

ATTITUDES AND OPINIONS OF PEOPLE WHO USE MEDICAL SERVICES
ABOUT PRIVACY AND CONFIDENTIALITY OF HEALTH INFORMATION IN
ELECTRONIC ENVIRONMENT

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
MASTER OF SCIENCE
IN
THE DEPARTMENT OF MEDICAL INFORMATICS

FEBRUARY 2011

Approval of the Graduate School of Informatics

Prof. Dr. Nazife BAYKAL
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Didem GÖKÇAY
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Prof. Dr. Osman SAKA
Co-Supervisor

Dr. Ali ARİFOĞLU
Supervisor

Examining Committee Members

Prof. Dr. Nazife BAYKAL (METU, II)_____

Dr. Ali ARİFOĞLU (METU, II)_____

Prof. Dr. Osman SAKA (Akdeniz Ü., TIP)_____

Assist. Prof. Dr. Yeşim AYDIN SON (METU, II)_____

Assist. Prof. Dr. Neşe ZAYİM (Akdeniz Ü., TIP)_____

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 and Surname : Özlem ÖZKAN

Signature :

ABSTRACT

ATTITUDES AND OPINIONS OF PEOPLE WHO USE MEDICAL SERVICES
ABOUT PRIVACY AND CONFIDENTIALITY OF HEALTH INFORMATION IN
ELECTRONIC ENVIRONMENT

ÖZKAN, Özlem

M.Sc., Department of Medical Informatics

Supervisor: Dr. Ali ARİFOĞLU

Co-Supervisor: Prof. Dr. Osman SAKA

February 2011, 77 pages

In health services, it is a necessity to keep the records of the patients. Although paper-based records are commonly used for this aim, they are not as convenient as computerized records. Therefore, many of the health facilities have recently started keeping patients' health records in electronic databases. However, new questions about confidentiality and privacy of these records were raised with this new system.

This study aims to investigate the opinions and attitudes of the people who use the health services of Turkey about the privacy and confidentiality of health information in electronic environment. In the survey, there are 596 participants from 64 different cities in six geographical regions of Turkey. The findings show that people feel comfortable about computer usage in health-care but they are concerned about the privacy and confidentiality of their information and also they are not sure if their medical information is safe and secure now. Moreover, they are mostly unaware about current regulations related to information privacy in Turkey. The study also shows that people trust in their doctors, health researchers in universities, pharmacist, nurses and other hospital staff but do not trust in insurance companies, government, private sector health researchers, information technology specialists and government health researchers for the privacy of their medical records.

Keywords: Privacy, Confidentiality, Information Privacy, Laws and Regulations in Turkey, Electronic Health Records

ÖZ

SAĞLIK HİZMETİNDEN YARARLANAN BİREYLERİN, ELEKTRONİK ORTAMDA TUTULAN SAĞLIK BİLGİLERİNİN GİZLİLİĞİ VE MAHREMİYETİ İLE İLGİLİ GÖRÜŞ VE DÜŞÜNCELERİ

ÖZKAN, Özlem

Yüksek Lisans, Tıp Bilişimi

Tez Yöneticisi: Dr. Ali ARİFOĞLU

Ortak Tez Yöneticisi: Prof. Dr. Osman SAKA

Şubat 2011, 77 sayfa

Sağlık servislerinde hastaların sağlık kayıtlarının tutulması bir zorunluluktur. Kağıt tabanlı kayıtlar bu amaçla geniş bir şekilde kullanılmalarına rağmen, bilgisayar kayıtları gibi kullanışlı veya kolay erişilebilir değildirler. Bu nedenle, son zamanlarda bir çok sağlık kurumunda hasta sağlık kayıtları elektronik veritabanlarında tutulmaya başlamıştır. Fakat bu kayıtların gizliliği ve güvenliği ile ilgili yeni sorular ortaya çıkmıştır. Bu çalışma sağlık hizmetlerinden yararlanan

bireylerin, elektronik ortamda tutulan sađlık bilgilerinin gizliliđi ve mahremiyeti ile ilgili grş ve dşncelerini ortaya ıkarmayı amalamaktadır. alıřmada Trkiye'nin altı farklı blgesinden ve 64 farklı ilinden 596 katılımcı vardır. Sonular gsteriyor ki insanlar sađlık hizmetinde bilgisayar kullanımını hakkında endiře hissetmiyorlar; fakat bilgilerinin gvenliđi ve mahremiyeti hakkında endiřeliler ve bilgilerinin řu an gvende olup olmadıđı konusunda kararsızlar. Dahası, Trkiye'de bilgi gvenliliđiyle ilgili sahip oldukları haklardan habersizler. alıřma aynı zamanda, bireylerin doktorlarına, niversitelere bađlı sađlık arařtırmacılarına, eczacılara, hemřire ve diđer sađlık alıřanlarına gvendiklerini ama sigorta řirketleri, devlet, zel sektr sađlık arařtırmacılarına, bilgisayar sistemlerini yrtmekle grevli uzmanlara ve devlete bađlı sađlık arařtırmacılarına bilgilerinin gvenliđi konusunda gvenmediklerini gstermiřtir.

Anahtar Kelimeler: Gizlilik, Mahremiyet, Bilgi Gvenliđi, Trkiye'deki Yasa ve Yaptırımlar, Elektronik Sađlık Kayıtları

To My Mother Ayşe & My Father Hasan ÖZKAN

And

To My Dear Friend Nurcan ALKIŞ

ACKNOWLEDGMENTS

I am greatly appreciative to *my Supervisor Dr. Ali ARİFOĞLU and my Co-Supervisor Prof. Dr. Osman SAKA* for their guidance and support throughout my study. I also thank to *Assist. Prof. Dr. Neşe ZAYİM*. They were all great at sharing their knowledge and experiences during my study.

I would like to express my deepest gratitude to *my friend Nurcan ALKIŞ*. She helped me a lot in all parts of my thesis and encouraged me during my study. I feel very lucky for having such a good friend.

I would like to thank specially to my best friend and love *Onur TİKİN*. He was always with me from the beginning and to the end of my thesis writing process.

I would like to also thank my friends *Erim ALKAN and Nihan OCAK*.

Neşe SEVİM, İdil ERTE, Seda MEŞELİ, Selen DİNÇER, Selma ÖZKAN, Memet ÜÇGÜL, Mahmut TEKER, Erdal COŞKUN and Çağlar YILDIRIM are gratefully acknowledged. They were always with me and ready to support me all time.

It is also to *my mother Ayşe ÖZKAN and my sister Çiğdem ÖZKAN DORKİP, my cousins, my student assistants of Computer Support Group in the Faculty of Education, especially Emrah GÜNER, and many of my other friends, especially Seçil KURBAL, Kemal EMİL and Onur GÖLBAŞI, who helped me during data collection process.*

I am thankful to the *Staff of Informatics Institute* for their helps in every stage of the bureaucratic tasks. I am also grateful to my thesis committee for their suggestions and valuable comments.

TABLE OF CONTENTS

ABSTRACT	iv
ÖZ	vi
DEDICATION	viii
ACKNOWLEDGMENTS	ix
TABLE OF CONTENTS	x
LIST OF TABLES	xiii
LIST OF FIGURES	xv
LIST OF ABBREVIATIONS	xvi
CHAPTER	
1. INTRODUCTION	1
1.1 Background to the Study	1
1.2 Purpose of the Study	3
1.3 Significance of the Study	4
2. BASICS OF PRIVACY	6
2.1 Primary Use	6
2.2 Secondary Use	7
2.2.1 Cryptography Applications	7
2.2.2 Anonymity	8
2.2.3 Pseudonymity	8
2.2.4 De-identification	9
2.2.5 Re-identification	10
2.3 Opt-in and Opt-out	11
2.4 Overview of Existing Privacy Policies	11
3. RELATED STUDIES	14
3.1 Related Studies in the World	14

3.2 Related Studies in Turkey	21
4. METHODOLOGY	23
4.1 Basics of Descriptive Study.....	23
4.1.1 Types of Descriptive Studies	24
4.2 Design of the Study	25
4.3 Pilot Study	26
4.4 Population and Sample	28
4.5 Data Collection.....	29
4.6 Instrumentation.....	29
4.7 Ethics Clearance	30
4.8 Data Analysis	31
5. RESULTS	32
5.1 Preliminary Analysis	32
5.2 Sample Profile	32
5.3 Experiences	34
5.4 Level of Concern	35
5.5 Opinions about Laws and Regulations	38
5.6 Differences between Groups	42
5.6.1 Genders	43
5.6.2 Age Groups (Older people vs. Younger people)	46
5.6.3 Education (Graduates vs. Non-graduates)	48
5.6.4 Geographical Regions.....	49
6. DISCUSSION	53
7. CONCLUSION	59
7.1 Shortcomings and Future Works	61
REFERENCES.....	62
APPENDICIES	
A. QUESTIONNAIRE - Demographic Information	68
B. QUESTIONNAIRE - Level of Concern	70
C. QUESTIONNAIRE - Awareness about Laws and Regulations	72
D. 2010 REFERANDUM - Item 20.....	75
E. ELEKTRONIK BELGE STANDARTLARI	76

F. APPROVAL LETTER OF PRACTICAL ETHICS RESEARCH BOARD 77

LIST OF TABLES

Table 1 Types of information that must be removed in order to make the information de-identified according to HIPAA (Neamatullah et al., 2008)	10
Table 2 Comparison of Some of the Countries' Laws about Privacy of Medical Information to those of Turkey (Berber et. al., 2010).....	12
Table 3 Summary of the related studies	19
Table 4 Distribution of genders of the sample in the pilot study	26
Table 5 Distribution of the subjects to the 6 different regions.....	28
Table 6 List of modified items and sources	30
Table 7 Reliability analysis result	32
Table 8 Demographic profile of main study participants.....	33
Table 9 Health status and Computer related information	34
Table 10 Respondents' experiences related with invasions of their medical records	35
Table 11 Participants' concerns and trust levels about computer-based environments	36
Table 12 Trust levels of the participants in health-care providers about the privacy of their medical information.....	37
Table 13 Trust levels of the participant in researchers about the privacy of their medical information	38
Table 14 Participants' awareness about laws and regulations	39
Table 15 Respondents' concerns about T.C. ID number usage in healthcare.....	40
Table 16 Respondents' opinions about access limits of the people or groups to their medical records	41
Table 17 Respondents' opinions about effectiveness of the legislations proposed to protect their privacy and confidentiality	42

Table 18 Comparison between women and men about their trust levels in the doctors and private sector health researchers about the privacy of medical information.....	44
Table 19 Comparison of women and men on their opinions about access limits to their records of their employer and pharmacies.....	46
Table 20 Comparison between younger and elder people on their opinions about access limits to their records of their spouses, parents/children and their employer .	47
Table 21 Comparison between graduates and non-graduates on their trust levels in the government about the privacy of their medical information.....	48
Table 22 Comparison between graduates and non-graduates on their opinions about access limits to their records of parents/ children and their doctors	49
Table 23 Comparison between the regions of Turkey about comfort levels on computer usage.....	50
Table 24 Comparison between the regions of Turkey about whether they trust the people or associations presented	51
Table 25 Comparison between regions of Turkey on how much access rights they are willing to give to some presented people or groups.....	52

LIST OF FIGURES

Figure 1 Protection providing levels of types of pseudonyms.....	8
Figure 2 Descriptive study design.....	24
Figure 3 Workflow of the study	25
Figure 4 Pie chart demonstration of gender distribution.....	26
Figure 5 Questionnaire exclusion process.....	29
Figure 6 Bar graph of trust levels of the participants in health-care providers about the privacy of their medical information.....	37
Figure 7 Bar graph of the comparison between women and men on their opinions about the security of their medical information	43
Figure 8 Bar graph of the comparison between women and men on their opinions about access limits to their records of their spouses	45
Figure 9 Bar graph of comparison between younger and older people on their opinions about access limits to their records of their spouses, parents/children and their employer	47

LIST OF ABBREVIATIONS

EHR	: Electronic Health Records
HCID	: Health Care Information Directive
HIPAA	: Health Insurance Portability and Accountability Act
METU	: Middle East Technical University
PHI	: Protected Health Information

CHAPTER 1

INTRODUCTION

1.1 Background to the Study

Today anywhere in the world, it is nearly impossible to collect one's entire medical information together since it is distributed around different hospitals, clinics or doctors' offices. There are two solutions for this problem: either patient can carry all the records with themselves or the records are made accessible over network (Huang, Chu, Lien, Hsiao, & Kao, 2009). Mark Rothstein (Silversides, 2010), the director of the Institute for Bioethics, Health Law and Policy at the University of Louisville in Kentucky, also stated that his own medical records are distributed around countless hospitals, even in different cities, clinics and private offices of some doctors. And he added "If someone wanted to get their hands on all my medical records, they couldn't. This is not good for continuity of care, but wonderful for privacy. Currently, keeping medical records in electronic environment is spreading around the world and it provides efficiency in the treatment and in the processes of clinical and financial services (Baumer, Earp, & Payton, 2000).

The advantages of exchanging the electronic health information can be sorted as:

- Improved health care quality
- Reduced medical errors
- Lower health care costs
- Early detection of infectious diseases

- Improved tracking of chronic disease management (Aspden, P., & Institute of Medicine, authors., 2004)

There is a variety of new health care information infrastructures to collect and use of medical data. Their features can be listed as:

- EHR; allows keeping birth to death medical records including health care status, diagnosis, treatments and financing costs.
- Databases; more exhaustive and organized data collection, usage and rearranging.
- Electronic Card Technology; owned by patient and enables to record the health data in it.
- Unique Health Identifiers; enables cross-match of patient records in different databases.
- Internal Networks; allows building connection in linked medical services.
- Public On-Line Networks; gives healthcare providers, researchers or hospital managers to share information in off-site locations (Gostin, 1997).

Although keeping and using medical data in electronic environment has several benefits, new questions had been turned out after this new technology was put into use:

- Which personnel may access to the data?
- Under what circumstances should it be available?
- How should it be used appropriately?
- How will the protection of the integrity of the data be provided? (O'Brien, & Yasnoff, 1999)

The privacy of the records has been reduced. In other words misuse of data has increased with computerized interface (Baumer et al., 2000). Smith and Eloff (1999) reported that after electronic systems were first introduced in health-care, security of patients' medical information, especially sensitive ones', became an important issue. Medical records include sensitive information about patients besides great deal of personal information like fertility and abortions, physiologic problems and psychiatric care, sexual transmitted diseases, HIV status, drug abuse, physical abuse, etc. Accessing to these kinds of information can cause serious damages to patients'

lives. For example, such an event can limit job opportunities of a person, can affect insurability, and can cause social embarrassment. Hence, patients may avoid being tested their health problems or healthcare providers may not store all the information in their patient records (Rindfleisch, 1997).

The most important threats about patient confidentiality are:

- Accidental Disclosures
- Insider Curiosity: for infringers' own curiosity or purposes
- Insider Subornation: done generally for profit
- Uncontrolled Secondary Usage
- Unauthorized Access (Rindfleisch, 1997)

Smith and Eloff (1999) went on to state that before an information system is used, being sure about the fact that the protection of integrity and confidentiality of the patients' information is essential. It was early 21st century that ethical concerns of the privacy of the medical records became a controversial issue (Tracy, Dantas, & Upshur, 2004). When the information technology and electronic records terms were mentioned, the concerns about the security of them increased, as proposed by Tracy et al. (2004). Precisely because of these reasons the Health Insurance Portability and Accountability Act (HIPAA) offered general rules in 1996 for the protection of the privacy of health information (Huang et al., 2009). Before the release of these regulations, HIPAA's main purpose was to develop the Medicare and Medicaid programs and to improve the efficiency and effectiveness of the whole medical system. HIPAA now aims to protect patients' rights about privacy and confidentiality and it has lots of regulations about computerized medical information (MacKenzie, 2004). In Turkey, there is a new legislation, under construction, about the protection of personal information, as well (Appendix D).

1.2 Purpose of the Study

The purpose of this study was to reveal awareness and concern levels of the people who use medical services of Turkey about their medical records stored in electronic environment. A questionnaire was applied to the people who were living in different places in Turkey and seven research questions were developed through this purpose.

