., & Hsieh, J. C. (2008). Immediate gain is long-term loss: Are there foresighted decision makers in the Iowa Gambling Task? *Behavioral and Brain Functions, 4*(1), 13-22.
- Clark, L., Lawrence, A., Astley-Jones, F., & Gray, N. (2009). Gambling near-misses enhance motivation to gamble and recruit win-related brain circuitry. *Neuron, 61*(3), 481-490.

- Critchley, H., Mathias, C., & Dolan, R. (2001). Neural Activity in the Human Brain Relating to Uncertainty and Arousal during Anticipation. *Neuron*, 29(2), 537-545.
- Damasio, A., Everitt, B., & Bishop, D. (1996). The somatic marker hypothesis and the possible functions of the prefrontal cortex. *Philosophical Transactions of the Royal Society B: Biological Sciences*, 351(1346), 1413-1420.
- de Gee, J. W., Knapen, T., & Donner, T. H. (2014). Decision-related pupil dilation reflects upcoming choice and individual bias. *Proceedings of the National Academy of Sciences of USA*, 111(5), 618-625.
- de Vries, M., Holland, R. W., & Witteman, C. L. (2008). Fitting decisions: Mood and intuitive versus deliberative decision strategies. *Cognition and Emotion*, 22(5), 931-943.
- Duchowski, A. (2007). *Eye Tracking Methodology: Theory and Practice* (2 ed.). Springer.
- Edwards, W., & Fasolo, B. (2001). Decision technology. *Annual Review of Psychology*, 52, 581-606.
- Einhäuser, W., Koch, C., & Carter, L. O. (2010). Pupil dilation betrays the timing of decisions. *Frontiers Human Neuroscience*, 4:18.
- Einhäuser, W., Stout, J., Koch, C., & Carter, O. (2008). Pupil dilation reflects perceptual selection and predicts subsequent stability in perceptual rivalry. *Proceedings of the National Academy of Sciences of the United States of America*, 105(5), 1704-1709.
- Ellsberg, D. (1961). Risk, ambiguity, and the savage axioms. *Quarterly Journal of Economics*, 75(4), 643-669.
- Ernst, M., & Paulus, M. P. (2005). Neurobiology of Decision Making: A Selective Review from a Neurocognitive and Clinical Perspective. *Biological Psychiatry*, 58(8), 597-604.
- Eshel, N., Nelson, E. E., Blair, R. J., Pine, D. S., & Ernst, M. (2007). Neural substrates of choice selection in adults and adolescents: development of the ventrolateral prefrontal and anterior cingulate cortices. *Neuropsychologia*, 45(6), 1270-1279.
- Evans, J. S., Barston, J. L., & Pollard, P. (1983). On the conflict between logic and belief in syllogistic reasoning. *Memory & Cognition*, 11(3), 295-306.

- Eysenck, S. B., Pearson, P. R., G, E., & Allsopp, J. F. (1985). Age norms for impulsiveness, venturesomeness and empathy in adults. *Personality and Individual Differences*, 6(5), 613-619.
- Fecteau, S., Knoch, D., Fregni, F., Sultani, N., Boggio, P., & Pascual-Leone, A. (2007). Diminishing Risk-Taking Behavior by Modulating Activity in the Prefrontal Cortex: A Direct Current Stimulation Study. *The Journal of Neuroscience*, 27(46), 12500-12505.
- Fellows, L. K. (2004). The cognitive neuroscience of human decision making: a review and conceptual framework. *Behav Cogn Neurosci Rev*, 3(3), 159-172.
- Fiedler, S., & Glöckner, A. (2012). The dynamics of decision making in risky choice: An eye-tracking analysis. *Frontiers in Psychology*, 3(335).
- Figner, B., & Weber, E. (2011). Who takes risks when and why? Determinants of risk taking. *Current Directions in Psychological Science*, 20(4), 211-216.
- Figner, B., Knoch, D., Johnson, E., Krosch, A., Lisanby, S., Fehr, E., & Weber, E. (2010). Lateral prefrontal cortex and self-control in intertemporal choice. *Nature Neuroscience*, 13(5), 538-539.
- Figner, B., MacKinlay, R., Wilkening, F., & Weber, E. (2009). Affective and deliberative processes in risky choice: Age differences in risk taking in the Columbia Card Task. *Journal of Experimental Psychology: Learning, Memory, and Cognition*, 35(3), 709-730.
- Finucane, M. L., Mertz, C. K., Slovic, P., & Schmidt, E. S. (2005). Task complexity and older adults' decision-making competence. *Psychology and Aging*, 20(1), 71-84.
- Geangu, E., Hauf, P., Bhardwaj, R., & Bentz, W. (2011). Infant pupil diameter changes in response to others' positive and negative emotions. *PLoS ONE*, 6(11), 1-10.
- Glimcher, P. W., & Fehr, E. (2013). *Neuroeconomics: Decision Making and the Brain* (2 ed.). Academic Press.
- Glimcher, P. W., & Rustichini, A. (2004). Neuroeconomics: the consilience of brain and decision. *Science*, 306(5695), 447-452.
- Glöckner, A., & Herbold, A. (2011). An eye-tracking study on information processing in risky decisions: Evidence for compensatory strategies based on automatic processes. *Journal of Behavioral Decision Making*, 24(1), 71-98.
- Gupta, R., Koscik, T., Bechara, A., & Tranel, D. (2011). The amygdala and decision-making. *Neuropsychologia*, 49(4), 760-766.

