

Addis Ababa
University
(Since 1950)



ADDIS ABABA UNIVERSITY
SCHOOL OF GRADUATE STUDIES
SCHOOL OF INFORMATION SCIENCE
AND
SCHOOL OF PUBLIC HEALTH

PRIVACY AND CONFIDENTIALITY ISSUES OF AN EMR
APPLICATION: HEALTH PROFESSIONALS, HEALTH
MANAGERS AND PATIENTS' PERCEPTION IN ZEWDITU
AND RAS DESTA DAMTEW HOSPITALS

BY
MAMUSH TADESSE

JUNE, 2013

ADDIS ABABA UNIVERSITY
SCHOOL OF GRADUATE STUDIES
SCHOOL OF INFORMATION SCIENCE
AND
SCHOOL OF PUBLIC HEALTH

PRIVACY AND CONFIDENTIALITY ISSUES OF AN EMR
APPLICATION: HEALTH PROFESSIONALS, HEALTH
MANAGERS AND PATIENTS' PERCEPTION IN ZEWDITU
AND RAS DESTA DAMTEW HOSPITALS

BY
MAMUSH TADESSE

JUNE, 2013

ADDIS ABABA UNIVERSITY
SCHOOL OF GRADUATE STUDIES
SCHOOL OF INFORMATION SCIENCE
AND
SCHOOL OF PUBLIC HEALTH

PRIVACY AND CONFIDENTIALITY ISSUES OF AN EMR
APPLICATION: HEALTH PROFESSIONALS, HEALTH
MANAGERS AND PATIENTS' PERCEPTION IN ZEWDITU AND
RAS DESTA DAMTEW HOSPITALS

BY
MAMUSH TADESSE

Members of the examining board:

Name	Title	Signature	Date
_____	Chairperson	_____	_____
_____	Advisor	_____	_____
_____	Advisor	_____	_____
_____	Examiner	_____	_____
_____	Examiner	_____	_____

Declaration

I, the under signed, declare that this is my original work and has never been presented in this or any other Universities.

Name _____

Signature _____

Place _____

Date of submission _____

This thesis has been submitted for examination with our approval as University advisors.

Name of Advisors:

Signature and Date

1. DR GETNET MITIKE
2. ATO ERMIAS ABEBE

ACKNOWLEDGEMENT

I would like to pass my deepest thanks for Addis Ababa University school of Public Health and Information Science for covering the cost required for this thesis.

I am deeply indebted to my advisors Dr. Getnet Mitike and Ato Ermias Abebe for their close follow up and help given in each step of this work.

I wish to express my gratitude to all staffs of Zewditu and Ras Desta Damtew Hospitals.

My thanks extended to Aman college of Health Science for sponsoring me to pursue my postgraduate education.

Finally I would like to thank the study participants, my beloved family and for those who had helped me while data collection.

TABLE OF CONTENTS

Acknowledgements-----	I
List of Figures -----	II
List of Tables -----	III
List of Acronyms -----	IV
Abstract -----	V
CHAPTER ONE	1
INTRODUCTION	1
1.1 Background.....	1
1.1.1 Paper-Based Medical Records	2
1.1.2 Electronic Medical Record (EMR)	3
1.2 Statement of the Problem.....	4
1.3 Objectives of the Research.....	5
1.3.1 General Objective	5
1.3.2 Specific Objectives	5
1.4 Scope and Limitations of the Study	5
1.5 Organization of the thesis	5
CHAPTER TWO	7
LITERATURE REVIEW.....	7
2.1 Privacy and Confidentiality.....	7
2.2 Privacy legislations.....	8
2.3 Security Breaches and Harm to Patients.....	9
2.4 Implications for Ethical Practice	11
2.5 Challenges of Adopting EMR in Developing Countries	12
2.6 Potential Safety Benefits of EMR.....	14
2.7 Smartcare Ethiopia	16
2.8 Why does privacy matter?	17
2.9 Related Works	17
CHAPTER THREE	21
METHODOLOGY	21
3.1 Study Area and Period	21
3.2 Study Design	22
3.3 Study Population	22