Answers of these questions will clarify awareness and concern levels of the participants.

The research questions are as follows:

1. What is the level of concern, trust, comfort and tolerance about their health information stored in computerized environment of the people who use health services of Turkey?
2. Are the people aware of the laws and regulations in Turkey about information privacy?
3. What are the opinions of the participants about who should be able to access their medical records?
4. What are the participants' perceptions and experiences related to electronic health information?
5. How do confidentiality concerns effect what the patients will share with healthcare providers?
6. Are there any differences about concern level between gender, age, education, geographical region and monthly salary groups?
7. Are there any differences about awareness level between gender, age, education, geographical region and monthly salary groups?

1.3 Significance of the Study

There are plenty of researches about the privacy of electronic medical records in the literature all over the world. In Turkey, however, there is a lack of resources about the topic. Although there are some papers about information privacy, none are specifically about health information. There is only one thesis study conducted in Başkent University, Ankara, partly about the confidentiality of medical information (Akyüz, 2008). Actually, it is more about the attitudes of nurses related with patient privacy. In this manner, this study can contribute to the existing literature in this manner.

As stated before, there are lots of studies in many countries in the world about confidentiality and privacy of patients' records. Australia and New Zealand (Whiddett, Hunter, Engelbrecht, & Handy, 2006); Canada (Nair, Willison, Holbrook,

& Keshavjee, 2004), (Pullman et al., 2009), (Tracy et al., 2004); Ireland (Buckley, Murphy, & MacFarlane, 2010); UK (Carman, & Britten, 1995), (Barrett, Cassell, Peacock, & Coleman, 2006) can be counted as examples for some of these surveys. Moreover, Sankar, Moran, Merz and Jones (2003), who searched MEDLINE (1966 to March 2001) and BIOETHICSLINE (1980 to March 2000), had reached 5746 studies about confidentiality in medicine and 110 specifically about patients' views of confidentiality (Sankar et al., 2003). Unfortunately, none of those papers were published from Turkey.

In addition to the articles, there are annual reports, conducted to understand the public perceptions about personal privacy and privacy of personal health information such as the surveys carried out by the governments of the USA in 1999 (Princeton Survey Research Associates, 1999) and Canada in 2003, 2004 and 2007 (EKOS Research Associates, 2007). There were over 2000 participants for both of these researches. Unfortunately, there is no such a public opinion survey conducted by Turkish government.

Sankar et al. (2003) grouped the papers about patient perspectives on medical confidentiality into 4 categories in their study. The categories are: 1) *Understanding and awareness*, understanding what the medical confidentiality is and awareness about ethical and legal basis; 2) *Limits of access*, patients opinions about who should reach their medical records; 3) *Effect on seeking care*, how their concerns affect patients' decisions to seek medical care; 4) *Effect on disclosure*, how confidentiality concerns effect what the patients will share with healthcare providers. None of the studies contained these 4 titles together but all will be discussed within the scope of the research questions of this thesis.

CHAPTER 2

BASICS OF PRIVACY

Confidentiality and security are the most confused terms with privacy yet there are some minor nuances between them. According to O'Brien & Yasnoff (1999), the definitions of them can be established as,

- **Privacy:** The right of humans to keep information about themselves secret, free from the knowledge of others.
- **Confidentiality:** The assurance that identifiable information about people is not disclosed without consent, except for legislation.
- **Security:** The mechanisms implemented in computer and telecommunication systems in order to provide privacy and confidentiality of the information (O'Brien & Yasnoff, 1999).

In this chapter the basics about privacy will be discussed. The titles are: Primary Use, Secondary Use, Cryptography Applications, Anonymity, Pseudonymity, De-identification, Re-identification, Opt-in and Opt-out, Overview of Existing Privacy Policies.

2.1 Primary Use

Primary uses mean uses or disclosures of the medical information for treatment purposes. The word *use* refers to sharing, employment, utilization, application, examination or analysis of health information within a care provider that maintains information whereas “disclosure” means for protected medical information, the

release, transfer, provision of access to, or divulging in any other manner of the identifiable medical information to the outside of the care provider (Rada, 2003).

2.2 Secondary Use

Secondary use of medical data means using the data in the areas which are not directly related to health-care.

The following can be counted as examples for secondary use (Safran et al., 2007):

- Activities as Analysis, Research, Quality and Safety Measurement
- Public Health
- Payment
- Provider Certification or Accreditation
- Marketing, and Other Business Applications
- Including Strictly Commercial Activities
- Developing Health Care Experiences for Individuals
- Expand Knowledge about Disease and Appropriate Treatments
- Strengthen Understanding about Effectiveness and Efficiency of Health Care Systems
- Support Public Health and Security Goals
- Aid Businesses in Meeting Customers' Needs

However, there should be lots of ethical, political, technical, and social issues before the secondary use of health data (Safran et al., 2007).

2.2.1 Cryptography Applications

Encryption technology's aim is to protect the data from being read by undesired people. It works by scrambling the data in such a way that the content will be unreadable (Smith, 1999). There are two encryption approach called symmetric and asymmetric encryption (Smith, 1999).

- **Symmetric Approach:** The same key is used in order to encrypt and decrypt the data. The information which is encrypted with a key can be decrypted by the one who has the same key.

- **Asymmetric Approach:** There are two keys in this approach: public and private. They are created as a mathematically related key pairs. Hence, encrypted data by the public key can only be decrypted by the private key.

2.2.2 Anonymity

Anonymity ensures that a user may use a resource or service without disclosing his or her identity. The requirements of anonymity provide protection of users' identities. According to Pankaj and Rohatgi (2000), "Anonymity is not intended to protect the subject identity. There are 2 types of anonymity; sender and receiver anonymity: (Fischer-Hübner, 2001).

- **Sender Anonymity** means that the receiver might not be anonymous but the sender, in the role of sender, the user, should be.
- **Receiver Anonymity** has opposite meaning; this time the user is anonymous in receiver role.

2.2.3 Pseudonymity

In case anonymity cannot be provided, pseudonymity can protect the identity of the user. Pseudonymity means using alias instead of actual names. Pseudonyms can be classified according to how much protection they are providing (See Figure 1).

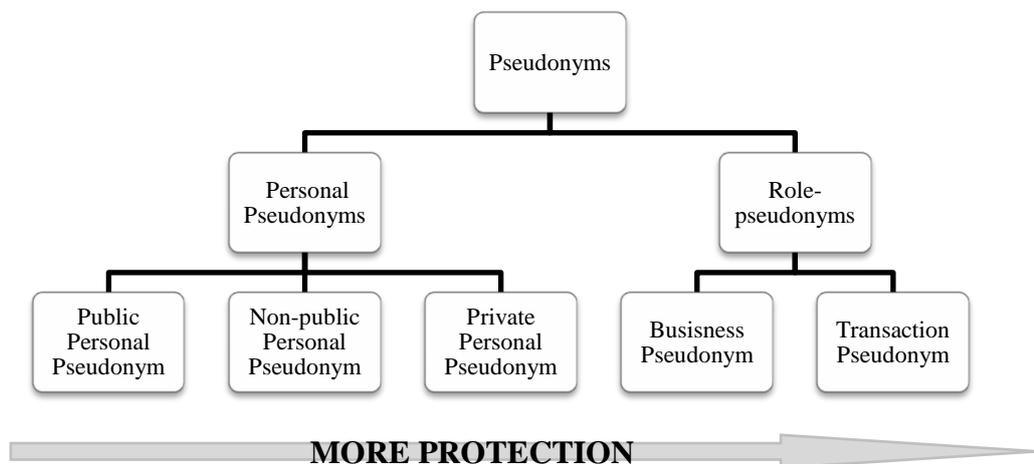


Figure 1 Protection providing levels of types of pseudonyms (Fischer-Hübner, 2001)

- **Personal Pseudonyms** are like the alias for the person. Public personal pseudonym, such as telephone numbers, can be known by everyone but non-public personal pseudonym, like credit card numbers, can only be known by certain parties and private personal pseudonyms is only known by their holders.
- **Role-pseudonyms** are related to the role that the individual performs. They have higher degree of protection than personal pseudonyms. Business pseudonym is used in business with various transactions of one business activity. Transaction pseudonym offers highest degree of protection since it is used only for one single transaction (Fischer-Hübner, 2001).

2.2.4 De-identification

De-identification is a process that removes personal identifiers from the consumers' information in order to protect their privacy (Solís, n.d.). According to the Health Insurance Portability and Accountability Act's regulations (HIPAA), there are 18 specific categories of information on these records that must be removed in order to use medical records for research purposes. Names, geographic locations, elements of dates except years, social security number, etc. are in some of these protected health information (PHI) categories. The actual list of HIPAA is in Table 1 (Neamatullah et al., 2008).

Table 1 Types of information that must be removed in order to make the information de-identified according to HIPAA (Neamatullah et al., 2008)

PHI Type	Notes
Names	Both full and partial, but not initials
Locations	All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes
Dates	All elements of dates (except years) for dates directly related to an individual, including birth date, admission date, discharge date, date of death
Ages > 89 years	All elements of dates (including year) indicative of an age over 89 years. Such ages and elements may be aggregated into a single category of age 90 or older
Telephone numbers	
Fax numbers	
Electronic mail addresses	
Social security numbers	
Medical record numbers	
Health plan beneficiary numbers	
Account numbers	
Certificate/license numbers	
Vehicle identifiers	Includes vehicle serial numbers and license plate numbers
Device identifiers and serial numbers	Not restricted to medical devices
Web Universal Resource Locators (URLs)	
Internet Protocol (IP) address numbers	
Biometric identifiers	Includes finger and voice prints
Any other unique identifying number, code, or characteristic	E.g., full face photographic images of full faces, scars or tattoos

2.2.5 Re-identification

Re-identification is the reverse process of de-identification; that is matching the personal data with depersonalized one (“Re-identification,” n.d.). According to the HIPAA rules (Landi, & Rao, 2003) “only the owners of the original data can re-identify the patient”. However, protected health information (PHI) is exposed to re-identification attacks. An attacker who has adequate supplementary knowledge about demographic information of a data subject can re-identify the data by using unique

combination of demographic data. Therefore, a measurement for the risk of re-identification in statistical databases is needed (Fischer-Hübner, 2001).

2.3 Opt-in and Opt-out

Opt in and opt out are the two confirmation ways for patient consents;

- **Opt-in:** In this method, participants should clearly state their consents to include for all information usages or disclosures. In other words, “no action” means not to participate (Bellman, Johnson, & Lohse, 2001).
- **Opt-out:** This method is the opposite of the opt-in method; that is, participants are in the program which disclosures or uses information, by default. If they want to exclude from the system, they should state that they do not want to take part in (Johnson, Bellman, & Lohse, 2002).

European Union and the USA have different views about these methods. According to EU, participants have to allow the usage of their information explicitly by opting-in. On the contrary the USA prefers opt-out method (Johnson et al., 2002).

Opt-out approach seems harmful at first view but there is no evidence to support this idea. However, there is a significant difference between these two approaches about participation rates. According to the results of the study, carried out by Junghans, Feder, Hemingway, Timmis, & Jones (2005), opt-out approach has higher response rates than opt-in. Mutch and King (1985) also stated that recruitment rate in opt-in is much more poorer.

2.4 Overview of Existing Privacy Policies

Confidentiality of private life was guaranteed with 20th Constitutional Provision of 1982 Constitution. However, real actions about the privacy of electronic records were taken in early 21s (Berber, Ülgü & Er, 2010).

The acts since that time can be summarized as;

- 2001 Medical Recording and Archiving Services Policies for Hospitals of Inpatient Treatment (Turkish Ministry of Health [TMH], 2001)
- 2004 Additional Policy to Medical Recording and Archiving Services Policies for Hospitals of Inpatient Treatment (TMH, 2004)
- 2005 Policy of the Security of Personal Health Records (TMH, 2005)
- 2007 Security of Information for Administrators (TMH, 2007)
- 2007 Security of Information for Staff (TMH, 2007)
- 2007 Modification for the Medical Recording and Archiving Services Policies for Hospitals of Inpatient Treatment (TMH, 2007)
- 2008 New Standards for Electronic Documents - TSE 13298 (Appendix E)
- 2010 Referendum for Amendment of the Constitution (not come into effect) – 20th Constitutional Provision (Appendix D)

There are lots of law examples in force around the world about privacy in general and many of them are specifically about privacy of health information. See Table 2 (Berber et. al., 2010). As the Table 2 indicates, there is no example of such laws in Turkey.

Table 2 Comparison of Some of the Countries' Laws about Privacy of Medical Information to those of Turkey (Berber et. al., 2010)

	Australia	England	Germany	Turkey
Confidentiality Law	1988			
Health Records Law	1997			
Data Protection Law		1984 & 1998-2000	2001	
Access Right to Health Records		1990		
Modernization of Health-insurance Law			2004	

Australia:

The legal policies about the privacy and confidentiality of health information in Australia are (Berber et. al., 2010, p. 228):

- 1988 Confidentiality Law: it defines the main points to obey about the privacy of personal information.

- 1997 Health Records Law (Confidentiality and Access): there are 12 main items and it has nearly the same content with 1988 Confidentiality Law.

Besides national policies that involve government and private sector, there are lots of regional policies.

England (Berber et. al., 2010, p. 236):

- 1984 Data Protection Law
- 1990 Access Right to Health Records Law
- 1998-2000 Data Protection Law: This law was replaced with two old laws, namely 1984 Data Protection Law, and 1990 Access Right to Health Records Law.

In England, there has been also a guide for the usage and protection of patient information since 1996.

Germany (Berber et. al., 2010, p.238):

According to German e-Health Strategy, people are the owner of their own records; that is, unless they want to share their medical information, nobody can see or use them.

- 2001 Federal Data Protection Law
- 2004 Modernization of Health-insurance Law

CHAPTER 3

RELATED STUDIES

Related Studies in the World and Related Studies in Turkey will be discussed in this chapter.

3.1 Related Studies in the World

There is a myriad of resources about information privacy in the literature. Privacy of health information, of course, is in demand among all types of information (Kalra, 2006). According to a literature review study about medical confidentiality (Sankar et al., 2003), there were 5746 articles searched only in MEDLINE (1966 to March 2001) and BIOETHICSLINE (1980 to March 2000). After the elimination processes 110 studies about the patient perspectives of medical confidentiality had remained. Then the responses were grouped into 4 categories after the examination processes: understanding and awareness, limits of access, effect on seeking care, and effect on disclosure. And finally, at the end of the study, 4 summary points were reached after the review of the articles (Sankar et al., 2003):

- 1) There were confusions about medical confidentiality's legal, ethical and practical limits among patients. They appeared not to understand which medical data is protected and how. Moreover, the word of "confidential" seemed not to be comprehended by all of the patients as well.
- 2) Patients' worries were mostly local or specific; that is, they did not have that much common concern about new regulations or policies. Instead, they, for example, were worried about whether someone saw them when they were

entering to the clinics or whether the doctor was sharing their information with nurses and other staff.

- 3) Patients preferred that health information should only be used for treatment.
- 4) The last and the most alarming finding of the study was that according to all these studies, patients commonly postpone or give up the treatment, or change the inception or the total story of illness. Because of the concerns about confidentiality many of adolescents, battered women, AIDS patients or the people who have high risks for AIDS, genetic tested women and people who had psychological disorders decided not to seek their illness (Sankar et al., 2003).

Whiddett (2006) reported that respondents in Australia and New Zealand were willing to share their information with healthcare providers but unwilling to share them with others (researchers, administrators, the departments of government, etc.). Although they were willing to share depersonalized information, they were reluctant to share sensitive and private information, and they were mostly uninformed about how their information would be used, which is why they would prefer to be asked for consent before their information would be used. Moreover, the responds showed that patients had high level of concern about the current system in New Zealand. The conclusion to be drawn from here is that the future practices about information sharing should be designed to compensate for patient preferences.

Buckley et al. (2010) stated that 67,5% of the respondents from Ireland did not agree to allow doctors to decide when researchers could access identifiable PHI but 89.5% of the participants stated that they would agree to allow doctors to share their de-identified PHI with researchers without their consent. Furthermore, exclusively the elderly, retired and low levels education people agreed on the idea that any personal medical information could be shared.