- Haken, H., Kelso, J., & Bunz, H. (1985). A theoretical model of phase transitions in human hand movements. *Biological Cybernetics*, *51*(5), 347-356.
- Hakerem, G. (1967). Pupillography. In P. H. VENABLES, & I. MARTIN (Eds.), *A Manual of Psychophysiological Methods* (pp. 335-349). Amsterdam: North-Holland Publishing Co.
- Harlé, K. M., Chang, L. J., van 't Wout, M., & Sanfey, A. G. (2012). The neural mechanisms of affect infusion in social economic decision-making: A mediating role of the anterior insula. *NeuroImage*, *61*(1), 32-40.
- Hooper, C. J., Luciana, M., & Conklin, H. M. (2004). Adolescents' performance on the Iowa Gambling Task: implications for the development of decision making and ventromedial prefrontal cortex. *Developmental Psychology*, *40*(6), 1148-1158.
- Hsu, M., Bhatt, M., Adolphs, R., Tranel, D., & Camerer, C. F. (2005). Neural systems responding to degrees of uncertainty in human decision-making. *Science*, *310*(5754), 1680-1683.
- Huettel, S. A., Stowe, C. J., Gordon, E. M., Warner, B. T., & Platt, M. L. (2006). Neural signatures of economic preferences for risk and ambiguity. *Neuron*, *49*(5), 765-775.
- Jepma, M., & Nieuwenhuis, S. (2011). Pupil diameter predicts changes in the exploration-exploitation trade-off: Evidence for the adaptive gain theory. *Journal of Cognitive Neuroscience*, *23*(7), 1587-1596.
- Jones, C., & Sutherland, J. (2008). Acoustic emotion recognition for affective computer gaming. In C. Peter, & R. Beale (Eds.), *Affect and Emotion in Human-Computer Interaction* (Vol. 4868). Heidelberg, Germany: Springer.
- Juliusson, E. A., Karlsson, N., & Garling, T. (2005). Weighing the past and the future in decision making. *European Journal of Cognitive Psychology*, *17*(4), 561-575.
- Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, *47*(2), 263-291.
- Kang, O., & Wheatley, T. (2015). Pupil dilation patterns reflect the contents of consciousness. *Consciousness and Cognition*, *35*, 128-135.
- Kelso, J., & Zanone, P. (2002). Coordination dynamics of learning and transfer across different effector systems. *Journal of Experimental Psychology: Human Perception and Performance*, *28*(4), 776-797.

- Klinger, J., Kumar, R., & Hanrahan, P. (2008). Measuring the task-evoked pupillary response with a remote eye tracker. *Proceedings of the 2008 symposium on Eye tracking research & applications*, 69-72.
- Kloosterman, N. A., Meindertsma, T., Loon, A. M., Lamme, V. A., Bonnef, Y. S., & Donner, T. H. (2015). Pupil size tracks perceptual content and surprise. *European Journal of Neuroscience*, 41(8), 1068-1078.
- Knoch, D., Gianotti, L. R., Pascual-Leone, A., Treyer, V., Regard, M., Hohmann, M., & Brugger, P. (2006). Disruption of Right Prefrontal Cortex by Low-Frequency Repetitive Transcranial Magnetic Stimulation Induces Risk-Taking Behavior. *The Journal of neuroscience: the official journal of the Society for Neuroscience*, 26(24), 6469-6472.
- Kovalchik, S., Camerer, C. F., Grether, D. M., Plott, C. R., & Allman, J. M. (2005). Aging and decision making: a comparison between neurologically healthy elderly and young individuals. *Journal of Economic Behavior & Organization*, 58(1), 79-94.
- Kuhnen, C., & Knutson, B. (2005). The neural basis of financial risk taking. *Neuron*, 47, 763-770.
- Lauriola, M., Panno, A., Levin, I. P., & Lejuez, C. W. (2014). Individual differences in risky decision making: A meta-analysis of sensation seeking and impulsivity with the Balloon Analogue Risk Task. *Journal of Behavioral Decision Making*, 27(1), 20-36.
- Lejuez, C. W., Aklin, W. M., Zvolensky, M. J., & Pedulla, C. M. (2003). Evaluation of the Balloon Analogue Risk Task (BART) as a predictor of adolescent real-world risk-taking behaviours. *Journal of Adolescence*, 26(4), 475-479.
- Lejuez, C., Read, P. J., Kahler, W. C., Richards, J. B., Ramsey, E. S., Stuart, L. G., . . . Brown, A. R. (2002). Evaluation of a behavioral measure of risk taking: The Balloon Analogue Risk Task (BART). *Journal of Experimental Psychology: Applied*, 8(2), 75-84.
- Lerner, J. S., Li, Y., Valdesolo, P., & Kassam, K. S. (2015). Emotion and decision making. *Annual Review of Psychology*, 66, 799-823.
- Lighthall, N. R., Sakaki, M., Vasunilashorn, S., Nga, L., Somayajula, S., Chen, E. Y., . . . Mather, M. (2012). Gender differences in reward-related decision processing under stress. *Social Cognitive and Affective Neuroscience*, 7(4), 476-484.
- Lin, C. H., Chiu, Y. C., Lee, P. L., & Hsieh, J. C. (2007). Is deck B a disadvantageous deck in the Iowa gambling task? *Behavioral and Brain Functions*, 3(1), 16-25.

- Loewenstein, G., & Lerner, J. S. (2003). The role of affect in decision making. In R. J. Davidson, K. R. Sherer, & H. H. Goldsmith (Eds.), *Handbook of Affective Sciences* (pp. 619-642). Oxford: Oxford University Press.
- Loewenstein, G., Rick, S., & Cohen, J. D. (2008). Neuroeconomics. *Annual Review of Psychology*, *59*, 647-672.
- Loewenstein, G., Weber, E., Hsee, C., & Welch, N. (2001). Risk as feelings. *Psychological Bulletin*, *127*(2), 267-286.
- Macmillan, M. (2000). Restoring Phineas Gage: A 150th retrospective. *Journal of the History of the Neurosciences*, *9*(1), 46-66.
- Maia, T., & McClelland, J. (2004). A reexamination of the evidence for the somatic marker hypothesis: What participants really know in the Iowa gambling task. *Proceedings of the National Academy of Sciences of the United States of America*, *101*(45), 16075-16080.
- Maia, T., & McClelland, J. (2005). The somatic marker hypothesis: Still many questions but no answers. *Trends in Cognitive Sciences*, *9*(4), 162-164.
- Marcus, B. (2003). An empirical examination of the construct validity of two alternative self-control measures. *Educational and Psychological Measurement*, *63*(4), 674-706.
- Marx, S., & Einhäuser, W. (2015). Reward modulates perception in binocular rivalry. *Journal of Vision*, *15*(1), 1-13.
- Marx, S., Gruenhage, G., Walper, D., Rutishauser, U., & Einhäuser, W. (2015). Competition with and without priority control: Linking rivalry to attention through winner-take-all networks with memory. *Annals of the New York Academy of Sciences*, *1339*(1), 138-153.
- Moretto, G., Ladavas, E., Mattioli, F., & di Pellegrino, G. (2010). A psychophysiological investigation of moral judgment after ventromedial prefrontal damage. *Journal of Cognitive Neuroscience*, *22*(8), 1888-1899.
- Morris, G., Nevet, A., Arkadir, D., Vaadia, E., & Bergman, H. (2006). Midbrain dopamine neurons encode decisions for future action. *Nature Neuroscience*, *9*(8), 1057-1063.
- Murphy, P. R., O'Connell, R. G., O'Sullivan, M., Robertson, I. H., & Balsters, J. H. (2014). Pupil diameter covaries with BOLD activity in human locus coeruleus. *Human Brain Mapping*, *35*(8), 4140-4154.