3.4 Inclusion Criteria.....	22
3.5 Exclusion Criteria	22
3.6 Sampling Procedure.....	23
3.7 Sample Size Determination	23
3.8 Data Collection Procedures	24
3.9 Data Quality Management and Analysis.....	24
3.10 Ethical Consideration	24
3.11 Dissemination of Results.....	25
3.12 Operational Definitions.....	25
CHAPTER FOUR	26
RESULTS	26
4.1 Socio-demographic Characteristics	26
4.1.1 Socio-demographic Characteristics of Health Professionals and Health Mangers.....	26
4.1.2 Socio-demographic Characteristics of patients	26
4.2 Knowledge of Health Professionals about Electronic Medical Records.....	27
4.3 Knowledge and Attitudes of Patients towards EMR system.....	31
4.4 Health professional perception towards EMR	32
4.5 Practice of Electronic Medical Records.....	34
4.6 DISCUSSION.....	36
4.7 Strength and limitation of the study.....	37
CHAPTER FIVE.....	38
CONCLUSION AND RECOMMENDATION	38
5.1 CONCLUSIONS	38
5.2 RECOMMENDATIONS.....	39
REFERENCES.....	40
Annex 1 Consent Form.....	45
Annex 2 Questionnaires for EMR Users.....	46
Annex 3 Questionnaires for Patients.....	52
Annex 4 Amharic version questionnaire for patients.....	55

List of figures

Pages

Figure 1. Adequacy of EMR training among health professional to keep patient privacy in Zewditu and Ras Desta Damtew memorial hospitals, May 2013.----- 29

Figure 2. EMR training status of users in Zewditu and Ras Desta Damtew Memorial Hospitals, A.A, May 2013 ----- 33

Figure 3. EMR user’s perception about poor adoption and utilization rate in Zewditu and Ras Desta Damtew Memorial Hospitals, A.A, May 2013 ----- 35

List of Table

Pages

Table 1. Socio-demographic characterestics of EMR users in Zewditu and Ras Desta Damtew Memorial Hospitals -----	27
Table 2. Socio-demographic characterstics of patients in Zewditu and Ras Desta Damtew Memorial Hospitals-----	28
Table 3. Knowledge of health professionals about medical record systems in Zewditu and Ras Ddesta Damtew hospitals, May 2013, A.A -----	30

LIST OF ACRONYMS

A. A.	Addis Ababa
AARHB	Addis Ababa Regional Health Bureau
AAU	Addis Ababa University
CPOE	Computerized physician order entry
EHR	Electronic health record
EMR	Electronic medical record
FMOH	Federal ministry of health
GP	General Practitioner
HIV	Human immune deficiency virus
ICT	Information communication technology
PHI	Personal health information
PHR	personal health record
RDDH	Ras Desta Damtew Hospital
ZMH	Zewditu Memorial Hospital

ABSTRACT

Introduction

Establishing a nationwide Electronic Health Record system has become a primary objective for many countries around the world in order to improve the quality of healthcare while at the same time decreasing its cost. However, implementation of EHR systems is being hindered by several obstacles, among which are concerns about data privacy and trustworthiness. With the introduction of e-health, concerns of right to data privacy became a primary concern for the patients and health professionals.

Objective

The objective of this study is to explore the perception of health professionals, managers and patients' towards privacy and confidentiality issues of Electronic Medical Records in Zewditu and Ras Desta Damtew memorial hospitals.

Method

A hospital based cross-sectional, quantitative study was conducted among 420 health professionals and patients to assess health care professionals, health managers and patients attitude towards privacy issues of EMR. The sample size was calculated using single population proportion formula. The data was collected through standardized questionnaire. Respondents were assessed by socio-demographic, knowledge, attitude and practice variables.

Result

Among users of EMR, 229 (79.8 %) are trained to use the software by NGO, Government, and by themselves or self trained. About 66 (28.8%) replied the training prepared them fully to keep patient privacy, 120 (52.2%) mostly prepared, 41(17.9%) somewhat prepared and the rest 2 (0.7%) said not at all. Forty eight (21%) of the respondents have no individual Log in Id and passwords. They have no other option to enter their patients data other than sharing others passwords. Nineteen (16.5%) of patients even don't know that their health data will go into computerized method.

In this study, patients who are relatively literate (assessed by their educational status) showed concerns of privacy issues but illiterate patients didn't know risks and benefits of computerized medical record. Almost all patients want to be asked before their health data is taken for research or other purpose. Overall managers, health professionals and patients are comfortable by the existing system except privacy concerns.