Carman & Britten (1995) found out that most of the British respondents wanted administrative and secretarial staff to have no access right, that some interviewees agreed on giving other doctors who were not involved in their treatment process the right to access their records provided that the doctors fulfilled their requirements, that patients were not aware of the fact that general practitioners had ready access to their

records, and that the patients felt uncomfortable about the confidentiality of electronic health records and had concerns about storage of nonmedical information in their medical records.

Another study conducted by Barrett et al. (2006) in order to figure out British public's views on the use of identifiable medical data by the National Cancer Registry revealed that 72% of the participants considered inclusion of postcode, name, address and the receipt of a letter which invites them to a research study on the basis of inclusion in the registry to be an invasion of their privacy by the National Cancer Registry. Moreover, most of the sample had no concerns about the invasions of their privacy.

Nair et al. (2004) researched patients' consent preferences regarding the use of their health information for research purposes in Canada. According to the results, respondents preferred to be consulted about the use of their information for research purposes by written consent forms. Also, most of the patients were unaware that their health data were being used for research purposes, a number of concerns were raised by patients about the safeguards applied to protect their records and they were willing to be ensured that their information would be anonymous and that only the researchers but not the funders would have access to the data.

The results of another study conducted in Canada by Pullman et al. (2009) indicated that people had generally poor awareness about privacy rights and responsibilities. Moreover, a significant number of professionals who used the PHI had much more concerns about the use of the patients' records for research than the ordinary people did. They were also not aware of the laws and regulations about Personal Health Information, and the basic necessities for research on patients. Furthermore, most of the respondents were unfamiliar with the basic requirements for patient-based research.

According to the results of the study conducted by Tracy (2004), investigating the feasibility of a patient decision aid regarding disclosure of personal health information, Canadian people had poor knowledge about the use of personal health information - how their health records are collected, used, and disclosed. Also, they

did not count on the security provisions since a wide variety of users could access their medical data: lawyers, psychologists, social workers, researchers, etc.

They do not trust in the relation between the protection of their privacy and the security of their medical data; numerous suggestions provided by the participants regarding the formatting of the HCID in order to facilitate implementation.

Today, many of the governments such as Canada and the USA have issued public questionnaires to understand what the society think about the privacy of their medical records, how concerned they are and what can be done for the reduction of the concerns.

The reports that Canada published before are (EKOS Research Associates, 2007):

- 2003, Public Attitudes to Electronic Health Records and its Linkages
- 2004, Canadian Health Information Privacy and Confidentiality Framework
- 2007, Canadians and the Privacy Landscape.

The questionnaire was made via telephone between June 22nd - July 19th, 2007 with random sample of 2,469 Canadians, who were 16 and older.

The objectives of the survey were as follows:

- Perceptions of personal privacy and privacy of personal health information,
- Awareness of laws/oversight bodies in relation to personal health information,
- Perceptions and experiences related to electronic health information,
- Secondary use of electronic health information,
- The public's level of trust, comfort and tolerance for the electronic health record.

According to the key findings of the survey, the consumers have

- Strong concern level about the safety and security of their personal health information,
- High trust level towards to health professionals (doctors, nurses, pharmacists, etc.); lower for other groups (administrators, government

departments, etc.); mixed for others (computer technicians, insurance companies, researchers, etc.),

- Modest level of awareness about laws.

And they are

- Supporting the development of EHRs,
- Thinking EHRs were better than paper-based systems in terms of privacy of patient information and their effectiveness for doctors, pharmacists, patients and nurses.

The survey conducted in the USA (Princeton Survey Research Associates, 1999) was also a telephone-based survey. The survey was conducted between November 12 and December 22, 1998 among 1,000 Americans and another 1,100 California respondents over the age of 18.

According to the key findings, despite new federal protections, consumers were:

- Concerned about the privacy of their personal health information
- Unaware of their rights
- Practicing “privacy-protective behaviors”

Willing to share their personal health information to gain certain benefits

As can be seen in the Table 3, concern levels and having concern or not about the privacy of medical records are the most frequently asked questions (eight out of nine). Being aware or informed before about their rights is the second (seven of them). Being comfortable or not with electronic environment recording is one of the rarely asked questions (only three out of seven).

Table 3 Summary of the related studies

Name of the paper or report:	Place	Method	N	Having concern	Being aware/ Informed	Comfortable with EHR
Patients' attitudes towards sharing their health information (Whiddett, 2006)	Australia & New Zealand	Questionnaire	200	x	x	-
Public attitudes to the use in research of personal health information from general practitioners' records: a survey of the Irish general public (Buckley et al., 2010)	Ireland	Informed by focus groups & Questionnaire	1575	-	-	-
Confidentiality of medical records: the patient's perspective (Carman & Britten, 1995)	UK	Semi-structure interviews	39	x	x	x
National survey of British public's views on use of identifiable medical data by the National Cancer Registry (Barrett et al., 2006)	UK	Face to face interviews	2872	x	-	-
Patients' consent preferences regarding the use of their health information for research purposes: a qualitative study (Nair et al., 2004)	Canada	Semi-structure interview survey	17	x	x	-
Sorry, You Can't Have That Information: Data Holder Confusion Regarding Privacy Requirements for Personal Health Information and the Potential Chilling Effect on Health Research (Pullman et al., 2009)	Canada	Questionnaire & follow-up focus groups	1550	x	x	-
Feasibility of a patient decision aid regarding disclosure of personal health information: qualitative evaluation of the Health Care Information Directive (Tracy, 2004)	Canada	Group meetings	28	x	x	-
Electronic Health Information and Privacy Survey: What Canadians Think - 2007(EKOS Research Associates, 2007)	Canada	Questionnaire	2469	x	x	x
USA Medical Privacy and Confidentiality Survey- 1999 (Princeton Survey Research Associates, 1999)	USA	Questionnaire	2100	x	x	x
TOTAL:				8	7	3

The followings are the presentations of the papers in Table 3 in detail;

The research, *Patients' attitudes towards sharing their health information* (Whiddett, 2006), was issued after Australia and New Zealand's laws which support sharing the health data via electronic environment between stakeholders. There were two main objectives of this research; the first was to see what the patients think about sharing their records and the latter was to ask them if they think they are informed enough about how their information will be used. Questionnaire method was applied to 200 patients in 5 different clinics in a New Zealand city.

Mixed methods, namely informed by focus groups, literature review, and a questionnaire were used in the study named *Public attitudes to the use in research of personal health information from general practitioners' records: a survey of the Irish general public* (Buckley et al., 2010). 1575 adults from Ireland filled out the questionnaire. The aim of the study was to assess the attitudes of the public about accessing their personal health records for research purposes and factors that influence these.

The aim of the study called *Confidentiality of medical records: the patient's perspective* (Carman & Britten, 1995), was to describe the views of the British public about their attitudes towards medical records in general practice. Semi-structure interviews were conducted among 39 British patients.

The objective of the study titled *National survey of British public's views on use of identifiable medical data by the National Cancer Registry* (Barrett et al., 2006), was to figure out the attitudes of the British public on the use of personal medical data without individual consent by the National Cancer Registry and to evaluate the usage of identifiable medical data. Face to face interview method was conducted among 2872 people, setting England, Wales and Scotland. The participants took part in another survey named the Office for National Statistics conducted in March and April 2005.

In the study titled *Patients' consent preferences regarding the use of their health information for research purposes: a qualitative study* (Nair et al., 2004), a semi-structure interview survey was conducted in Ontario, Canada, with 17 patients whose

health data were used for research purposes. The results were analyzed by using a constant comparative method.

The survey called *Sorry, You Can't Have That Information: Data Holder Confusion Regarding Privacy Requirements for Personal Health Information and the Potential Chilling Effect on Health Research* (Pullman et al., 2009), aimed to investigate the level of awareness, perceptions and concerns of the participants, who are healthcare providers, health researchers, data managers and ordinary people in Newfoundland and Labrador about the storage, use and disclosure of health records for research purposes by surveys and follow-up focus groups methods.

The aim of the survey titled *Feasibility of a patient decision aid regarding disclosure of personal health information: qualitative evaluation of the Health Care Information Directive* (Tracy, 2004), was to assess a patient decision aid, which is the Health Care Information Directive (HCID), and it aims to define the amount of information the patient is willing to share. Four focus group meetings, which consist of 28 men and women participants, were organized in a large city in Canada. Qualitative methods were used to analyze the data. Respondents were chosen among health care consumer advocates, urban professionals, senior citizens, and immigrants who were able to speak English.

3.2 Related Studies in Turkey

The searches were done through National Thesis Center of the Turkish Council of Higher Education, Databases of METU Electronic Sources and Google Scholar. Privacy, confidentiality, health, medical, information, data and Turkey keywords were used but there was only one study about patient privacy according to these searches. The study (Akyüz, 2008) was a thesis conducted in the school of nursing in Başkent University, Ankara. The title of the study was “The Opinions of Patients and Their Nurses about the Effects on Privacy of the Nursing Care Practices in Patients Having Surgery”. The sample was chosen from Başkent University Ankara Hospital and included 102 adult patients admitted to surgical wards and 47 nurses. Two different questionnaires were applied to each of the sample groups; patients and

nurses. The questions directed to the patients were generally aimed at understanding whether the nurses respect for patients' privacy or not. There were some questions directed to the both of the groups related with the information privacy. However, they were associated with nursing.

The results were as follows:

- Most of the participants stated that although a good level of respect was shown for their privacy, they had some concerns about the protection of the privacy of their medical data.
- Both nurses and patients had similar definitions about privacy and containing physical, psychological, social and informational aspect.
- Most of the patients wished some environmental requirements such as private/ single room for more privacy.

CHAPTER 4

METHODOLOGY

In this chapter methodology of the study will be presented. The title is divided into eight subtitles and they are Basics of Descriptive Study, Design of the Study, Pilot study, Population and Sample, Data collection, Instrumentation, Ethics Clearance, Data Analysis.

4.1 Basics of Descriptive Study

Descriptive study is one of three demonstration studies, namely correlation, comparative and descriptive. It is designed only for investigating one variable or a group of variables in a selected sample (Friedman & Jeremy, 1997). Descriptive statistics tries to answer the question “what is” rather than inferential statistics that concentrates on cause and effect. Descriptive research can be either quantitative or qualitative but it has a different definition from both methodologies. However, elements of them are commonly used in descriptive researches, even mostly within the same study (Knupfer, & McLellan, 1996). Figure 2 shows the schema of the descriptive study design (Friedman & Jeremy, 1997);

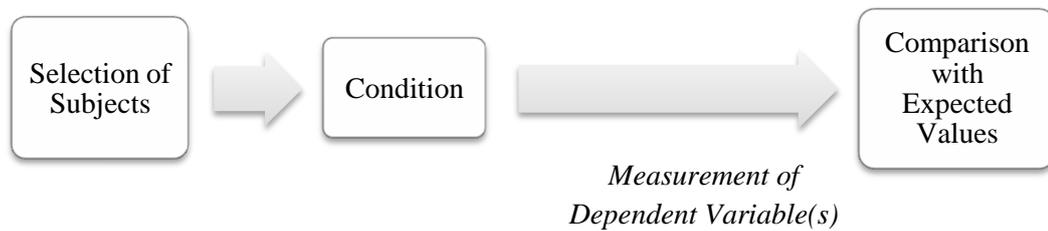


Figure 2 Descriptive study design (Friedman & Jeremy, 1997)

Descriptive studies have both advantages and limitations. Despite its low cost, efficient usage and small number of ethical difficulties, descriptive studies have important disadvantages, as well. There can be uncertain putative cause and effect relations or researcher might infer wrong causes when there is no possible (Wingo, Higgins, Rubin, & Zahniser, 1994).

“Even though they seem deceptively simple, descriptive studies can be highly informative.” (Friedman & Jeremy, 1997).

4.1.1 Types of Descriptive Studies

Types of the descriptive studies vary among two main targets; individuals and populations.

Studies about individuals are (Grimes & Schulz, 2002):

- **Case Report:** The researcher, generally clinician, prepares a report that is about a rare disease or an inflection or drug interactions. However, it does not necessarily have to be serious health threats.
- **Case-series Report:** The report consists of many individual reports. It is generally done when only one unusual case is not enough for further investigations.
- **Cross-sectional (Prevalence) Studies:** These studies are conducted to understand the health status of the public. They are generally carried out by governments. These studies can be conducted within small groups and can be generalized.

- **Surveillance:** This is one of the important kinds of descriptive studies and can be defined as watching and observing the society. The main feature of the study is feedback. Fundamental parts of the feedback loop are prevention and control of the problem.

And ecological correlation studies are done to examine the populations. Rather than individuals, they deal with relationships between exposures and outcomes in populations (Hennekens & Buring, 1987).

4.2 Design of the Study

The study is a descriptive study and its aim is to investigate the attitudes and opinions of the people who use medical services of Turkey about privacy and confidentiality of health information in electronic environment. The simple study workflow is given below (See Figure 3).

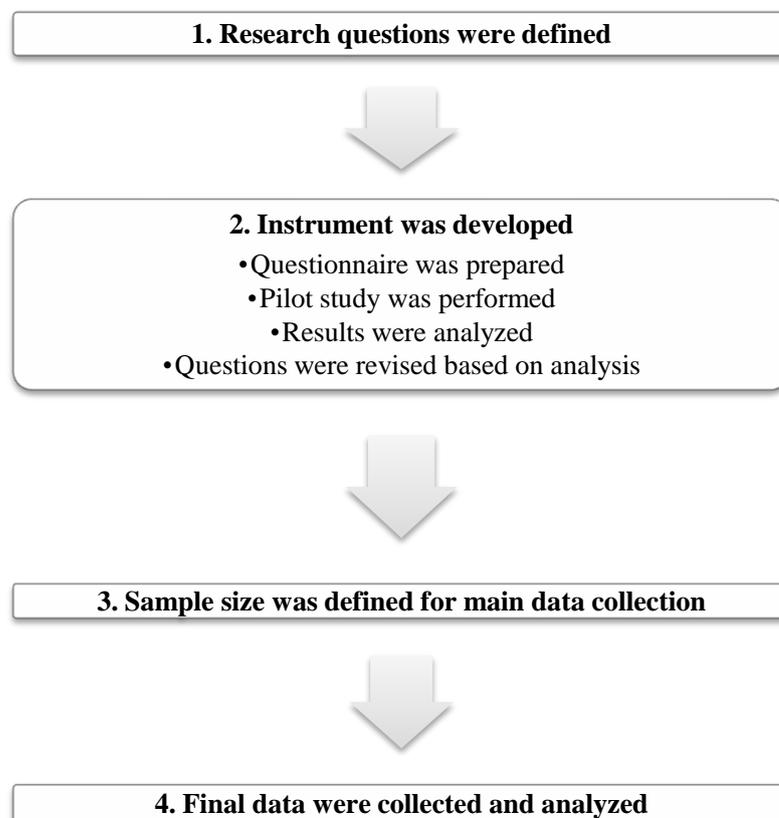


Figure 3 Workflow of the study

4.3 Pilot Study

Pilot study is the small scale of the entire study design (Earl Babbie, 1990, p.220). The pilot study was performed in Ankara in November 2010. 26 questions were prepared about three main areas, namely demographic information, awareness and the policies and directed to 200 respondents who were Turkish citizens and older than 18. Table 4 shows the gender distribution of the sample.

Table 4 Distribution of genders of the sample in the pilot study

Gender:	n	%
Female	97	48,5
Male	103	51,5
Total	200	100

Figure 4 shows the pie chart demonstration of gender percentages.