- Nicholson, N., Soane, E., Fenton-O'Creevy, M., & Willman, P. (2005). Personality and domain-specific risk taking. *Journal of Risk Research*, 8(2), 157-176.
- Orquin, J. L., & Mueller Loose, S. (2013). Attention and choice: a review on eye movements in decision making. *Acta Psychologica*, 144(1), 190-206.
- Orquin, J. L., Bagger, M. P., & Mueller Loose, S. (2013). Learning affects top down and bottom up modulation of eye movements in decision making. *Judgment and Decision Making*, 8(6), 700-716.
- Panno, A., Lauriola, M., & Figner, B. (2013). Emotion regulation and risk taking: Predicting risky choice in deliberative decision making. *Cognition and Emotion*, 27(2), 326-334.
- Partala, T., & Surakka, V. (2003). Pupil size variation as an indication of affective processing. *International Journal of Human-Computer Studies*, 59(1), 185-198.
- Paulus, M. P. (2005). Neurobiology of decision-making: quo vadis? *Cognitive Brain Research*, 23(1), 2-10.
- Payzan-LeNestour, E., Dunne, S., Bossaerts, P., & O'Doherty, J. P. (2013). The neural representation of unexpected uncertainty during value-based decision making. *Neuron*, 79(1), 191-201.
- Peter, C., & Beale, R. (2008). *Affect and Emotion in Human-Computer Interaction*. Heidelberg: Springer.
- Phelps, E. A., Lempert, K. M., & Sokol-Hessner, P. (2014). Emotion and decision making: multiple modulatory neural circuits. *Annual Review of Neuroscience*, 37, 263-287.
- Platt, M. L., & Huettel, S. A. (2008). Risky business: the neuroeconomics of decision making under uncertainty. *Nature Neuroscience*, 11, 398-403.
- Plous, S. (1993). *The Psychology of Judgment and Decision Making*. McGraw-Hill series in social psychology. McGraw-Hill.
- Preuschoff, K., Hart, B. M., & Einhäuser, W. (2011). Pupil dilation signals surprise: evidence for noradrenaline's role in decision making. *Front. Neuroscience*, 5(115). doi:10.3389/fnins.2011.00115
- Privitera, C. M., Carney, T., Klein, S., & Aguilar, M. (2014). Analysis of microsaccades and pupil dilation reveals a common decisional origin during visual search. *Vision Research*, 95, 43-50.

- Rabiner, L., & Juang, B. H. (1986). An introduction to hidden Markov models. *ASSP Magazine, IEEE*, 3(1), 4-16.
- Rao, H., Korczykowski, M., Pluta, J., Hoang, A., & Detre, J. (2008). Neural correlates of voluntary and involuntary risk taking in the human brain: An fMRI Study of the Balloon Analog Risk Task (BART). *Neuroimage*, 42(2), 902-910.
- Ratcliff, R. (1978). A theory of memory retrieval. *Psychological Review*, 85(2), 59-108.
- Ratcliff, R., & McKoon, G. (2008). The diffusion decision model: theory and data for two-choice decision tasks. *Neural Computation*, 20(4), 873-922.
- Rayner, K., Pollatsek, A., Ashby, J., & Clifton, C. (2011). *Psychology of Reading* (2 ed.). Psychology Press.
- Reid, R. (1986). The psychology of the near miss. *Journal of Gambling Behavior*, 2(1), 32-39.
- Reimann, M., & Bechara, A. (2010). The somatic marker framework as a neurological theory of decision-making: Review, conceptual comparisons, and future neuroeconomics research. *Journal of Economic Psychology*, 31(5), 767-776.
- Rogers, R. D., Owen, A. M., Middleton, H. C., Williams, E. J., Pickard, J. D., Sahakian, B. J., & Robbins, T. W. (1999). Choosing between small, likely rewards and large, unlikely rewards activates inferior and orbital prefrontal cortex. *The Journal of neuroscience: the official journal of the Society for Neuroscience*, 19(20), 9029-9038.
- Rolfs, M. (2009). Microsaccades: Small steps on a long way. *Vision Research*, 49(20), 2415-2441.
- Ruff, C. C., & Huettel, S. A. (2013). Experimental Methods in Cognitive Neuroscience. In P. W. Glimcher, & E. Fehr (Eds.), *Neuroeconomics: Decision Making and the Brain* (2 ed., pp. 77-108). Academic Press.
- Rustichini, A. (2009). Neuroeconomics: what have we found, and what should we search for. *Current Opinion in Neurobiology*, 19(6), 672-677.
- Sanfey, A. G., & Chang, L. J. (2008). Multiple systems in decision making. *Annals of the New York Academy of Sciences*, 1128, 53-62.
- Schonberg, T., Fox, C., & Poldrack, R. (2011). Mind the gap: bridging economic and naturalistic risk-taking with cognitive neuroscience. *Trends in Cognitive Sciences*, 15(1), 11-19.