Conclusion and Recommendation

In this study, all respondents believe that EMR system is likely to increase the quality of care. At the same time, respondents have significant concerns about the privacy of their medical records. There is no means to control (audit trail) over who can access patient data among employees. Most respondents are obliged to share passwords because they have no individual Log in Id and passwords. This shows the presence of some gaps not to ensure privacy of patient information. Even though respondents are comfortable by the EMR system, privacy concerns are still there. Therefore, government and other responsible bodies should implement and enforce strategies to strengthen privacy. Health care providers should inform to their patients how their health data is being stored in order to increase their awareness, avoid confusion and build public trust.

CHAPTER ONE

INTRODUCTION

1.1 Background

Improving access to health care services in developing countries through ICTs has been receiving particular attention. Electronic health records (EHRs) form an integral part of the healthcare system and it is imperative that EHRs are safe. EHRs have a variety of functionalities which include storage of health information and data, result management, order entry and management, decision support, electronic communication and connectivity, patient support, administrative processes and reporting [1].

Establishing a nationwide electronic health record system has become a primary objective for many countries around the world in order to improve the quality of healthcare while at the same time decreasing its cost. However, implementation of EHR systems is being hindered by several obstacles, among them concerns about data privacy and trustworthiness [2]. The proper management of personal health information is important to the healthcare system. Patients share personal information with their physician in the expectation it will be used to improve their health and comfort. The physician adds information regarding his or her diagnosis and treatment of the patient. Information is also generated by laboratories, pharmacies, hospitals, and other healthcare stakeholders [3].

Privacy is the right of individuals to keep information about themselves from being disclosed to others; the claim of individuals to be left alone, from surveillance or interference from other individuals, organizations or the government. The information that is shared as a result of a clinical relationship is considered confidential and must be protected. The information can take various forms including identification data, diagnoses, treatment, progress notes, and laboratory results and can be stored in multiple media e.g., paper, video, electronic files [4].

1.1.1 Paper-based medical records

Despite the documented benefits of the EMR, most clinical encounters are still recorded by hand in a paper record. This is not without reason. Dick and Steen (1991) note that the traditional paper record is still used due to its familiarity to users, portability, ease of recording “soft” or “subjective” findings, and its browsability for non-complex cases. There is also a sense of ownership of paper records, due to their being only one copy, which increases the sense of their security (although it will be noted below that this may be a false sense of security).

Nonetheless, there are many problems with paper based medical records. The first is that the record can only be used in one place at one time. This is a problem for patients with complex medical problems, who interact with numerous specialists, nurses, physical therapists, etc. Another problem is that paper records can be much disorganized. Not only can they be fragmented across different physician offices and hospitals, as noted above, but the record at each location itself can often be disorganized, with little overall summary. In most paper records, pages are added to the record as they are generated chronologically, making the viewing of summarized data over time quite difficult. Another problem with the paper record is incompleteness. In an analysis of U.S. Army outpatient clinics, Tufo and Speidel (1971) found as many as 20% of charts had missing information, such as laboratory data and radiology reports, a finding consistent with more recent observations (Korpman & Lincoln, 1988; Romm & Putnam, 1981).

A final problem with the paper-based record is security and confidentiality. Although usually ascribed as a problem of the EMR, there are attributes of the paper record that increase its vulnerability to access by non authorized outsiders. Its difficulty in duplication leads to a great deal of photocopying and faxing among providers and institutions. Furthermore, abstractions of the paper record are stored in large databases, such as those of the Medical Information Bureau, which are maintained by health insurance companies to prevent fraud but contain medical information of more than 12 million Americans (Rothfeder, 1992).

1.1.2 Electronic Medical Record (EMR)

The electronic medical record is a computerized patient tracking and patient caring system. In health informatics, an EMR is considered by some to be one of several types of electronic health records, but in general usage EMR and EHR are synonymous. The term has sometimes included other systems which keep track of medical information, such as the practice management system which supports the electronic medical record. EHR is an essential technology for health care and a necessary tool for improving patient safety and the quality of care. Availing quality and timely health information at various levels of decision points throughout the country's health system is very essential for the improvement of health care and overall health system in Ethiopia.