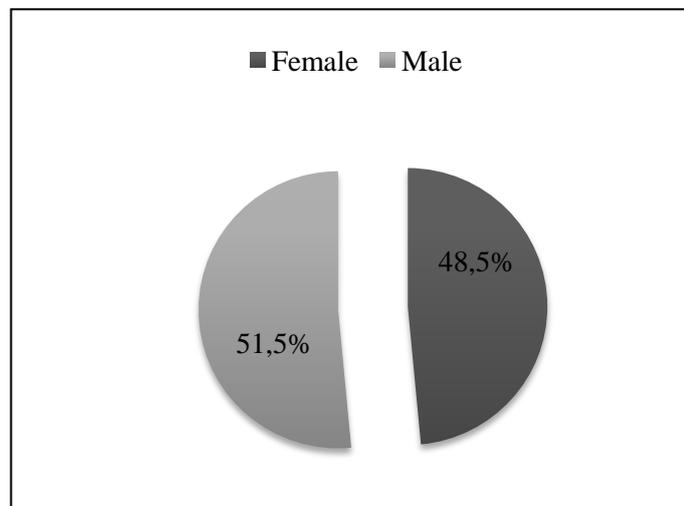


Figure 4 Pie chart demonstration of gender distribution

Reliability of the data was (Cronbach Alpha) 0,771 and error interval was $\pm 5\%$. As for the significant results of the pilot study,

- People trust doctors most (70,5 percent), and it is followed by university researchers with 46 percent and the government is one of the lasts with 22,5 percent.

- Moreover, almost all the participants want to have access to everything in his or her medical records (93%) but very little allow their insurance company or employer to access their information (less than 15 percent).
- 59,5% of people among the participants have concerns about the usage of TC identity number for healthcare and 69% want a unique health identifier instead.
- 74,5% percent of the participants feel confident about usage of computer in healthcare.
- Over half of the participants (53%) are very concerned or somewhat concerned about the breach of their medical information.
- According to the participants, the biggest threat of the privacy and confidentiality of personal medical records kept on computer-based systems is disclosure by people with authorized access and without authorized access equally (54,5%) and the second biggest percentage belongs to unauthorized access with 34,5%.
- There are, quite a lot actually, 11 people (6 women, 5 men) who decided not to be tested because others might find out about the results. Moreover, three of the females and one of the males had asked a doctor not to write down their health problem in his or her medical records or asked the doctor to put a less embarrassing diagnosis into the record than was actually the condition.

Furthermore, an interview was performed with five people about intelligibility of the questions. After these tests, some modifications were applied to the questionnaire:

- Four questions were removed from the questionnaire:
 - Two of them seemed unnecessary: one of them was removed after the interview and the other after the results of questionnaire (no variety)
 - The last two were excluded because of the reduction in the reliability
- 11 questions were updated:
 - After the results of the questionnaire some choices were added to and removed from 11 of the questions.
- Two questions were combined and some parts were deleted:
 - After the interview they seemed very similar; therefore, they were combined.

- Two new questions were added:
 - After the analyzing process of the results of the pilot study, questions about age and city of residence were added.

4.4 Population and Sample

In order to figure out the opinions and attitudes of the people who live in different geographical regions of Turkey, the questionnaire was delivered to 694 people from six geographical regions and the responses of 596 people were included in the analysis process. The mean of the participants' ages is 28,63 and the ages vary between 18 and 70. There are 279 women (46,8%) and 317 men (53,2%) in the sample. Education levels of the respondents range between elementary school to PhD level. The subjects in the sample are from 64 different cities in six regions of Turkey. The distribution of the subjects to the regions is Mediterranean Region (9,9%), Inner Anatolia Region (25,5%), Black Sea Region (11,4%), Aegean Region (16,3%), Marmara Region (29,9%), and East Regions (7%). Table 5 shows the distribution of the subjects to the regions in detail.

Table 5 Distribution of the subjects to the 6 different regions

Regions:	n	%
Marmara Region	178	29,9
Inner Anatolia Region	152	25,5
Black Sea Region	68	11,4
Aegean Region	97	16,3
Mediterranean Region	59	9,9
East Regions	42	7,0
Total	596	100,0

4.5 Data Collection

Data collection was performed with two different methods:

- Online survey: The questionnaire was accessed by 594 people via the Internet. Seven of the subjects did not fill any of the questions and 69 of the subjects had too much missing answers so they were eliminated and 518 useful online subjects remained.
- In-person survey: 100 paper-based questionnaires were distributed but only 80 of them were returned. Two of the subjects were eliminated; one did not answer too many of the questions and the other participant's age was not appropriate for the survey (15).

Questionnaire exclusion process is summarized in Figure 5.

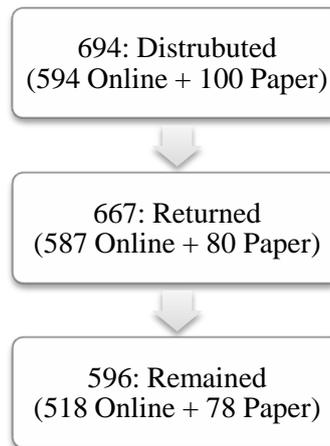


Figure 5 Questionnaire exclusion process

4.6 Instrumentation

The language of the instrumentation was chosen participants' native language, Turkish. There are 23 questions in the instrument. The study instrument has three different sections:

- 1) Demographic information (Appendix A)
- 2) Level of concern (Appendix B)
- 3) Awareness about laws and regulations (Appendix C)

10 of the questions in the questionnaire were selected and modified from two different surveys: Privacy Survey: What Canadians Think (EKOS Research Associates, 2007) and Medical Privacy and Confidentiality Survey (Princeton Survey Research Associates, 1999). Table 6 shows the modified questions and the sources. The rest of the questions were designed for the survey.

Table 6 List of modified items and sources

Items	Modified from
Item 9	(EKOS Research Associates, 2007)
Item 10	(Princeton Survey Research Associates, 1999)
Item 11	(Princeton Survey Research Associates, 1999)
Item 12	(EKOS Research Associates, 2007)
Item 13	(EKOS Research Associates, 2007)
Item 14	(EKOS Research Associates, 2007) & (Princeton Survey Research Associates, 1999)
Item 15	(Princeton Survey Research Associates, 1999)
Item 16	(EKOS Research Associates, 2007)
Item 22	(Princeton Survey Research Associates, 1999)
Item 23	(EKOS Research Associates, 2007) & (Princeton Survey Research Associates, 1999)

4.7 Ethics Clearance

The pilot study was conducted in Middle East Technical University (METU). Therefore, an application was done to Practical Ethics Research Board at METU and approved (Appendix F).

4.8 Data Analysis

PASW 18 was used as a statistical analysis program for the whole data analysis process. Descriptive statistics was given by frequencies with numbers and percentages.

Standard Deviation: It was calculated for only continuous variable (Age) in the study.

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, 2007). The results of the analysis should be at least 0,7 or above in order to talk about a consistency (Pallant, 2007). In the study, it is calculated as 0,814.

Chi Square: Chi square test is used between two or more groups and used for determination of differences or connection between qualitative variables (Alpar, 2006). In order to mention a significant difference between groups, the calculation should be greater than 0,05. Chi square test was used to figure out if there were any differences between the groups: genders, ages (elderly vs. younger), education levels (higher education vs. other levels), income groups (≤ 1600 vs. > 1601) and geographical regions of Turkey.

CHAPTER 5

RESULTS

In this chapter results of the study will be presented within six subtitles; Preliminary Analysis, Sample Profile, Experiences, Level of Concern, Opinions about Laws and Regulations, Differences between Groups.

5.1 Preliminary Analysis

The reliability analysis was checked for internal consistency of the instrument (Ary et al., 2002). Coefficient alpha or Cronbach's alpha is one way of calculating it (Ary et al., 2002; Huck, 2004; Pallant, 2007). "Ideally, Cronbach's alpha coefficient of a scale should be above 0,7" (Pallant, 2007). The value of the obtained Cronbach's alpha score (0,814) meet the required value. The result of the reliability analysis of the instrument is given in Table 7.

Table 7 Reliability analysis result

Cronbach's Alpha	N of Items
0,814	38

5.2 Sample Profile

The sample consists of 596 people (279 women, 317 men) with average age level 28,63 (\pm 9,12) from 64 different cities in six geographical regions of Turkey. The participants are from different educational backgrounds, namely primary school and

below, secondary school, high school, undergraduate and graduate, with an average income level 1580 TL. The sample is dominated by undergraduate (67,8%) and graduate (19,5%) levels. The other education levels' percentages are primary school and below (2,2%), secondary school (2%), high school (8,6%). The overall profile of the respondents is shown in Table 8.

Table 8 Demographic profile of main study participants

Item:	Average	Min-Max	SD
Age	28,63	18-70	± 9,12
Item:	Average	Min-Max	Median
Income	1580,49	0-15000	1300
Items:	n	%	
Gender:			
Women	279	46,8	
Men	317	53,2	
Education Level:			
Primary school and below	13	2,2	
Secondary school	12	2	
High school	51	8,6	
Undergraduate	404	67,8	
Graduate	116	19,5	

Health status of the participants is mostly average and above. The participants who chose "Bad" (2,3%) and "Very bad" (0,7%) are only 3% of the whole sample. On the other hand, total percentages of the participants whose health status are "Average" (16,8%), "Good" (61,4%) and "Very good" (18,8%) are 97% of all of the participants. The responses of the items about computer ownership and ability show that the sample's interest in computer is generally in high level. 96,6% of the respondents have computer in their houses and totally 93,1% of general participants' computer abilities are average (36,1%) or above (56,9%). "Don't know" (3%) and "Under the average" (3,9%) choices have totally 6,9% (See Table 9).

Table 9 Health status and Computer related information

Items:	n	%
Health status:		
Very bad	4	0,7
Bad	14	2,3
Average	100	16,8
Good	366	61,4
Very good	112	18,8
Computer ownership:		
Yes	576	96,6
No	20	3,4
Computer ability:		
Don't know	18	3
Under average	23	3,9
Average	216	36,2
Over the average	339	56,9

5.3 Experiences

There are three questions related to patients' experiences in the instrument; Item nine, 10 and 11. According to the results, there are five participants (0,8%) who have experienced an inappropriate usage or release of their medical records without their consent. There is a quite big percent of the respondents (12,5%) who avoided being tested in case someone might see the results. Moreover, nine of the participants (1,5%) asked their doctors to write a less embarrassing illness into their medical records instead of the actual condition. All of the frequencies and percents of the responses are presented in detail in Table 10.

Table 10 Respondents' experiences related with invasions of their medical records

Items:	Yes		No		Don't know/ Reject to answer	
	n	%	n	%	n	%
Item 9: Have you or a member of your family ever experienced a serious breach where your personal health information was used inappropriately or released without your consent?	5	0,8	468	78,5	123	20,6
Item 10: Have you ever decided not to be tested for medical condition because you were concerned that others might out about the results?	75	12,6	521	87,4		n/a*
Item 11: 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?	9	1,5	587	98,5		n/a*

* Not Applicable

5.4 Level of Concern

There are five questions (from Item 12 to Item 16) in the questionnaire in order to find out concern levels of the participants about computer usage in healthcare. 66,3% feel comfortable about computer usage in healthcare and the people who feel uncomfortable are 7,2%. The rest chose the "Didn't think" choice. Most of the participants (64,4%) are not sure as to whether or not their health information is safe and secure. The response rates of "Not safe and secure" and "Safe and secure" choices are very close to each other (18,3% and 16,9%). Answers of the question about being concerned with invasion of personal information in Turkey are "Yes" with vast majority (68,5%). "Not concern" choice has only 11,4% and the rest of the participants (20,1%) did not think on this topic. According to the respondents, disclosures by people with authorized and unauthorized access are both equally dangerous for the privacy and confidentiality of electronic health records (61,6%). 28.5% of the participants believe that the second biggest danger is "Disclosure by people without authorized access who break into computer systems". Table 11 shows these four questions and answers in detail.

Table 11 Participants' concerns and trust levels about computer-based environments

Items:	n	%
Item 12: Do you feel uncomfortable with doctors and other health care professionals using computers to record and share personal health information within the health care system?		
Feel	43	7,2
Don't feel	395	66,3
Didn't think	158	26,5
Item 13: In your opinion, is the health information which exists about you safe and secure?		
Not safe and secure	109	18,3
Safe and secure	101	16,9
Not sure / Don't know	384	64,4
Item 14: Are you concerned about the invasion of your personal information in Turkey?		
Concern	408	68,5
Not concern	68	11,4
Didn't think	120	20,1
Item 15: Which do you think is the biggest threat to the privacy and confidentiality of personal medical records kept on computer-based systems?		
Disclosure by people with authorized access, such as those who are in hospitals, doctor's offices	40	6,7
Disclosure by people without authorized access who break into computer systems	170	28,5
Both equally	367	61,6
Neither	17	2,9

The results reveal that people trust in their doctors (68,8%), health researchers in universities (42,4%), pharmacist (41,4%), nurses and other hospital staff (33,6%) but do not trust in insurance companies (58,1%), government (51%), private sector health researchers (48,8%), information technology specialists (48,5%) and government health researchers (43,8%). Table 12 and 13 gives the details of the answers.

Table 12 Trust levels of the participants in health-care providers about the privacy of their medical information

	Trust		Not trust		Not sure		Missing values	
	n	%	n	%	n	%	n	%
Your doctor	410	68,8	71	11,9	114	19,1	1	0,2
Pharmacist	247	41,4	188	31,5	153	25,7	8	1,3
Nurses and other hospital staff	200	33,6	193	32,4	199	33,4	4	0,7
Government	151	25,3	304	51	141	23,7	-	
Insurance companies	100	16,8	346	58,1	145	24,3	5	0,8
Information technology specialists	97	16,3	289	48,5	203	34,1	7	1,2

Figure 6 is the graphical demonstration of Table 12.

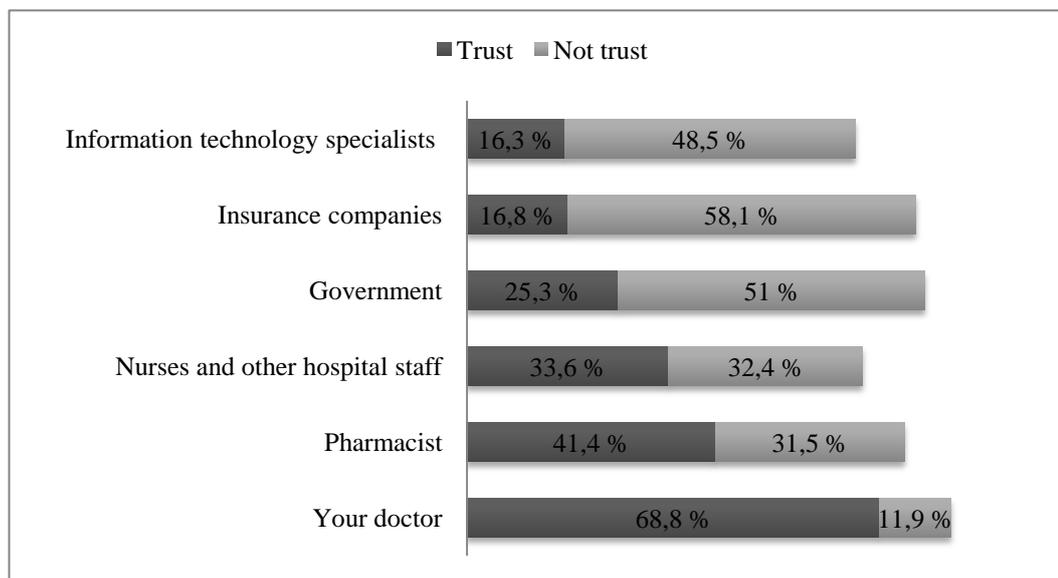


Figure 6 Bar graph of trust levels of the participants in health-care providers about the privacy of their medical information

Table 13 Trust levels of the participant in researchers about the privacy of their medical information

Items:	Trust		Not trust		Not sure		Missing values	
	n	%	n	%	n	%	n	%
Health researchers in universities	253	42,4	167	28	173	29	3	0,5
Government health researchers	147	24,7	261	43,8	186	31,2	2	0,3
Private sector health researchers	111	18,6	291	48,8	191	32	3	0,5

5.5 Opinions about Laws and Regulations

There are seven questions about the laws and regulations in Turkey. Questions arise as to whether they are aware of their rights, whether they have any concern about existing circumstances in Turkey and about which kinds of modifications they want to be done so as to reduce their concern.

In the first three questions, Item 17, 18 and 19, the existing laws and regulations are directed to participants. The questions are as follows:

Item 17: As far as you know, do you have rights to reach your medical records and to demand modifying or deleting them in Turkey?