- Shah, A. K., & Oppenheimer, D. M. (2008). Heuristics made easy: An effort-reduction framework. *Psychological Bulletin*, *134*(2), 207-222.
- Shen, L., Wang, M., & Shen, R. (2009). Affective e-Learning: Using "emotional" data to improve learning in pervasive learning environment. *Journal of Educational Technology & Society*, *12*(2), 176-189.
- Simpson, H. M., & Hale, S. M. (1969). Pupillary changes during a decision making task. *Perceptual and Motor Skills*, *29*, 495-498.
- Sitkin, S. B., & Weingart, L. R. (1995). Determinants of risky decision-making behavior: A test of the mediating role of risk perceptions and propensity. *Academy of Management Journal*, *38*(6), 1573-1592.
- Smith, D. G., Xiao, L., & Bechara, A. (2012). Decision making in children and adolescents: impaired Iowa Gambling Task performance in early adolescence. *Developmental Psychology*, *48*(4), 1180-1187.
- Sykes, J. (2010). Affective games: How iOpiates elicit an emotional fix. In D. Gökçay, & G. Yıldırım (Eds.), *Affective Computing and Interaction: Psychological, Cognitive and Neuroscientific Perspectives* (pp. 344-358). New York: IGI Global.
- Taskin, K., & Gokcay, D. (2015). Investigation of Risk Taking Behavior and Outcomes in Decision Making with Modified BART (m-BART). *Affective Computing and Intelligent Interaction*. Xi'an: The Association for the Advancement of Affective Computing.
- Taskin, K., & Gokcay, D. (2016). Temporal aspects of decision making: Pupillary responses reveal alternating levels of arousal related to dynamic risk-taking states. *International Journal of Human Computer Interactions*.
- Tobler, P., Christopoulos, G., O'Doherty, J., Dolan, R., & Schultz, W. (2009). Risk-dependent reward value signal in human prefrontal cortex. *Proceedings of the National Academy of Sciences*, *106*(17), 7185-7190.
- Tversky, A., & Kahneman, D. (1992). Advances in prospect theory: Cumulative representation of uncertainty. *Journal of Risk and Uncertainty*, *5*(4), 297-323.
- van Gelder, T. (1998). The dynamical hypothesis in cognitive science. *Behavioral and Brain Sciences*, *21*(5), 615-665.
- von Neumann, J., Morgenstern, O., Kuhn, H. W., & Rubinstein, A. (2007). *Theory of Games and Economic Behavior* (60th Anniversary Commemorative ed.). Princeton University Press.

- Wakker, P. (2010). *Prospect Theory: For Risk and Ambiguity*. Cambridge University Press.
- Wakker, P., & Fennema, H. (1997). Original and cumulative prospect theory: a discussion of empirical differences. *Journal of behavioral decision making*, *10*(10), 53-64.
- Wallsten, T. S., Pleskac, T. C., & Lejuez, C. W. (2005). Modeling behavior in a clinically diagnostic sequential risk-taking task. *Psychological Review*, *112*(4), 862-880.
- Weber, E. U., Blais, A. R., & Betz, N. (2002). A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors. *Journal of Behavioral Decision Making*, *15*, 263-290.
- Weber, E., & Johnson, E. (2008). Decisions under Uncertainty: Psychological, Economic, and Neuroeconomic Explanations of Risk Preference. In P. Glimcher, E. Fehr, C. Camerer, & A. Poldrack (Eds.), *Neuroeconomics: Decision Making and the Brain* (pp. 127-144). London: Academic Press.
- Weller, J. A., Levin, I. P., Shiv, B., & Bechara, A. (2007). Neural correlates of adaptive decision making for risky gains and losses. *Psychological science: a journal of the American Psychological Society*, *18*(11), 958-964.
- West, R. F., Toplak, M. E., & Stanovich, K. E. (2008). Heuristics and biases as measures of critical thinking: Associations with cognitive ability and thinking dispositions. *Journal of Educational Psychology*, *100*(4), 930-941.
- White, T. L., Lejuez, C. W., & de Wit, H. (2008). Test-retest characteristics of the Balloon Analogue Risk Task (BART). *Experimental and Clinical Psychopharmacology*, *16*(6), 565-570.
- Wu, G., Zhang, J., & Gonzalez, R. (2005). Decision under risk. In D. Koehler, & N. Harvey (Eds.), *Blackwell Handbook of Judgment and Decision Making* (pp. 299-423). London: Wiley-Blackwell.
- Yu, A. J., & Dayan, P. (2005). Uncertainty, neuromodulation, and attention. *Neuron*, *46*(4), 681-692.
- Zak, P. J. (2004). Neuroeconomics. *Philosophical Transactions of the Royal Society B: Biological Sciences*, *359*(1451), 1737-1748.
- Zeelenberg, M. (1999). Anticipated regret, expected feedback and behavioral decision making. *Journal of Behavioral Decision Making*, *12*(2), 93-106.

Zuckerman, M. (1994). *Behavioral expressions and biosocial bases of sensation seeking*. Cambridge: Cambridge University Press.



## APPENDICES

### APPENDIX A

#### APPROVAL LETTER OF THE PRACTICAL ETHICS RESEARCH BOARD

UYGULAMALI ETİK ARAŞTIRMA MERKEZİ  
APPLIED ETHICS RESEARCH CENTER



DUMLUPINAR BULVARI 06500  
ÇANKAYA ANKARA/TURKEY  
T: +90 312 210 22 91  
F: +90 312 210 79 59  
ueam@metu.edu.tr  
www.ueam.metu.edu.tr

Sayı: 28620816/10-6

07.01.2015

Gönderilen : Y. Doç. Dr. Yeşim Aydın Son  
Enformatik Enstitüsü  
Sağlık Bilişimi

Gönderen : Prof. Dr. Canan Sümer  
IAK Başkanı Vekili

İlgi : Etik Onayı

Danışmanlığını yapmış olduğunuz Tıp Bilişimi Bölümü öğrencisi  
Özlem Özkan'ın "İnternet Bankacılığında Kullanılan Güvenlik  
Korumalarının Bulut PHR'a Adaptasyonu" isimli araştırması "İnsan  
Araştırmaları Komitesi" tarafından uygun görülerek gerekli onay  
verilmiştir.