The benefits of using an EMR includes, increasing the quality and speed of access to health information and the effectiveness of the health system. At the same time computerized medical records are open to potential abuses and threats. Some have pointed out that large amounts of sensitive healthcare information held in data centers are vulnerable to loss, leakage, or theft. (Concept notes and status of ICT Programmes implementation 2009, 16)

In Ethiopia, the implementation of EMR is through software called *SmartCare*. *TUTAPE* (Tulane University's Technical Assistance Program for Ethiopia) is developing the SmartCare software in partnership with *Tulane* University, communicable disease control (*CDC*) and the Federal Ministry of Health Ethiopia (*FMOH*). SmartCare was first developed, tested and deployed in Zambia by CDC for HIV/AIDS care and treatment. Besides the rich and advanced functionality and features, SmartCare has also been proven to work in limited resources environment of developing countries particularly in Africa. SmartCare possesses numerous advantages and features in comparison to existing EMR applications. Ethiopia thus adapted SmartCare as the preferred EMR application. (Tewodros Mengesha, Electronic solutions for Ethiopian health sector)

1.2 Statement of the Problem

It's not time taking to think about the importance of privacy and confidentiality issues of patient medical records. With the introduction of e-health, concerns of right to data privacy became a primary concern for the patients. A patient's medical record accumulates significant personal information including identification, history of medical diagnosis, medication history, sexual preference, genetic information, psychological profiles, employment history, income and physicians' subjective assessments of personality and mental state. Enhanced availability of health information facilitates easy access for further use and reference but it brings a concomitant concern of greater risk for loss of privacy among health care participants. [4]

Even though, e-health is somewhat a new phenomenon in developing countries, there exists a wide range of projects strengthening the health care delivery systems in Ethiopia. Despite the high expectations and interest in EMRs, their overall adoption rate is relatively low and they face several problems. Those projects are deployed without considering patients involvement and there are no studies related to attitude towards privacy and confidentiality issues of EMR. As the country makes transition from paper based to electronic health records, it is critical to address such issues that will arise in due course. However, FMOH and other healthcare stakeholders do not always see the perspective of those who will be the most affected by a move to electronic records. Timely recognition of patients' concerns will help the Ministry of Health and implementers to look for remedies and design considerations during its scale up. (*mHealth: new horizons for health through mobile technologies*)

Therefore, this study is planned to assess perception of health care providers, patients and health managers about privacy and confidentiality issues of EMR application.

This research thus tries to answer the following research questions:

How do patients and EMR users perceive privacy and confidentiality issues?

What is health consumers' level of awareness about electronic medical records?

Are privacy protection policies sufficiently related with health IT?

1.3 Objectives of the Research

1.3.1 General Objective

- The general objective of this study is to assess privacy and confidentiality issues of EMR: health professional, and health managers' and patient' perception in ZMH and RDDH, Addis Ababa

1.3.2 Specific Objectives

- To assess the potential benefits and risks of electronic health records related to privacy and confidentiality from patients' perspective.
- To identify patient, health professional and health managers sources of concern regarding the potential negative impacts of EHR's

1.4 Significance of the study

EMR system is not fully implemented in all health institutions in Ethiopia and enough studies are not conducted to assess users and patient's perception. So this research may give an overview of the existing EMR system. The most beneficiaries of this study are FMOH, patients, hospitals and responsible stakeholders because assessment of health consumers' perception towards privacy and confidentiality issues is very important to identify area for improvement and encourage better health care utilization. In addition it may be an input for who need research on related issue. Besides these, the study can provide information for policy makers about the overall situation of EMR and to give attention for consumers' involvement in related issues.

1.5 Scope and Limitations of the Study

The scope of the study is limited to assessing privacy and confidentiality issues of EMR among health care providers, health managers and patients.

1.6 Organization of the thesis

This thesis is organized into five chapters. The first chapter briefly introduces the research; Background, Statement of the problem, and Objectives of the study are among others. The second chapter is devoted to literature review about paper-based medical record, electronic medical record (EMR), Smartcare Ethiopia, privacy and confidentiality, security breaches and harm to patients, implications for ethical practice, and challenges of adopting EMR in developing countries and potential safety benefits of EMR.

The third chapter explains methodology of the research. The fourth chapter is all about findings and presentations. In this chapter analysis has been made about the respondents involved in the study. The last chapter, chapter five is about conclusion and recommendation of the study.