Item 18: As far as you know, are there any laws in Turkey which prevent your medical data from being used without your consent?

Item 19: As far as you know, are there any regulations in Turkey which prohibit reaching medical data via internet?

According to the results, a big majority of people chose “Don’t know” choice for all these three items. This means that people are generally unaware about the laws and regulations in Turkey. For detailed answers see the Table 14.

Table 14 Participants' awareness about laws and regulations

Items:	Yes		No		Don't know		Missing vales	
	n	%	n	%	n	%	n	%
Item 17: As far as you know, do you have rights to reach your medical records and to demand modifying or deleting them in Turkey?	47	7,9	151	25,3	398	66,8	-	
Item 18: As far as you know, are there any laws in Turkey which prevent your medical data from being used without your consent?	76	12,8	97	16,3	423	71	-	
Item 19: As far as you know, are there any regulations in Turkey which prohibit reaching medical data via internet?	41	6,9	134	22,6	418	70,5	3	0,5

The items 20 and 21 are about an existing regulation in Turkey. T.C. ID number has recently been introduced into use for medical data storage. The questions;

Item 20: Do you have any concern about the usage of T.C. ID number to keep your medical records?

Item 21: Do you prefer a special number for your medical data storage instead of T.C. identity number?

Of all the participants, 327 (55,1%) of them have concerns about T.C. ID number usage in medical data storage and 370 (62,1%) of the participants prefer a special number for this purpose (See Table 15).

Table 15 Respondents' concerns about T.C. ID number usage in healthcare

Items:	Yes		No		Missing values	
	n	%	n	%	n	%
Item 20: Do you have any concern about the usage of T.C. ID number to keep your medical records?	327	55,1	266	44,9	3	0,5
Item 21: Do you prefer a special number for your medical data storage instead of T.C. ID number?	370	62,1	226	37,9	-	

Item 22 is about access rights: how much access the respondents are willing to give to some presented people or groups. According to the results, generally family members are wanted to have more access rights than the other groups (See Table 16). The biggest majority of the respondents (90,6%) give themselves access rights to reach everything in their medical records. The second and third biggest majorities belong to their doctors with 63,4% and with 47,5% to their spouses, respectively. Many of the participants believe that other doctors or staff, and parents and children should have limited access rights with 49,2% and 47,5%. And the rest has no access rights and they can be listed in order as: drug companies (71%), their employer (56%), pharmacies (45,8%) and lastly their insurance company (43,8%).

Table 16 Respondents' opinions about access limits of the people or groups to their medical records

	No access		Limited access		Access to everything		Not sure		Missing values	
	n	%	n	%	n	%	n	%	n	%
You, yourself	6	1	46	7,7	540	90,6	3	0,5	1	0,2
Your doctor	21	3,5	179	30	378	63,4	14	2,3	4	0,7
Your husband/ wife	61	10,2	226	37,9	283	47,5	10	1,7	16	2,7
Parents/ children	98	16,4	283	47,5	196	32,9	10	1,7	9	1,5
Other doctors or staff	190	31,9	293	49,2	76	12,8	30	5	7	1,2
Your insurance company	261	43,8	243	40,8	50	8,4	38	6,4	4	0,7
Pharmacies	273	45,8	245	41,1	47	7,9	30	5	1	0,2
Your employer	334	56	205	34,4	33	5,5	14	2,3	10	1,7
Drug companies	423	71	115	19,3	15	2,5	41	6,9	2	0,3

According to the results of the Item 23, all of the suggested legislations in order to protect privacy and confidentiality would be “very” effective (See Table 17). Nevertheless, participants generally think that:

- **Choice 6:** Requiring their permission prior to using or distributing any of their medical information would be the most effective legislation (67,4%) among all the other proposed ones.

The other three following most effective recommended legislations are:

- **Choice 4:** Having the right to see when and by whom their records are retrieved (62,2%)
- **Choice 1:** Establishing new legislations with serious punishments for people or organizations that violate medical privacy (61,7%)
- **Choice 2:** Requiring doctors, hospital, and other health facilities to set up security systems on their computers (61,7%)

The other choices listed in order are as follows:

- **Choice 5:** Having the right to see and make corrections IN their own medical records (57,2%)
- **Choice 8:** Having the right to hide or mask sensitive information to some users who would be authorized to access their health records (56,0%)
- **Choice 3:** Regular audits undertaken by government for the privacy and security provisions of electronic health systems' health records (52,2%)
- **Choice 7:** Requiring using information that doesn't personally identify people for purposes not for healthcare whenever you want (such as researches) (39,1%)

Table 17 Respondents' opinions about effectiveness of the legislations proposed to protect their privacy and confidentiality

Choices:	No impact		Little		Very much		Not sure		Missing values	
	n	%	n	%	n	%	n	%	n	%
Choice 6	41	6,9	102	17,1	402	67,4	42	7	9	1,5
Choice 4	40	6,7	135	22,7	371	62,2	43	7,2	7	1,2
Choice 1	42	0,7	149	25	368	61,7	35	5,9	2	0,3
Choice 2	38	6,4	148	24,8	368	61,7	38	6,4	4	0,7
Choice 5	41	6,9	150	25,2	341	57,2	53	8,9	11	1,8
Choice 8	41	6,9	145	24,3	334	56	68	11,4	8	1,3
Choice 3	76	12,8	159	26,7	311	52,2	45	7,6	5	0,8
Choice 7	61	10,2	192	32,2	233	39,1	103	17,3	7	1,2

5.6 Differences between Groups

Whether there are any differences or not within five groups in ten questions is checked with Chi-Square test. The questions analyzed are 12, 13, 14, 16, 17, 18, 19 and 22 and the groups are genders, ages (≤ 40 vs. >40), education levels (have university degree vs. not), income groups (≤ 1600 vs. >1600) and geographical region groups. There are some significant differences within the groups of genders, ages, education levels and geographical regions. However, there is no meaningful or significant difference within income groups for all the items.

Details about the compare groups are as follows.

5.6.1 Genders

Women and men have significantly different views on Item 13 (Sig. 0,001) which asks their opinion about if the current health information which exists about them is safe and secure? Unlike women, men do not think that their medical data are safe and secure (See Figure 7). There is no significant difference between genders in Items 12 and 14.

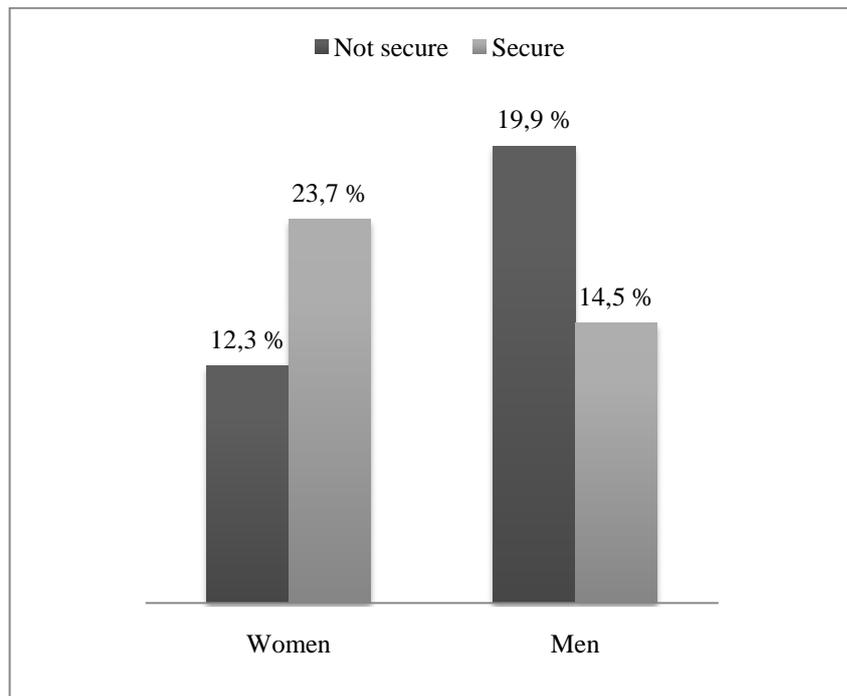


Figure 7 Bar graph of the comparison between women and men on their opinions about the security of their medical information

Statistical results show that there are significant differences between the ideas of men and women regarding Item 16. Both of the genders trust in their doctors but do not trust in private sector health researchers. Nevertheless, the percentage of women who trust in doctors is larger than that of men (Sig. 0,028). As for private sector health researchers, the percentage of the women who voted for the choice “Don’t trust” is less than that of men (Sig. 0,018).

Table 18 Comparison between women and men about their trust levels in the doctors and private sector health researchers about the privacy of medical information

		Women		Men		Sig.*
		n	%	n	%	
Doctors	Don't trust	25	11	46	18,1	0,028
	Trust	202	89	208	81,9	
Private sector health researchers	Don't trust	114	66,3	177	77	0,018
	Trust	58	33,7	53	23	

* *Chi Square test*

In Items 17, 18 and 19, which are about awareness levels of people about laws and regulations in Turkey, there are no significant differences between the answers of genders.

There are some differences between genders about access rights for groups in Item 22, which asks how much access to their medical records they are willing to give to some presented groups. Men and women want significantly different access levels (Sig. 0,01) for their wives and husbands. According to the results, unlike women, men tend to give more access rights to their wives (See Figure 8).

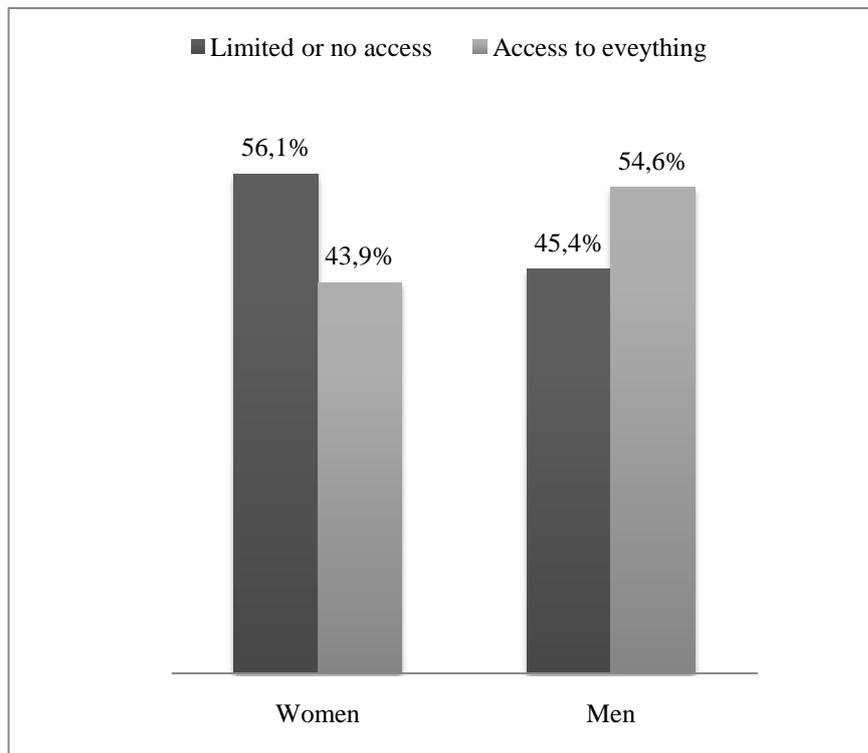


Figure 8 Bar graph of the comparison between women and men on their opinions about access limits to their records of their spouses

Item 22 has significant different results between genders on access limits of respondents' employers (Sig. 0,007) and pharmacy (Sig. 0,01). 97% of women give no access or limited access to their employers but this percentage is 91,8 for men (No access and Limited access choices are combined for analysis). On the other hand, men are more likely to give no access or limited access rights to pharmacies. Table 19 gives detailed information about these results.

Table 19 Comparison of women and men on their opinions about access limits to their records of their employer and pharmacies

		Women		Men		Sig.*
		n	%	n	%	
Your employer	No access or limited access	260	97	279	91,8	0,007
	Access to everything	8	3	25	8,2	
Pharmacies	No access or limited access	231	88,5	287	94,4	0,01
	Access to everything	30	21,7	17	5,6	

* *Chi Square test*

5.6.2 Age Groups (Older people vs. Younger people)

The age of 40 was chosen for cut point of ages in this analysis because 40 is an important age for information age. 40 years old people do not mainly deal with computers, the Internet or other technologic developments. Moreover, in Turkey education level of older ages are generally lower than younger ages. In the results of the instrumentation this distinctions are obvious too. 32,5% of older ages has computer knowledge below the average but only 3,1% of the younger ages have lack of computer knowledge. 37,7% of the elderly do not have graduate degree on the other hand this percentage is only 9,1% for younger people.

There are no significant differences between age groups (≤ 40 and >40) within the Items 12, 13, 14, 16, 17, 18 and 19.

The answers about the access limits (Item 22) differed in two of the choices: access limits of their spouses and parents or children. Unlike young people, most of the older people give more access rights to their spouses (No access and Limited access choices are combined for analysis). This situation is the same for parents and children's access right; that is, the elderly tend to give more access rights for their children or parents than younger people. There is also a significant difference (Sig. 0,000) between the answers of the groups about access limits of their employers but they both give no access or limited access rights to their employers. Percentage of young group who made these choices is more than that of the elderly. Table 20 gives details about these comparisons.

Table 20 Comparison between younger and elder people on their opinions about access limits to their records of their spouses, parents/children and their employer

		Age≤40		Age>40		Sig.*
		n	%	n	%	
Your wife/ husband	No access or limited access	262	52,5	25	35,2	0,006
	Access to everything	237	47,5	46	64,8	
Parents/ children	No access or limited access	348	68,9	33	45,8	0,000
	Access to everything	157	31,1	39	54,2	
Your employer	No access or limited access	479	95,6	60	84,5	0,000
	Access to everything	22	4,4	11	15,5	

* *Chi Square Test*

Figure 9 is the graphical demonstration of the Table 20.

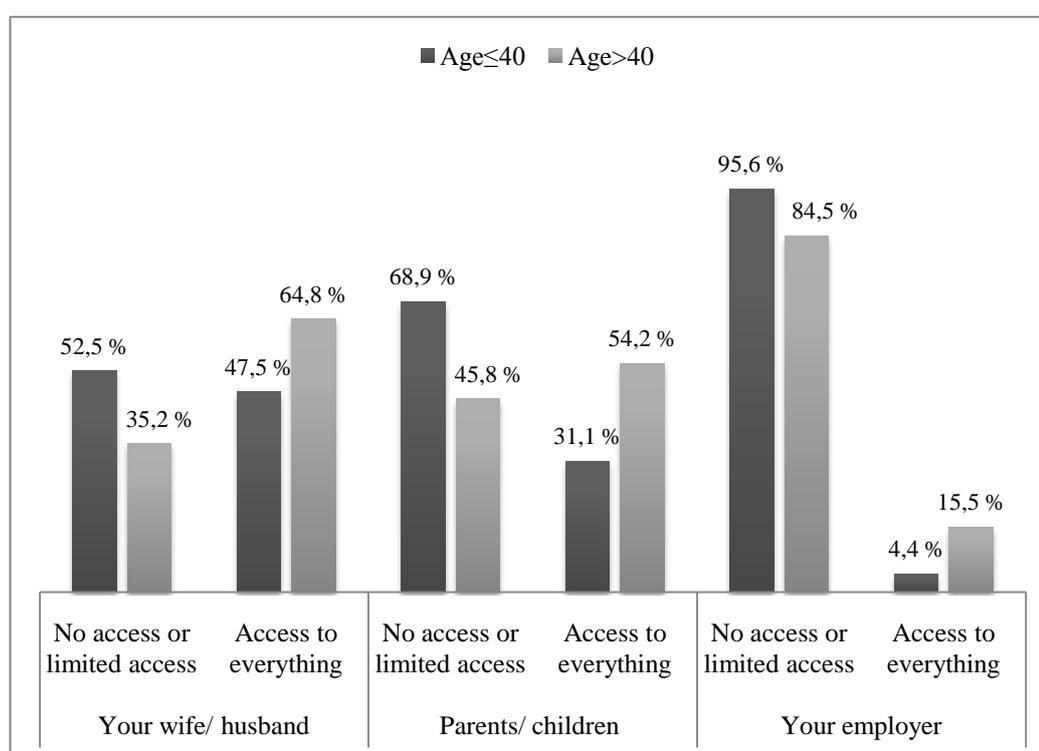


Figure 9 Bar graph of comparison between younger and older people on their opinions about access limits to their records of their spouses, parents/ children and their employer

5.6.3 Education (Graduates vs. Non-graduates)

Education levels were divided into two subgroups for comparison; people who graduated from university and did not graduate from university. The main reason of this division is to answer the question if the university degree affects people's opinions and attitudes on the privacy of their medical data.