Bilgilerinize saygılarımla sunarım.

Etik Komite Onayı

Uygundur

07/01/2015

Prof.Dr. Canan Sümer  
Uygulamalı Etik Araştırma Merkezi  
(UEAM) Başkanı Vekili  
ODTÜ 06531 ANKARA

## APPENDIX B

### EXAMPLE OF PARTICIPANT CONSENT

#### **İnternet Bankacılığı Güvenlik Önlemleri ve Sağlıkta Bilgi Güvenliği Anketi**

Bu çalışma, araştırma görevlisi ve Tıp Bilişimi Bölümü doktora öğrencisi Özlem ÖZKAN tarafından, ODTÜ’de yürütülen bir doktora tezi kapsamında hazırlanmış ve ODTÜ Uygulamalı Etik Araştırma Merkezi (UEAM) tarafından incelenip, 7 Ocak 2015 tarihinde onaylanmıştır. Anket önlü arkalı 3 sayfa ve 26 sorudan oluşmaktadır. Çalışmanın amacı internet bankacılığı güvenlik önlemlerinin, bilgi güvenliği açısından ne kadar güvenilir görüldüğünü ve sağlık alanına uygulanabilirliğini ölçmektir. Çalışmaya katılım tamamiyle gönüllülük esastır ve kişisel herhangi bir bilgi istenmemektedir. Ankete verdiğiniz yanıtlar sadece araştırmacılar tarafından değerlendirilecek, elde edilecek bilgiler bilimsel yayınlarda kullanılacaktır.

Çalışma, genel olarak kişisel rahatsızlık verecek soruları içermemektedir. Ancak, katılım sırasında sorulardan ya da herhangi başka bir nedenden ötürü kendinizi rahatsız hissederseniz cevaplamayı yarıda bırakabilirsiniz. Böyle bir durumda (varsa) çalışmayı uygulayan kişiye, çalışmayı tamamlamadığınızı söylemeniz yeterli olacaktır. Çalışma sonunda, bu çalışmayla ilgili sorularınız varsa iletişim adresleri vasıtasıyla cevaplanacaktır.

Çalışma hakkında daha fazla bilgi almak için Eğitim Fakültesi araştırma görevlisi Özlem ÖZKAN (ODTÜ Eğitim Fakültesi Oda: EF21, Tel: +90312 210 4186, E-posta: oozkan@metu.edu.tr) ya da öğretim üyesi Doç. Dr. Yeşim AYDIN SON (Oda: B-207, Tel: +90312 210 7708, E-posta: yesim@metu.edu.tr) ile iletişim kurabilirsiniz. Bu çalışmaya katıldığınız için teşekkür ederiz.

**“Bu çalışmaya tamamen gönüllü olarak katılıyorum ve istediğim zaman yarıda kesip çıkabileceğimi biliyorum. Verdiğim bilgilerin bilimsel amaçlı yayınlarda kullanılmasını kabul ediyorum.”**



## APPENDIX C

### THE SURVEY QUESTIONS IN ENGLISH

1. The city you live in: .....
2. Your birth year: .....
3. Gender:
4. Your educational status:
5. Income:
6. What can you say about your computer skills?
7. What can you say for your smartphone skills?
8. Which of the following security protections have you previously used?
9. Have you ever used online banking service until now?
10. If yes, indicate for which bank or banks:
11. Do you find the security measures of internet banking sufficient for the security of your information?
12. Have you ever faced a negative situation without your approval while you were using internet banking?
13. How much information do you have about who can access your current medical records?
14. How much information do you have on genetic science?
15. Did you or a family member have a genetic test before?
16. If "No" is your answer, which of the following options best describes your views on genetic testing?
17. Have you ever experienced a serious breach where your personal health information was used inappropriately or released without your consent?
18. Have you ever decided not to be tested for medical condition because you were concerned that others might out about the results?
19. Have you ever asked a doctor not to write down your health problem in your medical records, or asked the doctor to put a less serious or less embarrassing diagnosis into the record than was actually the condition?
20. Which of the following security measures do you think necessary for the security of an application where you store health and genetic information?

21. Which level of access do you want to give the following people or organization to your health records containing genetic information?
22. How effective do you think the proposed regulations for protecting the confidentiality and privacy of your electronic health records, which contain your genetic information, might be effective?
23. Which of the following information do you want in an application where you store health records for your smartphone?
24. Do you trust the following stakeholders to keep your medical and genetic data private?
25. What do you think about the security risks of storing the following information in a mobile application (mobile application)?
26. If there is something you want to add, you can specify it in this section:

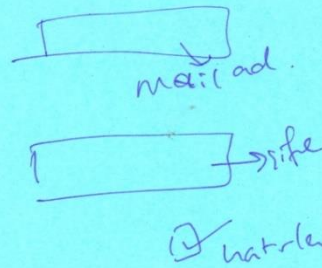
## APPENDIX D

### PAPER PROTOTYPES OF PD WORKGROUP

---

1.

GIRI EKRAMI



Sosyal hesaplar.

Sitremi mutter

Yeni kapt



Kayıt Sayfası

\* Ad - Soyad

\* Doğum Yılı

\* cinsiyet = Kadın

\* mail

\* Şifre

\* Şifre tekrar

→ Aktivasyon YOK X

Okudum, kabul ediyorum

Sözleşme \*

Kayıt

Kayıt  
→ Kayıt Başarısızsa kullanıcıyı bilgilendir  
→ Başarılıysa ona profil sayfasına yönlendir

- kişisel bilgilerimin  
kullanılacağına  
POPUP!

1.2

Profil Oluşturma

Demografik

- kan grubu
- boy + kilo
- eğitim + meslek
- evli + çocuk

Kan Grubu  
A B O → Rh<sup>+</sup>

input (double)

Gesle her öne  
15 yaşında  
kısımları

Drop down  
menu

Bu kadar

Günlük yaşamında  
yeterli aktivite  
orta aktivite  
az aktivite

Yaşam Stili

- Sigara Alkol
- egzersiz

Sigara

- içiyorum
- hiç içmedim
- birlikte

genel olarak  
sigara bilgilendirme  
• Kas yapıcı  
• sigara? istemiyorsanız  
• sigara? istemiyorsanız  
• sigara? istemiyorsanız

Egzersiz 2  
Düzenli egzersiz yapıyor muyuz?

Alkol

- her gün
- hafta da bir
- ayda bir
- hiç içmiyorum

2

# Ana Sayfa

Profil Ayarlar

Anilur menu



Tıbbi ~~kişisel~~ <sup>özgeçmiş</sup>  
→ Hastalıklar  
→ Ameliyathalar  
→ Alerjiler

Teknik Sonuçları  
→ Laboratuvar sonuçları  
→ Görüntüleme sonuçları

İlaçlar  
→ ~~Rapor hatırlatma~~  
→ Rapor hatırlatma  
→ İlaç hatırlatma  
→ İlaç ekle  
→ İlaçlarım

Acil durum Butonu

TAKİM  
17.00  
Aralık  
01.2015

Ana ekrana istediğini koyabilir

Tel:   
\* Ana ekranda  
Tel:   
Acil durum mesajı  
Koruma bilgisi ek

Sms k tarafında bildir  
default mesaj bekleniyor  
→ Randevu hatırlatma  
→ İlaç hatırlatma  
→ Rapor hatırlatma  
→ Koruyucu hekimlikle ilgili hatırlatma  
→ Teknik randevu hatırlatma

Arama  
Masa ih... var  
wm...  
- Kala plardim Komum

Alerji  
- Kan grubu  
- Eran



# Ana Sayfa Devam



Koruyucu  
hekimlik

- Takvim ana sayfadaki takvime bağlantılı
- Kanser Taraması
- ~~Diş~~ Kalp damar hastalıkları taraması
- Göz hastalıkları taraması
- Diş hekimliği ile ilgili taramalar
- Gen- Aşılar
  - ↳ Aşı takvimi bunun altında

- Kan, İller, tansiyon, şeker
- Kilo takibi



Genetik  
Bilgi

- Genetik hastalıklar
- Genetik testler / sonuçlar
  - Kübra örnek getirecek
  - ~~Ma Saygı~~
  - Genetik raporları?

3

# İlaçlar

Reçeteler  
⊕ İlaç Ekle  
→ Rapor Hatırlatma  
→ İlaç Hatırlatma

- Reçeteli ilaç  
- Reçetesiz ilaç

## 3.1 İlaç Ekle

QR Kod  
İlaç (Ekleme Adı) Adı  
Doz: xxx mg  
+ Difer (elle girilebilir)  
Sıklık:   
□ Hatırlatma  
Notlar:

- ### Sıklık
- Haftada bir
  - Günü aşırı
  - 12 saatte 1
  - 6 saatte 1
  - 4 saatte 1
  - Saatte 1
  - Yatmadan önce
  - Sabah
  - Akşam

- If Reçeteli  
□ Raporlu İlaç  
Yenilene Rapor T.  
Rapor S.  
1 yıl  
2 yıl  
1 kaydet

- ### Hatırlatma
- Baslangic T.
  - Baslangic S.
  - Bitis T.
  - Bitis S.
  - Uyarı

### 3.2 İlaçların

İlaç Adı  
Basınca ilaç ekle'den gelen deşaylar  
Düzenle

### Rapor Hatırlatma

İlaç Adı Yenilene T.  
Basınca Rapor T.  
Rapor S.  
Düzenle


### 3.4 İlaç Hatırlatma


İlaç Adı Sıklık  
Basınca Baslangic T.  
" S.  
Bitis T. Düzenle




4

## Tıbbi Örgenmiş

⊕ HASTALIKLAR 

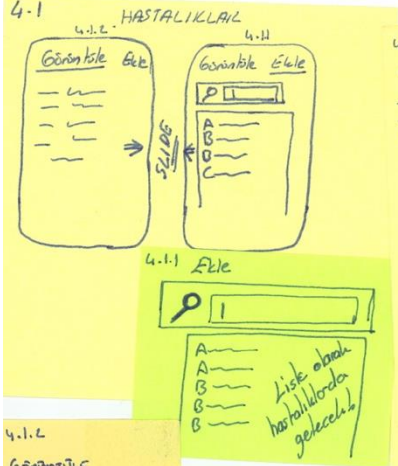
⊕ AMELİYATLAR 

⊕ ALERJİLER 

4.1

# HASTALIKLAR

Doktorları ve hastalarını  
güncel olarak kaydet sonra  
dan direkt gelebilirler.



4.1.1.1

- Tanıyı koyan dr : \_\_\_\_\_

- Tanı konulan hastane \_\_\_\_\_

- Tanı tarihi \_\_\_\_\_

⊕ İLAÇLAR

↳ 3.1'e gönderdik

NOTLAR

- Görüntüle ekle

- Lab sonuç ekle

- Ameliyath

- Kontrol tarihi hatırlat

↳ Takvim / randevu hat-sf

KAYDET

4.1.1.2

Görüntüle

Hastalık 1

2

...

HASTALIK 1 X

- hastalık ekleden  
gelen detaylar  
pop-up olarak  
görüntülenecek.

ICD10 koda hesapla

DÜZETLE!

İster miyiz ?

• Evet 'se

Konuyu hekimlere

Selam, Oberste

Kilo takip  
yapıldı!

4.2

## AMELİYATLAR

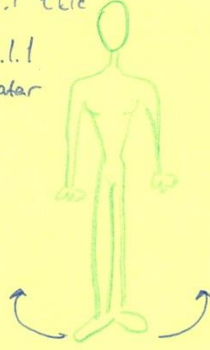
4.2

- Kayar eleren



4.2.1 Elle

4.2.1.1  
Avatar



4.2.1.2

Avatar'dan sonra  
egzen ve konik  
üstteol, eklem  
Cilt

4.2.1.3

Ameliyat Adı

Organ Ameliyatı

Tarih:

Doctor:

Hastane:

Kontrol T.