According to the results of the analysis, there is no significant difference between education groups in Items 12, 13, 14, 17, 18 and 19 but there is a significant difference (Sig. 0,044) about their trust levels in government. Both of the groups do not trust the Turkish government but graduate people voted for "Don't trust" choice more than non-graduates (See Table 21).

Table 21 Comparison between graduates and non-graduates on their trust levels in the government about the privacy of their medical information

		Don't have a graduate degree		Have a graduate degree		Sig.*
		n	%	n	%	
Government	Don't trust	32	55,2	272	68,5	0,044
	Trust	26	44,8	125	31,5	

* *Chi Square test*

Moreover, there is a significant difference (Sig. 0,000) between graduate and non-graduate people on their opinions about access limits of their doctors. Unlike graduate people, most of the lower educated people think that their doctors should have no access or limited access rights to reach their medical data (No access and Limited access choices are combined for analysis). Table 22 gives details about these comparisons. According to the results, both of the graduate and non-graduate people agree on the idea about their parents' and children's access right limits; they tend to give no access or limited access rights to their parents and children. However, there is a significant difference (Sig. 0,045) between their answers. The percentage of highly-educated (graduate) people who made the choice "No access" or "Limited access" is larger than that of non-graduate people.

Table 22 Comparison between graduates and non-graduates on their opinions about access limits to their records of parents/ children and their doctors

		Don't have a graduate degree		Have a graduate degree		Sig.*
		n	%	n	%	
Parents/ children	No access and limited access	40	55,6	341	67,5	0,045
	Access to everything	32	44,4	164	32,5	
Your doctor	No access and limited access	39	53,4	161	31,9	0,000
	Access to everything	34	46,6	344	68,1	

* *Chi Square test*

5.6.4 Geographical Regions

The participants in this study are from six different regions of Turkey, namely;

- Inner Anatolia Region
- Aegean Region
- East Regions
- Mediterranean Region
- Black Sea Region
- Marmara Region

There are from 42 to 178 participants who represent each of the regions. Nevertheless, there are significant differences between regions about education (Sig. 0,000) and age (Sig. 0,001) levels.

There is a significant difference between (Sig. 0,012) these six regions on Item 12 which asks if they feel comfortable about computer usage in health-care. The participants from all the regions feel comfortable but the participants from Aegean Region has the biggest percentage (98,6%) and East Regions has the least one (75%). Table 23 gives details about these comparisons. According to the results of Fisher's exact test, the differences on Item 12 are between Inner Anatolia Region - Aegean Region (Sig. 0,020) and Aegean Region - East Regions (Sig. 0,001).

Table 23 Comparison between the regions of Turkey about comfort levels on computer usage

Item 12: Do you feel uncomfortable with doctors and other health care professionals using computers to record and share personal health information within the health care system?													
Regions:	Inner Anatolia		Aegean		East		Mediterranean		Black Sea		Marmara		Sig.*
	n	%	n	%	n	%	n	%	n	%	n	%	
Feel	12	10	1	1,4	7	25	5	12,5	7	14,6	11	8,3	0,012
Don't feel	108	90	68	98,6	21	75	35	87,5	41	85,4	122	91,7	

* Chi Square test

There are also significant different views among six regions on five choices of Item 16 (1, 3, 4, 5, and 6) which asks whether the participants trust in the presented people or associations or not. The whole regions trust in their doctors (Sig. 0,025) and the percents are quite similar to each other but East Regions has the least percent among the regions (64,5%). Trust levels about pharmacies are also significantly different among regions (Sig. 0,021). However, this time the views on trust level about pharmacies differ region to region. The participants from Black Sea Region (55,6%) and East Regions (60,6%) generally do not trust in pharmacies but the rest of the regions think opposite. Black Sea Region has also significantly different view (Sig. 0,000) about trusting in government. Unlike other regions most of the participants from Black Sea Region trust government about their medical information's privacy (53,6%). Moreover, there is a significant difference (Sig. 0,024) between regions about trust levels in insurance companies. Percent of the participant who chose "Don't trust" choice is the biggest in East Regions (86,1%). Lastly, ideas about if the participants trust in information specialists or not are significantly different (Sig. 0,040) among the regions, as well. Table 24 shows the details about these comparisons. Views of Aegean Region and East Regions are significantly different on Choice 1 (Sig. 0,004) and Choice 3 (Sig. 0,014). Besides of this, Marmara Region and Black Sea Region are significantly different views on Choice 3 (Sig. 0,01), Choice 4 (Sig. 0,035) and Choice 6 (Sig. 0,01). There are also significant differences on Choice 1 (Sig. 0,044) and Choice 4 (Sig. 0,007) between East Regions and Mediterranean Region. Lastly, people from Mediterranean Region and Black Sea Region have significantly different opinions about Choice 6 (Sig. 0,030).

Table 24 Comparison between the regions of Turkey about whether they trust the people or associations presented

Item 16: Do you trust the following people or association?													
Choice 1: Your doctor													
Regions:	Inner Anatolia		Aegean		East		Mediterranean		Black Sea		Marmara		Sig.*
	n	%	n	%	n	%	n	%	n	%	n	%	
Don't trust	16	12,9	9	11,5	11	35,5	8	16	10	17,5	17	12,1	0,025
Trust	108	87,1	69	88,5	20	64,5	42	84	47	82,5	124	87,9	
Choice 3: Pharmacies													
Regions:	Inner Anatolia		Aegean		East		Mediterranean		Black Sea		Marmara		Sig.*
	n	%	n	%	n	%	n	%	n	%	n	%	
Don't trust	50	45	26	35,1	20	60,6	19	47,5	30	55,6	43	35	0,021
Trust	61	55	48	64,9	13	39,4	21	52,5	24	44,4	80	65	
Choice 4: Government													
Regions:	Inner Anatolia		Aegean		East		Mediterranean		Black Sea		Marmara		Sig.*
	n	%	n	%	n	%	n	%	n	%	n	%	
Don't trust	89	74,8	56	75,7	29	82,9	22	53,7	26	46,4	82	63,1	0,000
Trust	30	25,2	18	24,3	6	17,1	19	46,3	30	53,6	48	36,9	
Choice 5: Insurance company													
Regions:	Inner Anatolia		Aegean		East		Mediterranean		Black Sea		Marmara		Sig.*
	n	%	n	%	n	%	n	%	n	%	n	%	
Don't trust	97	82,9	64	82,1	31	86,1	26	60,4	33	66	95	76,6	0,024
Trust	20	17,1	14	17,9	5	13,9	15	36,6	17	34	29	23,4	
Choice 6: Information specialists													
Regions:	Inner Anatolia		Aegean		East		Mediterranean		Black Sea		Marmara		Sig.*
	n	%	n	%	n	%	n	%	n	%	n	%	
Don't trust	67	70,5	57	77	26	88,7	28	70	40	88,9	71	68,9	0,040
Trust	28	29,5	17	23	3	10,3	12	30	5	11,1	32	31,1	

* Chi Square test

There are significant differences between the views of the participants from different regions on the choices of Item 22 (1, 2, 5, and 6) which is about how much access the participants are willing to give presented people or groups. Bigger percents of participants from all the regions are willing to give the right to access to everything to themselves but there is still a significant difference (Sig. 0,030) between regions. Mediterranean Region has the biggest percent with 96,6 and the least one is East Regions with 85,7. Views on spouses' access rights differ from region to region (Sig. 0,023), as well. Participants from Inner Anatolia and East Regions give mostly limited or no access rights to their spouses but the rest of the regions give mostly access to everything right to their spouses. Moreover, views on access rights of doctors also significantly differ (Sig. 0,045) among regions. Percents of Inner Anatolia and Marmara Regions' participants are the biggest ones with 70,2. Lastly, opinions about other doctors or hospital staff's access rights are significantly different (0,043) among the regions. %97,4 of the participants from East Region

chose “No access” or “Limited access” right choices for other doctors or hospital staff. Table 25 gives the details about these comparisons. Views of people from Aegean Region and Inner Anatolia are significantly different on Choice 2 (Sig. 0,034). In addition to this, Marmara Region and Black Sea Region are significantly different views on Choice 1 (Sig. 0,016) and Choice 6 (Sig. 0,026). There are also significant differences on Choice 2 (Sig. 0,04) and Choice 6 (Sig. 0,007) between East Regions and Aegean Region. People from Mediterranean Region and Black Sea Region have significantly different opinions about Choice 1 (Sig. 0,021), as well. Lastly, East Regions and Mediterranean Region have significantly different views on Choice 2 (Sig. 0,05) and Choice 6 (0,045).

Table 25 Comparison between regions of Turkey on how much access rights they are willing to give to some presented people or groups

Item 22: How much access are you willing to give to some presented people or groups?													
Choice 1: Yourself													
Regions:	Inner Anatolia		Aegean		East		Mediterranean		Black Sea		Marmara		Sig.*
	n	%	n	%	n	%	n	%	n	%	n	%	
No access and limited access	17	11,2	5	5,2	6	14,3	2	3,4	11	16,2	11	6,3	0,030
Access to everything	135	88,8	92	94,8	36	85,7	56	96,6	57	83,8	164	93,7	
Choice 2: Your wife or husband													
	n	%	n	%	n	%	n	%	n	%	n	%	
No access and limited access	87	59,2	43	45,3	25	67,6	27	47,4	29	43,9	76	45,2	0,023
Access to everything	60	40,8	52	54,7	12	32,4	30	52,6	37	56,1	92	54,8	
Choice 5: Your doctor													
	n	%	n	%	n	%	n	%	n	%	n	%	
No access and limited access	45	29,8	32	33,7	19	50	26	44,8	27	41,5	51	29,8	0,045
Access to everything	106	70,2	63	66,3	19	50	32	55,2	38	58,5	120	70,2	
Choice 6: Other doctors or hospital staff													
	n	%	n	%	n	%	n	%	n	%	n	%	
No access and limited access	125	86,8	77	81,1	37	97,4	47	83,9	60	95,2	137	84	0,043
Access to everything	19	13,2	18	18,9	1	2,6	9	16,1	3	4,8	26	16	

* *Chi Square test*

CHAPTER 6

DISCUSSION

In the literature, there is no study on people's attitudes and opinions about the privacy and confidentiality of electronic health records in Turkey. This study presents a large overview on the opinions of people who use medical services in Turkey about computerized medical information's effects on privacy and confidentiality. In the Introduction section (Chapter 1), under purpose of the study section seven research questions were proposed and in the Results part (Chapter 6), the statistical analysis based on these research questions was presented.

According to the participants' experiences, very little percentage of people or a member of their families have experienced a serious breach of their health information. In the results of the survey in Canada (EKOS Research Associates, 2007), this percentage is four times more than Turkey. Moreover, the percentages of the people, who have asked a doctor not to write down their health problem in their medical records, or have asked the doctor to put a less serious or less embarrassing diagnosis into the record than was actually the condition, in the USA (Princeton Survey Research Associates, 1999) are two times more than the percentages in Turkey. However, the percentage of the people who prefer not be tested because of their concern about that others might learn about the results, in Turkey is , very high, six times more than the percentage of the people in the USA (Princeton Survey Research Associates, 1999). Also, for the results of a literature review study, which review lots of papers published about this topic, patients tended to postpone or give up the treatment, or change the inception or the total story of their illness because of the concerns about confidentiality (Sankar et al., 2003). These results can be

interpreted that a lot of people are afraid of breach of their medical records in Turkey as well and even more.

Therefore, they choose wrong methods in order to avoid it. To do so, most of the people abstain from being tested. This result is the most alarming finding of the study and it should be taken under control immediately. The attitude “refraining from being tested for the illness” can cause irreparable results such as being late for a fatal illness’s treatment or spreading an incurable illness to more people. Hence, necessary measures should be taken immediately such as serious punishments for invasions of medical data or giving patients the opportunity to hide sensitive medical information.

According to the results of the statistical analysis, a big majority of participants do not feel uncomfortable about computer usage for treatment purposes. In the survey conducted in Canada, (EKOS Research Associates, 2007) 73% of the respondents feel also comfortable with computer usage for medical purposes. Similar results show that computer usage in medical area do not disturb people in general.

The participants seem uncertain about whether their health information is safe and secure in Turkey. In Canada, a similar question in the survey (EKOS Research Associates, 2007) shows quite different results. More participants in Canada think their health information is safe and secure than in Turkey. However, like the people in the USA, participants of this survey have also concerns about the invasion of their personal information (Princeton Survey Research Associates, 1999). Very little and close percentages of people in both countries have no concern (~10%). In the UK the patients also feel uncomfortable about the confidentiality of electronic health records (Carman & Britten, 1995). To sum up, unlike Canadian people, the participants are not sure about the privacy of their information in Turkey and do not feel comfortable about the privacy of their medical information similar to the participants from the USA and the UK.

American people think the biggest threat to the privacy and confidentiality of personal medical records kept on computer-based systems can more likely be access of unauthorized people (Princeton Survey Research Associates, 1999). On the other hand, people in this survey in Turkey mostly see access of authorized and

unauthorized people equally dangerous. This result can be interpreted that a big majority of people do not trust even executive people and this is a very big problem, against which the government should take immediate measures such as establishing new regulations with serious punishments for people or organizations even for public servants that violate medical privacy and requiring doctors, hospital, and other health facilities to set up security systems on their computer and regular audits of them should be done by the government.

According to the results, the sequence of groups and people in terms of trust levels from maximum to minimum is doctors, pharmacists, nurses and other hospital staff, government, insurance company and lastly information technology specialists. The sequence of the researchers is health researchers in universities, government health researchers and lastly private sector health researchers. These results are quite similar to the results of the survey Electronic Health Information and Privacy Survey: What Canadians Think 2007 (EKOS Research Associates, 2007) but there are small nuances. In Canada, people trust nurses as much as pharmacists and they see insurance companies less trustful than information technology specialists. Moreover, Canadian people think that private sector health researchers are the most trustful among researchers but in Turkey the most trustful ones are university researchers. Except these small differences it can be said that in general, people intend to trust people who are directly related to their treatment more than the government or insurance companies. These results may help understand with whom the participants want to share their medical records more in Turkey and thus taking these into consideration, new arrangements may be done.

The answers of the questions about regulations show that people are not aware of the laws and regulations in Turkey. Approximately 70 percent of the people have chosen the “Don’t know” choices of the regulation questions. After the examination of plenty of studies about electronic health records’ privacy, it is indicated that there are confusions about medical confidentiality’s legal, ethical and practical limits among patients (Sankar et al., 2003). According to the results of the survey conducted in the USA (Princeton Survey Research Associates, 1999), people in the USA are unaware of their rights too. Actually, in Turkey there are not enough laws or regulations

which protect the privacy of the personal data but there are still some and there is also a draft law approved with 2010 Referendum (Appendix D) and directly about personal data protection. The results show that public health messages that link technology, privacy, and health benefits are not delivered to people in Turkey. To overcome this problem, Turkish Ministry of Health should develop and execute a public awareness campaign to educate public about the privacy rights and protections provided. Moreover, laws and regulations about the privacy protections should be broadened immediately and they should be more vigorously enforced.

According to the results, people participated in the survey have concerns about the usage of T.C. identity number in health-care and they prefer a special number, instead. The studies conducted in New Zealand (Buckley et al., 2010), Ireland (Whiddett, 2006), UK (Barrett et al., 2006) and in Canada (Nair et al., 2004) also showed that people are not willing to share their identified information. Similarly, today T.C. identity number is easy to access via the Internet by anyone. Therefore, using a de-identified special number for medical data storage may be a better solution for privacy.