İlaç Ekle

Notlar:

4.2.2 Görüntüle

- Ameliyat 1

Aslır Pencere

Ameliyat 1

X

Ameliyat eledeki  
gelen detaylar

Detaylar

4.3

# ALERJİLER

4.3  
Kıyer Ekran  
Görüntüle: Ekle

4.3.1 Ekle

Alerjen:

Derece: <sup>1</sup> <sup>2</sup> <sup>3</sup> <sup>4</sup> <sup>5</sup>  
Hafif Orta Orta Orta Orta

Reaksiyon:

Notlar:  İlaç Ekle sayfasına  
yeni ekler

Notlar:

4.3.2 Görüntüle

- Alerji 1

ALERJİ 1   
Ekle'den gelen detaylar

## ⑤ Tetkik Sonuçları

⊕ Sonuç Ekle

- Başlık, tarih  
- Başlık, tarih  
- Başlık, tarih



Başlık  
Tarih  
Sonucun alındığı yer  
Notlar  
Görüntüler (önizleme  
şeklinde)  
☐ ☐ ☐ ☐  
Dizente

5.1

## ⊕ Sonuç Ekle

[Sonuç başlığı]

[Tarih]

[Sonucun alındığı yer]

[Görüntü ekle]

[Notlar]

Görüntü  
ekleye basınca

Galeri  
fotoğraf çek  
Link ekle  
Dosya ekle

②

# Takvim

+

≡ (Listele)

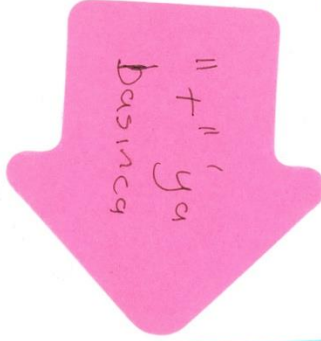
🔍 (Arama)

Ocak 2016 +

1 2 3 4 5 6  
Cumart. Pazart. Salı Çarşamba

Tarihle ötene!  
basınca ↓

Saat Başlık  
Notlar



Başlık   
Tam gün   
Başlangıç

Bitiş

Yinele → Tam saat içinde  
Uyarı → 5 dk  
→ 1 saat  
→ 1 hafta önce gibi

Notlar





# Genetik Bilgi

7.1

ANKET

(Kayıtlı mülki)

7.1

- Kardeş sayısı
- Çocuk sayısı
- Tezde sayısı
- Amca sayısı
- Hala sayısı
- Dayı sayısı

(evlilik otomatik olarak iptal)

7.0

- Bildiğiniz genetik hastalığınız var mı?

search  (+)

- Hiç düşünmüyor musunuz?  
Evet hayır (erkek kadına göre)

7.2 - Soy ağacı oluşturma?

Bu hastalıklardan herhangi birini taşıyan yakınınız var mı?

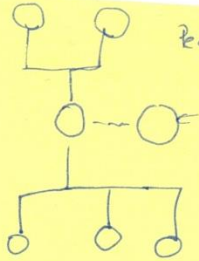
- Diyabet
- Kalp Damar
- Kanser

7.2.5 - Hiç düşünmüyor musunuz?

- evet peşkeş  
BECA

Anne  
Baba  
...  
Dava  
} Liste  
İzlenecek

7.3



- anne
- ~~baba~~
- amca
- kardeş

İhtiyaçları

- hastalıklar
- Değerler



# Genetik Bilgi

7.2

## ~~Sonuç~~ Test Sonuç Ekle

+ Sonuç Ekle

- Başlık, tarih
- Başlık, tarih
- Başlık, tarih
- ...

Herhangi  
birine  
basınca

- Başlık
- Tarih
- Sonuçun alındığı yer
- Notlar
- Görsüntüler (örizleme  
şeklinde)
- □ □ ...
- Düzenle

- Hastalık
- Diaplan test 
  - Kromozom
  - GC
  - Array
  - ...
- Sonuç
- yorum

8

# Sosyal Sayfa

Profil Dizele

Mevcut hastalıklarınızdan  
bu sayfada post etmek istedik-  
lerinizi seçiniz:

\_\_\_\_\_  
 \_\_\_\_\_

(Not: Bu programı kullanırken teferru-  
atları görülmeyecektir)

\_\_\_\_\_ hastalığınızla  
ilgili foruma katılmak  
isteyebilirsiniz?

△ → notifikasyon  
nehi name ile görülebiliyor  
olması !

Ana ekinde  
göster  
Kan grubu  
Kan gruplarının  
burada duyulması

↓  
\_\_\_\_\_ kan vizesi!  
⋮

Ana ekinde  
göster  
Alesjiler

9

## Koruyucu Hekimlik

Genetik ~~bilgi~~ kısmını doldurursanız bu kısmdaki uyarı ve bilgiler sizin için daha doğru bir şekilde sunulacaktır.

UYARI  
Amerikan Aile Hekimleri  
Derneğinin Koruyucu  
2015 Kasım

Hekimlik klavuzuna göre hareket ettirin.  
Bunları uygulamadan önce doktorunuza danışın.

Zaman içerisinde değişebilir.

Bu hastalıklar narin kronik bir hastalığınız var mı?  
(sisteme kayıtlı hastalıklarınızı getir)  
PAPA  
Gebelik var mı?  
Devlet Dınyar

Bana özelliği gösterir

- Göz
  - Diş
  - Kalp Damar
  - Kanser
  - Gebelik
  - Aşılar
  - Testler (CAGE, Oberite, Framingham, FLAX...)
  - +65 testler
- Genel ~~testler~~ <sup>testler</sup>
- Diğer

10

# Doktorlar

Görüntü

Doktorlar

☆☆☆☆☆

☆☆☆☆☆

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

Hikayesi

Doktor

\_\_\_\_\_ detaylı

\_\_\_\_\_

Özellik

etik

Ad Soyad

Bölümü

Hastanesi

11

# Profil Sayfası

Dozenti

Ad Soyad Yaş (D. Terim)  
Cinsiyet  
Kullanıcı Adı (e-mail)  
~~Ad Soyad~~ ~~Yaş~~  
Kan grubu  
Eğitim  
Meslek  
Evlü  çocuk sayısı

Yaşam Stili  
Sigara  
- içi... -  
↳ netip içişim  
Alkol (kas p...)  
- içiyim - - - -  
↳ netip...  
Egzersiz .  
- Dozeli y...  
- Hiç - - -

Şu kısımlara girilen  
Sife var  
- - - - -  
- - - - -  
- - - - -  
- - - - -  
} Altınla  
de  
dahil.

12

ADD to ANASAYFA

Ana başlık 1  
 Alt B. 1  
 Alt B 2  
⋮  
Ana başlık 2  
⋮

## CURRICULUM VITAE

### PERSONAL INFORMATION

**Surname, Name:** ÖZKAN, Özlem

**Date and Place of Birth:** 13/05/1983 – TURKEY

**Marital Status:** Married

**Address:** Grazer Damm 149, 12157 Berlin/GERMANY

**E-mail:** ozlemkan@gmail.com

### EDUCATION

Middle East Technical University, Department of Medical Informatics - Bioinformatics  
PhD Program, Ankara/Turkey (February 2011- July 2018)

*GPA: 3.50 / 4.00 - High Honor Degree*

*Qualification Date: 30 November 2013 on Bioinformatics & Object-Oriented  
Programming Java*

*Thesis: Data Privacy and Security in Genetic Information Included Personal  
Health Record Systems*

COBRA Summer School, San Candido/ Italy

COBRA Workshop on Biological and Chemical IT (September 2012)

*Three weeks summer school program. The Courses: chemical computing,  
molecular computing, bacterial computing, protocell technologies, electronic  
chemical cells and hybrid microfluidic systems*

Middle East Technical University, Department of Medical Informatics

Master Program, Ankara/Turkey (September 2007 - February 2011)

*C.GPA: 3.29 / 4.00 - Honor Degree*

*Thesis: Attitudes and Opinions of People Who Use Medical Services about  
Privacy and Confidentiality of Health Information in Electronic Environment  
(Published also as a Book)*

University of Copenhagen, Department of Computer Science

Master Exchange Program, Copenhagen/Denmark (August 2009 - February 2010)

*One Semester Exchange Program Courses: Programming and IT Design Project*

Middle East Technical University, Department of Computer Education and Instructional  
Technology

Bachelor Program, Ankara/Turkey (September 2002 - June 2007)

*Graduation Date: June 2007 C.GPA: 3.11 / 4.00 - Honor Degree*

## **WORK EXPERIENCE**

Middle East Technical University, Faculty of Education, Ankara (October 2007 – July 2017)

Research Assistant of Computer Center: Responsible for network infrastructure and server admin

DKFZ - German Cancer Research Center, Heidelberg, Germany (June - August 2013)

Intern: Responsible for development of an application on methylation analysis

Middle East Technical University, Graphic Design Office, Ankara (November 2006 - August 2007)

Designer

Middle East Technical University, Computer Center, Ankara (March 2004 - March 2006)

Computer Laboratory Assistant (User Support Group)

## **BOOK**

Özkan, Ö., Saka, O., A., Arifoğlu (2011). Attitudes of People Who Use Medical Services about Privacy of EHR: Opinions on Privacy and Confidentiality of Health Information in Electronic Environment

**Germany: LAMBERT. ISBN 978-3-8454-1772-1**

## **ORAL PRESENTATIONS**

Özkan, Ö. Focus Group Meetings: Personal Data Protection Law and Health/Genetic Data Privacy in Turkey

Turkelogentag 2018

Bamberg, Turkey, September 19-21, 2018

Özkan, Ö. Genetik Veri, Kişisel Sağlık Kayıtları Sistemlerine Nasıl Entegre Edilmeli?

Science and Technology Studies (STS TURKEY 2018)

Ankara, Turkey, September 10-11, 2018

Özkan, Ö., Aydınoglu, A. U., Aydin Son, Y., Security and Privacy Issues of Genetic Information in Mobile Environment,

X. International Medical Informatics Conference (MIA 2017)

Antalya, Turkey, October 12-15, 2017

Özkan, Ö., Aydınoglu, A., Son, Y., A Survey to Determine Security and Privacy Measures Needed for Genetic Information Exchange in Personal Health Records

InfraHealth 2015



Trento, Italy, June 18-19, 2015

Özkan, Ö., Saka, O., Arifoğlu, A., Attitudes and Opinions of People Who Use Medical Services about Privacy and Confidentiality of Health Information in Electronic Environment

IADIS e-Health 2011

Rome, Italy, July 20-22, 2011

Özkan, Ö., Saka, O., Arifoğlu, A., Attitudes and Opinions of Turkish People about Privacy and Confidentiality of Keeping Health Information in Electronic Environment

VII Medical Informatics Conference (TurkMI'10)

Cyprus 2010, TRNC, October 14-17, 2010

Erte I., Koseoglu P., Özkan, Ö., et al., Predicting Cancer Risk Group of Countries Based on OECD Health Data

24TH EUROPEAN CONFERENCE ON OPERATIONAL RESEARCH (EURO XXIV)

Lisbon, PORTUGAL July 11-14, 2010

## **POSTER**

Özkan, Ö., Yalçın, A., Döm, A., Yaldiz, B., Narci, K., Baloğlu, O., Aydınoğlu, A. U., Aydin Son, Y., Participatory Design Meetings: Genetic Information Included Personal Health Record Application,

HIBIT 2017

Cyprus 2017, TRNC, June 28-30, 2017

Özkan, Ö., Usability Analysis of Two of the Biggest Turkish Public Training and Research Hospitals' Websites

MIE 2014

Istanbul, Turkey, August 31- September 3, 2014

## **LANGUAGE SKILLS**

Turkish: Native Speaker

English: Good command of spoken and written English

*IELTS Overall (Examination date): 6.5/9 (June 2011)*

*YDS-Turkish English Proficiency Exam Overall (Examination date): 87.5 (March 2016)*

German: A1 Level

*ÖSD Overall (Examination date): 91/100 (March 2017)*