When the access rights were asked to the participants, a big majority of the people gave the right to access everything to themselves and then their doctors and husbands/wives. It is interesting that most of Americans (Princeton Survey Research Associates, 1999) think that doctors should access to everything. However, less people want to access to everything in their records. Moreover, the participants believe that insurance companies, pharmacies, their employers and drug companies should not be able to access their records. These results can be inspiration for new policies about access rights to personal information. For example, the right for patients to hide or mask sensitive information from some users who would be authorized to access their health records whenever patients want, necessitating using information that doesn't personally identify patient for purposes not for healthcare, and getting patients' permission prior to using or distributing any of their medical information can be some of these policies.

People think that legislations suggested in the survey in order to protect privacy and confidentiality would be “very” effective. The proposed policies are actually essentials of data privacy. For example, requiring permission prior to using or distributing any medical information legislation is an unwritten rule in Turkey, as well but it is not taken into consideration. The other suggestions are having the right to see when and by whom their records are retrieved, establishing new legislations with serious punishments for people or organizations that violate medical privacy, requiring doctors, hospital, and health plans to set up security systems on their computers, having the right to see and make corrections in their own medical records, having the right to hide or mask sensitive information to some users who would be authorized to access their health records, regular audits undertaken by government for the privacy and security provisions of an electronic health system health records, and requiring using information that doesn’t personally identify people for purposes besides healthcare whenever they want (such as researches) should become laws and be enforced in order to ensure data privacy.

Statistical results show that there are some significant differences between genders about their opinions and attitudes toward privacy issues. Most of the women think their health information is safe and secure in Turkey, but male participants think the opposite. Besides, the question about access limits of their spouses (Item 22) has different answers among genders. Men give more access rights to their wives than women do. There are discriminations between men and women in all societies and this discrimination is very obvious in Turkey. It is women that undergo the negative effects of this discrimination (Terzioğlu, Taşkın, 2008). Therefore, these findings are consistent with this common knowledge. Because of social pressure, women do not feel as comfortable as men about indication of their private information to their husbands.

Results identified that older people think different from younger people about access limits. Young people are in favor of having more protected personal data. Unlike the elderly, they are reluctant to share their medical information with their spouses and their parents or their children. These results are also parallel to the results of the study conducted in Ireland in 2010 (Buckley et al., 2010). According to the results,

unlike younger people, elderly and retired people agreed that any personal medical information could be shared. Nevertheless, education level is not a factor that affects information sharing as in this survey (Buckley et al., 2010). According to the results, however, education level plays a prominent role in people's opinions about the privacy of electronic medical records but highly-educated people prefer more access rights for their doctors in Turkey.

According to the results of the study there are significant differences between six regions views on some questions. These results are valuable but as it was mentioned under the title age and education levels of the regions are also significantly different from each other and they do not represent the regions of Turkey. Hence these results can occur coincidentally.

CHAPTER 7

CONCLUSION

Today, computerized systems are used almost in every area and especially for public utility. Health-care is one of the largest areas of usage. Storage of medical data in electronic databases is widely used in Turkey. Necessarily, opinions of the system users should be asked before these kinds of systems are implemented. However, in the literature, there is no example of such research studies conducted in Turkey. In this manner, this study will contribute a lot to the literature.

The sample consists of 596 people from 64 different cities in six geographical regions of Turkey in order to figure out their attitudes and opinions about privacy of their medical information in electronic environment. The results of the study show that people feel comfortable about computer usage in health-care. However, they are not sure if their medical information is safe and secure in electronic environment, and they are concerned about the privacy of their data. Moreover, the respondents think that disclosure of their medical information by authorized and unauthorized is equally dangerous. Almost all of the participants were unaware about the entire three regulations asked in the survey. According to the results, participants have concerns about the usage of T.C. Identity number for medical data storage, which is why they prefer a unique number instead. The respondents think that all of the suggested legislations in the survey would be very effective. The findings of the study also show that people trust in their doctors, health researchers in universities, pharmacist, nurses and other hospital staff but do not trust in insurance companies, government, private sector health researchers, information technology specialists and government health researchers in descending order. The respondents give themselves, their

doctors and spouse the right to access everything in their medical records. They give other doctors or staff, and parents and children limited access rights. Lastly, they do not give any access right to drug companies, their employers, pharmacies and their insurance companies.

There are some significant differences between the groups (ages, genders, education levels and geographical regions). Unlike women, men do not think that their medical data are safe and secure and they tend to give more access rights to their wives. Unlike the elderly, most of the younger people give less access rights to their spouses, parents and children. Lower educated people think that their doctors should have no or limited rights to access their medical data but highly-educated people think the opposite.

This study will help understand whom people trust about the privacy of their medical data and with whom they want to share them. Moreover, their concerns about current system and awareness levels about laws and regulations will be understood with the results of the study. These contributions will be valuable for inspiring Turkish Ministry of Health to increase the public awareness about the privacy rights and protections provided. Furthermore, laws and regulations about the privacy protections may be broadened and more vigorously enforced to reduce public concerns. A unique de-identified number for medical data storage may be used to prevent invasions and this will reduce people's concerns about their privacy. The study proposed several implications to reduce people concern levels about privacy of their records. Requiring patient's permission before using or distributing any of their medical information; having the right to see when and by whom their records are retrieved; establishing new legislations with serious punishments for people or organizations that violate medical privacy; requiring doctors, hospital, and other health facilities to set up security systems on their computers; having the right to see and make corrections in their own medical records; having the right to hide or mask sensitive information from some users who would be authorized to access their health records; regular audits undertaken by government for the privacy and security provisions of an electronic health system health records; getting patients' permission

prior to using or distributing any of their medical information are above-mentioned suggestions.

7.1 Shortcomings and Future Works

The sample size is large enough to compare many of the groups but some of them had still small sizes. For example, lower educated, older ages and lack of computer literacy groups occupy a small percentage of the participant. The main reason of this is that the questionnaire was conducted via the Internet. Because of the need for computer usage, people who completed the online questionnaire were mostly younger ages, higher educated and not surprisingly have higher level of computer literacy. Consequently, generalization cannot be made for Turkish public since the sample profile is not a mirror of Turkish public.

Although reaching to the elderly and/or lower educated people was necessary in order to figure out the public opinions and to make comparisons between age and education level groups, it was not possible not only because of internet usage but also because of complexity of the questions for them. Many of the questionnaires which were filled by these groups were not completed properly or the answers were generally “Don’t know”, “Not sure”, etc.

In online questionnaire, people were more honest about their past experiences when it was compared to paper based ones. However, according to the notes they wrote at the end of the questionnaire, there were even some people worried about disclosure by the one who conducted the survey.

Also, as another limitation, because of the new law changes, it is not easy to be sure if they have meant that laws when they chose the correct answers. Therefore, this study should be repeated several years later.

Future studies should conduct a public research and thus they can identify what the public are thinking about the privacy of their health records and whether they are aware of the new regulations and legislations.

REFERENCES

Aspden, P., & Institute of Medicine, authors. (2004). *Patient safety: achieving a new standard for care*. National Academies Press.

Akyüz, E. B. (2008). *The opinions of patients and their nurses about the effects on privacy of the nursing care practices in patients having surgery* (Master's thesis). Available from National Thesis Center of the Turkish Council of Higher Education Dissertations and Theses database. (UMI No. 225956)

Alpar, R. (2006). *Spor bilimlerinde uygulamalı istatistik: Ki-kare testleri*. Nobel: Ankara

Ary, D., Jacobs, L. C., & Razavieh, A. (2002). *Introduction to Research in Education*. USA, Belmont: Thomson Learning.

Babbie, E. (1990). *Survey research methods: Pretests and pilot studies*. California: Wadsworth Publishing Company.

Barrett, G., Cassell, J. A., Peacock, J. L., & Coleman, M. P. (2006). National survey of British public's views on use of identifiable medical data by the National Cancer Registry. *BMJ : British Medical Journal*, 332(7549), 1068-1072. doi:10.1136/bmj.38805.473738.7C

Baumer, D., Earp, J. B., & Payton, F. C. (2000). Privacy of medical records: IT implications of HIPAA. *ACM SIGCAS Computers and Society*, 30(4), 40–47.

Bellman, S., Johnson, E. J., & Lohse, G. L. (2001). To opt-in or opt-out? It depends on the question. *Communications of the ACM*, 44(2), 25–27.

Berber, L., K., Ülgü, M., M., Er, C. (2009). *Elektronik sağlık kayıtları ve özel hayatın gizliliği*. İstanbul: Karakter Color

Buckley, B. S., Murphy, A. W., & MacFarlane, A. E. (2010). Public attitudes to the use in research of personal health information from general practitioners' records: a survey of the Irish general public [Abstract]. *Journal of Medical Ethics*. doi:10.1136/jme.2010.037903

Carman, D., & Britten, N. (1995). Confidentiality of medical records: the patient's perspective. *The British Journal of General Practice*, 45(398), 485.

EKOS Research Associates(2007). *Electronic Health Information and Privacy Survey: What Canadians Think*. Ottawa

Fischer-Hübner , S. (2001). *IT-Security and privacy - design and use of privacy-enhancing security mechanism*. New York : Springer

Friedman, C. P., & Jeremy, C. W. (1997). *Evaluation methods in medical informatics*. New York: Springer - Verlag.

Gostin, Lawrence.(1997). Health care information and the protection of personal privacy: ethical and legal considerations. *Annals of Internal Medicine*, 127(8), 684-690.

Grimes, D. A., & Schulz, K. F. (2002). Descriptive studies: what they can and cannot do. *The Lancet*, 359(9301), 145-149. doi:10.1016/S0140-6736(02)073737

Huang, L., Chu, H., Lien, C., Hsiao, C., & Kao, T. (2009). Privacy preservation and information security protection for patients' portable electronic health records. *Comput. Biol. Med.*, 39(9), 743-750.

Huck, C. W. (2004). *Reading statistics and research*. USA: Pearson Education Inc.

Hennekens, C. H., & Buring, J. E. (1987). *Epidemiology in medicine*. Boston: Little, Brown and Company.

Johnson, E. J., Bellman, S., & Lohse, G. L. (2002). Defaults, framing and privacy: Why opting in-opting out 1. *Marketing Letters*, 13(1), 5–15.

Junghans, C., Feder, G., Hemingway, H., Timmis, A., & Jones, M. (2005). Recruiting patients to medical research: double blind randomised trial of "opt-in" versus "opt-out" strategies. *BMJ*, 331(7522), 940-0. doi:10.1136/bmj.38583.625613.AE

Kalra, D. (2006). Electronic health record standards. *IMIA Yearbook of Medical Informatics*, 2006, 136–144.

Knupfer, N. N., & McLellan, H. (1996). Descriptive research methodologies in jonassen, D. H. (Eds.), *Handbook of Research for Educational Communications and Technology* (1196-1212). New York: Simon & Schuster Macmillan.

Landi, W., & Rao, R. B. (2003). Secure de-identification and re-identification. *AMIA Annu Symp Proc 2003*(1), 905-905.

MacKenzie, M. A. (2004). *A Dissertation submitted to the Faculty of Claremont Graduate University in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the Graduate Faculty of Political Science* (Doctoral dissertation). Available from Proquest Dissertations and Theses database. (UMI No. 3383635)

Mutch, L., & King, R. (1985). Obtaining parental consent--opting in or opting out? *Archives of Disease in Childhood*, 60(10), 979-980. doi:10.1136/adc.60.10.979

Nair, K., Willison, D., Holbrook, A., & Keshavjee, K. (2004). Patients' consent preferences regarding the use of their health information for research purposes: a qualitative study. *Journal of Health Services Research & Policy*, 9(1), 22.

Neamatullah, I., Douglass, M. M., Lehman, L. H., Reisner, A., Villarroel, M., Long, W. J., Szolovits, P., et al. (2008). Automated de-identification of free-text medical records. *BMC Medical Informatics and Decision Making*, 8(1), 32.

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), 351–358.

Pallant, J. (2007). *SPSS survival manual*. Buckingham: Open University Press.

Pankaj, J. R., & Rohatgi, P. (2000). Proceedings from the 9th USENIX Security Symposium'00: *Can Pseudonymity Really Guarantee Privacy?*. p.7-7. Denver, Colorado

Princeton Survey Research Associates (1999). Medical privacy and confidentiality survey. California.

Pullman, D., Buehler, S. K., Felt, L. , Gallagher, K., House, J., Keough, T. M. Ryan, A. (2009). Sorry, you can't have that information: data holder confusion regarding privacy requirements for personal health information and the potential chilling effect on health research. *Healthcare Policy*, 4(4), 61-76.

Rada, R. (2003). *HIPAA@IT essentials: Health information transactions, privacy, and security, 2nd Edition*. Baltimore: HIPAA-IT LLC

Re-identification. (n.d.). *In EPIC*. Retrieved November 2, 2010 from <http://epic.org/privacy/reidentification/>

Rindfleisch, T. C. (1997). Privacy, information technology, and health care. *Communications of the ACM*, 40(8), 92-100. doi:10.1145/257874.257896

Safran, C., Bloomrosen, M., Hammond, W. E., Labkoff, S., Markel-Fox, S., Tang, P. C., & Detmer, D. E. (2007). Toward a national framework for the secondary use of health data: An american medical informatics association white paper. *Journal of the American Medical Informatics Association : JAMIA*, 14(1), 1-9. doi:10.1197/jamia.M2273

Sankar, P., Mora, S., Merz, J. F., & Jones, N. L. (2003). Patient perspectives of medical confidentiality. *Journal of General Internal Medicine*, 18(8), 659–669.

Silversides, A. (2010). “Chaos” protects health privacy. *CMAJ*, 182(1), E37-E38. doi:10.1503/cmaj.109-3115

Smith, E., & Eloff, J. H. P. (1999). Security in health-care information systems—current trends. *International Journal of Medical Informatics*, 54(1), 39–54.

Solís, C. F. (n.d.). De-identification and Re-identification. In *The University of Texas Health Science Center Website*. Retrieved November 2, 2010, from: http://www.uth.tmc.edu/hipaa/policies/Section_05.01_De-identification_and_Re-identification.html

Terziođlu, F., & Tařkın, L. (2008). Kadının toplumsal cinsiyet rolünün liderlik davranıřlarına ve hemřirelik mesleđine yansımaları. *C.Ü. Hemřirelik Yüksekokulu Dergisi*, 12(2), 62-67

Tracy, C. S., Dantas, G. C., & Upshur, R. E. (2004). Feasibility of a patient decision aid regarding disclosure of personal health information: qualitative evaluation of the Health Care Information Directive. *BMC Medical Informatics and Decision Making*, 4(1), 13.

Turkish Ministry of Health: *Kiřisel Sađlık Kayıtlarının Güvenliđi Politikası*. (2005). Retrieved from: http://www.istanbulsaglik.gov.tr/w/mev/mev_gen/01249.pdf

Turkish Ministry of Health: *Personel İin Bilgi Güvenliđi Politikası*. (2007). Retrieved from: http://www.kdh.gov.tr/bilgi_guvenligi_politikasi.htm

Turkish Ministry of Health: *Yataklı Tedavi Kurumları Tıbbi Kayıt Ve Arřiv Hizmetleri Yönergesi*. (2001). Retrieved from: <http://www.saglik.gov.tr/TR/belge/1-2460/yatakli-tedavi-kurumlari-tibbi-kayit-ve-arsiv-hizmetler-.html>

Turkish Ministry of Health: *Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arřiv Hizmetleri Yönergesinde Deđişiklik Yapılmasına Dair Yönerge*. (2004). Retrieved from: <http://www.saglik.gov.tr/TR/belge/1-4688/eski2yeni.html>

Turkish Ministry of Health: *Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arřiv Hizmetleri Yönergesinde Deđişiklik Yapılmasına Dair Yönerge*. (2007). Retrieved from: <http://www.saglik.gov.tr/IODB/belge/1-4688/yatakli-tedavi-kurumlari-tibbi-kayit-ve-arsiv-hizmetler-.html>

Turkish Ministry of Health: *Yöneticiler İin Bilgi Güvenliđi Politikası*. (2007). Retrieved from: <http://www.muglasm.gov.tr/files/bilgiguvenligi/yonetici.pdf>

Whiddett, R., Hunter, I., Engelbrecht, J., & Handy, J. (2006). Patients' attitudes towards sharing their health information. *International Journal of Medical Informatics*, 75(7), 530–541.

Wingo P., Higgins J., Rubin G., & Zahniser S. (1994). *An epidemiologic approach to reproductive health*. Geneva: WHO

Whiddett, R., Hunter, I., Engelbrecht, J., & Handy, J. (2006). Patients' attitudes towards sharing their health information. *International Journal of Medical Informatics*, 75(7), 530–541.

APPENDICIES

APPENDIX A: QUESTIONNAIRE - Demographic Information

1. Yaşadığınız şehir: (.....)
2. Yaşınız: (.....)
3. Cinsiyetiniz: a. Kadın b. Erkek
4. Eğitim durumunuz?
a. İlkokul b.Ortaokul c. Lise d.Üniversite e.Diğer(.....)
5. Aylık geliriniz: (.....TL)
6. Evinizde bilgisayarınız var mı?
a. Evet b. Hayır
7. Bilgisayar kullanma becerileriniz için ne söyleyebilirsiniz?
a. Ortalamanın altında
b. Ortalama
c. Ortalamanın üzerinde
d. Bilgisayar kullanmayı bilmiyorum
8. Genel olarak sağlık durumunuzu nasıl değerlendirirsiniz?
a. Çok kötü b. Kötü c. Orta d. İyi e. Çok iyi

9. Daha önce sizin ya da aile bireylerinizden birisinin kişisel sağlık bilgileri rızanız dışında uygun olmayan amaçlar için kullanıldı ya da yayınlandı mı?

a. Evet b. Hayır c. Cevap vermek istemiyorum

10. Daha önce başkalarının sonucu görmesinden çekindiğiniz için sağlık durumunuzu test ettirmediğiniz bir durum yaşadınız mı?

a. Evet b. Hayır

11. Daha önce doktorunuzdan teşhisinizi sağlık kayıtlarınıza geçirmemesini veya teşhisinizin yüz kızartıcı olduğunu düşündüğünüzden başka bir teşhis yazmasını talep ettiniz mi?

a. Evet b. Hayır

APPENDIX B: QUESTIONNAIRE - Level of Concern

12. Doktorların ya da diğer sağlık çalışanlarının bilgilerinizi kayıt ederken ve/veya paylaşırken bilgisayar kullanmaları konusunda rahatsızlık hissediyor musunuz?
- Hissediyorum
 - Hissetmiyorum
 - Hiç düşünmedim
13. Size göre şundaki sağlık bilgileriniz ne kadar emniyette ve güvenli?
- Emniyette değil
 - Emniyette
 - Emin değilim/ Bilmiyorum
14. Türkiye’de kişisel bilgilerinizin ihlali konusunda ne kadar endişelisiniz?
- Endişeliyim
 - Endişele değilim
 - Hiç düşünmedim
15. Sizce Türkiye’de elektronik ortamda sağlık kayıtlarının tutulduğu bir sağlık sisteminde gizlilik ve mahremiyet açısından en büyük tehlike nedir?
- Bilgileri görme yetkisine sahip kişilerin (doktorlar, hemşireler, hastane yöneticileri...) bilgilerimi ifşa etmesi
 - Yetki sahibi olmayan kişilerin, bilgisayar sistemine gizlice girerek veya rüşvet vererek bilgilerime erişmesi ve ifşa etmesi
 - İkisi de eşit
 - Hiçbiri (Açıklayınız:.....)

16. Aşağıda bahsi geçen kişi ya da kurumlara tıbbi bilgilerinizin mahremiyeti konusunda ne kadar güvenirsiniz?

	Güvenmiyorum	Güveniyorum	Kararsızım
Doktorunuza;			
Hemşire ve diğer sağlık çalışanlarına;			
Eczacılara			
Devlete			
Sigorta şirketlerine			
Bilgisayar sistemlerini yürütmekle görevli uzmanlara			
Devlete bağlı sağlık araştırmacılarına			
Üniversitelere bağlı sağlık araştırmacılarına			
Özel sektöre bağlı sağlık araştırmacılarına			

APPENDIX C: QUESTIONNAIRE - Awareness about Laws and Regulations

17. Bildiđiniz kadarıyla řuanda Trkiye’de kiřiler kendi sađlık kayıtlarına eriřme, bunların dzeltilmesini veya silinmesini isteme hakkına sahipler mi?

a. Evet b. Hayır c. Bilgim yok

18. Bildiđiniz kadarıyla řuanda Trkiye’de tıbbi verilerinizin rızanız dıřında iřlenebilmesini nleyen yasalar var mı?

a. Evet b. Hayır c. Bilgim yok

19. Bildiđiniz kadarıyla řuanda Trkiye’de sađlık kayıtlarınıza internet zerinden ulařmanızı engelleyen herhangi bir yaptırım var mı?

a. Evet b. Hayır c. Bilgim yok

20. Tıbbi verilerinizin saklanması TC kimlik numarasının kullanılması konusunda endiřeleriniz var mı?

a. Evet b. Hayır

21. TC Kimlik Numarasının yerine sađlık hizmetinde kullanılacak zel bir numara verilmesini ister miydiniz?

a. Evet b. Hayır

22. Aşağıdaki bahsi geçen kişilerin sağlık kayıtlarınıza hangi derecede ulaşabilmesini isterdiniz?

	Erişemesin	Kısıtlı erişimi olsun	Her şeye erişebilsin	Kararsızım
Siz, kendiniz				
Evli iseniz; Eşiniz				
Ebeveyn ve/veya çocuklarınız				
Çalışıyorsanız; İşvereniniz				
Sigorta şirketiniz				
Doktorunuz				
Diğer doktor ve hastane personelleri				
Eczaneler				
İlaç şirketleri				

23. Aşağıda gizlilik ve mahremiyeti korumaya yönelik önerilen düzenlemelerin ne kadar etkili olabileceğini düşünüyorsunuz?

	Hiç	Az	Çok	Kararsızım
Sağlık bilgilerine izinsiz erişenlere yeni düzenlenecek yasalar vasıtasıyla ciddi yaptırımlar uygulanması				
Veri depolayan kişi ya da kurumların bilgisayarlarına verileri şifreleyen ve parola kullanılan sistemler gibi güvenlik sistemlerinin kurulmasını zorunlu hale getirmek				
Elektronik sağlık kayıt sisteminin güvenlik ve gizliliğinin hükümet organlarınca düzenli olarak denetlenmesi				
İstediginizde bilgilerinize kimin, ne zaman eriştiğini görebilmek				
Sağlık kayıtlarınıza dilediğiniz vakit ulaşabilmek, doğrulama yapabilmek ve düzeltmeleri rapor edebilmek;				
Herhangi bir tıbbi verinizin kullanılmasından veya dağıtılmasından önce izninizin alınması				
Sağlık hizmeti haricinde veri ihtiyacı durumunda kimlik bilgileri içermeyen verileri kullanmalarını sağlamak (araştırma...vb)				
Dilediğinizde tüm bilgilerinize erişim izni olan kişilerin hassas bilgilerinizi görebilmesini engelleyebilmek.				

APPENDIX D: 2010 REFERANDUM - İtem 20

TÜRKİYE CUMHURİYETİ ANAYASASININ BAZI MADDELERİNDE DEĞİŞİKLİK YAPILMASI HAKKINDA KANUN TEKLİFİ KARŞILAŞTIRMA TABLOSU 22.03.2010

1982 Anayasası	Teklif Metni
<p>X. Kanun önünde eşitlik</p> <p>MADDE 10 – Herkes, dil, ırk, renk, cinsiyet, siyasi düşünce, felsefi inanç, din, mezhep ve benzeri sebeplerle ayırım gözetilmeksizin kanun önünde eşittir.</p> <p>Kadınlar ve erkekler eşit haklara sahiptir. Devlet, bu eşitliğin yaşama geçmesini sağlamakla yükümlüdür.</p> <p>Hiçbir kişiye, aileye, zümreye veya sınıfa imtiyaz tanınamaz.</p> <p>Devlet organları ve idare makamları bütün işlemlerinde kanun önünde eşitlik ilkesine uygun olarak hareket etmek zorundadırlar.</p>	<p>X. Kanun önünde eşitlik</p> <p>MADDE 10 – Herkes, dil, ırk, renk, cinsiyet, siyasi düşünce, felsefi inanç, din, mezhep ve benzeri sebeplerle ayırım gözetilmeksizin kanun önünde eşittir.</p> <p>Kadınlar ve erkekler eşit haklara sahiptir. Devlet, bu eşitliğin yaşama geçmesini sağlamakla yükümlüdür. <u>Bu maksatla alınacak tedbirler eşitlik ilkesine aykırı olarak yorumlanamaz.</u></p> <p><u>Cocuklar, yaşlılar ve engelliler gibi özel surette korunması gerekenler için alınacak tedbirler eşitlik ilkesine aykırı sayılamaz.</u></p> <p>Hiçbir kişiye, aileye, zümreye veya sınıfa imtiyaz tanınamaz.</p> <p>Devlet organları ve idare makamları bütün işlemlerinde kanun önünde eşitlik ilkesine uygun olarak hareket etmek zorundadırlar.</p>
<p>A. Özel hayatın gizliliği</p> <p>MADDE 20 – Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. (Üçüncü cümle mülga: 3/10/2001-4709/5 md.)</p> <p>(Değişik: 3/10/2001-4709/5 md.) Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması</p>	<p>A. Özel hayatın gizliliği</p> <p>MADDE 20 – Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. (Üçüncü cümle mülga: 3/10/2001-4709/5 md.)</p> <p>(Değişik: 3/10/2001-4709/5 md.) Millî güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlâkın korunması veya başkalarının hak ve özgürlüklerinin korunması</p>

1 / 29

1982 Anayasası	Teklif Metni
<p>sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.</p>	<p>sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hâkim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kâğıtları ve eşyası aranamaz ve bunlara el konulamaz. Yetkili merciin kararı yirmidört saat içinde görevli hâkimin onayına sunulur. Hâkim, kararını el koymadan itibaren kırksekiz saat içinde açıklar; aksi halde, el koyma kendiliğinden kalkar.</p> <p><u>Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak, kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir.</u></p>
<p>V. Yerleşme ve seyahat hürriyeti</p> <p>MADDE 23 – Herkes, yerleşme ve seyahat hürriyetine sahiptir.</p> <p>Yerleşme hürriyeti, suç işlenmesini önlemek, sosyal ve ekonomik gelişmeyi sağlamak, sağlıklı ve düzenli kentleşmeyi gerçekleştirmek ve kamu mallarını korumak;</p> <p>Seyahat hürriyeti, suç soruşturma ve kovuşturması sebebiyle ve suç işlenmesini önlemek;</p> <p>Amaçlarıyla kanunla sınırlanabilir.</p> <p>Vatandaşın yurt dışına çıkma hürriyeti, <u>vatandaşlık ödevi ya da ceza</u> soruşturması veya kovuşturması sebebiyle sınırlanabilir.</p>	<p>V. Yerleşme ve seyahat hürriyeti</p> <p>MADDE 23 – Herkes, yerleşme ve seyahat hürriyetine sahiptir.</p> <p>Yerleşme hürriyeti, suç işlenmesini önlemek, sosyal ve ekonomik gelişmeyi sağlamak, sağlıklı ve düzenli kentleşmeyi gerçekleştirmek ve kamu mallarını korumak;</p> <p>Seyahat hürriyeti, suç soruşturma ve kovuşturması sebebiyle ve suç işlenmesini önlemek;</p> <p>Amaçlarıyla kanunla sınırlanabilir.</p> <p>Vatandaşın yurt dışına çıkma hürriyeti, <u>ancak suç</u> soruşturması veya kovuşturması sebebiyle <u>hâkim kararına bağlı olarak</u></p>

2 / 29

APPENDIX E: ELEKTRONİK BELGE STANDARTLARI

16 Temmuz 2008 ÇARŞAMBA

Resmî Gazete

Sayı : 26938

GENELGE

Başbakanlıktan:

Konu: Elektronik Belge Standartları.

GENELGE

2008/16

Kamu adına görev yapan kurum ve kuruluşların faaliyetleri sonucu oluşan belgelerin kayıt altına alınması ve bu belgelerin istenildiği anda erişilebilir şekilde yönetilmesi, kurumsal faaliyetlerin ayrılmaz bir parçası ve bir kamu görevidir. Herkesin, her zaman, her yerden kolaylıkla ulaşabileceği şeffaf, verimli ve sade bir kurum yapısı günümüzde modern ve demokratik kurumların temel hedefi haline gelmiştir. Elektronik ortamda sunulan hizmetlerin ve e-kurum yapısının temelini elektronik bilgi sistemleri oluşturmaktadır.

Kamu kurum ve kuruluşlarınca üretilen elektronik bilgi ve belgelerin idari, mali, hukuki ve tarihi gerekçelerle korunmasının sağlanması ve bunların gelecek nesillere aktarılması ancak standart belge yapılarının oluşturulması ile mümkündür. Elektronik belgeye ilişkin standartlar ile belgelerin korunmasına ve erişimine imkan sağlayacak tedbirlerin elektronik belge yönetim sistemlerinin tasarım aşamasında ele alınması gerekmektedir.

Elektronik belgelerin kayıt altına alınması, kullanılması ve arşivlenmesi konularında çalışma yapma görevi E-Dönüşüm İcra Kurulu'nun 9 Eylül 2004 tarih ve 7 numaralı Kararı ile Devlet Arşivleri Genel Müdürlüğü'ne verilerek TSE 13298 no'lu standardın yayınlanması sağlanmıştır. Hazırlanan bu standart kamu kurum ve kuruluşlarının kullanacakları elektronik belge yönetim sistemleri için temel bir kaynak teşkil etmektedir.

Kamu kurum ve kuruluşları oluşturacakları elektronik belge yönetim sistemlerinde TSE 13298 no'lu standarda göre işlem yapacak, ayrıca üretmiş oldukları elektronik belgenin kurumlar arası paylaşımını www.devletarsivleri.gov.tr internet adresinde belirlenen kurumlar arası elektronik belge paylaşım hizmeti kriterlerine göre gerçekleştirecektir. Genelgenin yayımı tarihinden önce kurulan sistemler ise ilgili kamu kurum ve kuruluşlarınca gözden geçirilerek iki yıl içinde standarda uyumlu hale getirilecektir.

Bilgilerini ve gereğini rica ederim.

APPENDIX F: APPROVAL LETTER OF PRACTICAL ETHICS RESEARCH BOARD



1956

Orta Doğu Teknik Üniversitesi
Middle East Technical University

Öğrenci İşleri Daire Başkanlığı
Registrar's Office

06531 Ankara, Türkiye
Phone: +90 (312) 2103417
Fax: +90 (312) 2107960
www.oidb.metu.edu.tr

B.30.2.ODT.72.00.00420-6358-520

11/10/2010

ENFORMATİK ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Üniversitemiz Sağlık Bilişimi Anabilim Dalı (MIN) yüksek lisans programı öğrencisi Özlem Özkan'ın 02 Eylül 2010-28 Şubat 2011 tarihleri arasında "*Mahremiyet ve Gizlilik Açısından Sağlık Bilgisinin Elektronik Ortamda Tutulması Hakkında Vatandaşın Görüşleri ve Düşünceleri*" başlıklı araştırmasına ilişkin olarak ODTÜ öğrencilerine ve çalışan yetişkinlere uygulama yapmak için, öğrencinin isteği doğrultusunda görevlendirilmesi Etik Komite onayı ile uygun görülmüştür.

Uygulamanın yapılabilmesi için gereğini arz ederim.

Saygılarımla.


Nesrin Ünsal
Öğrenci İşleri Daire Başkanı

Ekler:

- 1- İAEK Başvuru Formu
- 2-İAEK Başvuru Kontrol Listesi
- 3-İAEK Başvuru Formu Proje Bilgi Formu
- 4-Anket

BD