CHAPTER TWO

LITERATURE REVIEW

2.1 Privacy and Confidentiality

In the context of personal information, concepts of privacy are closely intertwined with those of confidentiality and security. Privacy addresses the question of what personal information should be collected or stored at all for a given function. In contrast, confidentiality addresses the issue of how personal data that has been collected for one approved purpose may be held and used by the organization that collected it, what other secondary or further uses may be made of it, and when the permission of the individual is required for such uses. Unauthorized or inadvertent disclosures of data are breaches of confidentiality [5].

Electronic health record includes patients' sensitive health information and if the information is disclosed accidentally or unintentionally, there could be detrimental effects on the patient. Misuse of patient data may harm patients and undermine the quality of healthcare. The data protection of health records against intrusion, unauthorized use, data corruption, intentional or unintentional damage, theft, and fraud is a universal concern and a high priority issue in most countries. Given the sensitive nature of healthcare information and the high degree of dependence on trustworthy records, issues of reliability, security, and privacy are of particular significance. There is, however, ambivalence about privacy because of the potential benefits of community access to personal information. Unfortunately, since regulation and legislation often lag behind technology, privacy is generally addressed in reactive rather than proactive mode [6]. Therefore, electronic health record systems need to build the consumer and healthcare provider trust to have full usage of the system.

Electronic health record systems available through network are more vulnerable to attacks and misuse. Proper security measures such as encryption, public key infrastructure, firewall and network service management, software management, rights management tools and system vulnerabilities management tools would provide more security for electronic health record systems [7].

There are a lot of incidences of breach of confidentiality of electronic health record systems. A hacker infiltrated the University of Washington Medical Center's computer system and stole at least 5000 cardiology and rehabilitation medicine patients' records. In another incidence, a Dutch hacker had pointed out the vulnerabilities of the system, because he had penetrated an unidentified medical centre in New York and another in Holland [8].

The University of Michigan Medical Center patients' records were left exposed to the public on the Internet because they thought that they were on a special server protected with special password. It was an innocent mistake but the patient's confidentiality was breached. The case of the Florida state public health worker who sent the names of 4000 HIV positive patients to two Florida newspapers was a case of abuse of access privilege and access for the purpose of profit. Therefore, privacy and confidentiality of health data is important for the successful implementation of electronic health record system. [9]

Thus, quality, privacy, interoperability are important for the successful integration of electronic health record systems. Health information available through electronic health records and health information available through the Internet enhances communication between healthcare providers and healthcare consumers. Better information decisions can be made through the information availability and it enhances health information knowledge management. [10]

2.2 Privacy legislations

In developing countries, worryingly there is little consideration of privacy policy and technology. In fact, where poor privacy practices may make already vulnerable people even more vulnerable, privacy is often perceived as an impediment to their care. Where it matters most is where it is mostly ignored. Concerns with privacy in eHealth are not, however, the preserve of the high-income countries. In a recent study researchers argued that the processing of information ranging from simple communication between patients and medical staff to complex sharing of data between care institutions is integral to good health care. The results of the project made clear however that many developing nations are poorly equipped to maintain adequate levels of patient privacy. [*Electronic health privacy and security in developing countries and humanitarian operations, 2010*]

Health privacy legislation is found mainly in developed countries. Based on the belief that patient privacy is a core element of good health care practice and that legislation is a key tool in protecting privacy. Given that privacy of the doctor-patient relationship is at the heart of good health care. The protection of privacy will also be a significant issue in supporting the changing nature of health care in developing countries. It will significantly impact the potential of using valuable e-Health tools such as EHRs across organizations or countries. (*mHealth: new horizons for health through mobile technologies*).

Survey results show that a generally sound base of generic privacy protection exists: some 70% of the 113 responding countries reported having legislation providing a basic right to privacy, and the remaining 30% anticipate that such legislation would be adopted by 2015. When reviewing the existence of legislation specifically protecting the privacy of the e-health these values are reversed, however: only 30% globally reported having such legislation in place. Further analysis of the responses on the use of legislation to ensure privacy in sharing EHRs for treatment or research purposes reveals that very few countries have established comprehensive legal frameworks. [Higgins G. The history of confidentiality in medicine: the physician-patient relationship]

2.3 Security Breaches and Harm to Patients

Electronic medical records deal with medical information of patients, and this should be treated as private and confidential. Physicians believe that keeping such information safe is very important because otherwise it could create legal issues. However, there is a lack of clear security standards which can be followed by those who are involved in the use of EMRs.

Few studies in the literature examine patient perceptions of EMR use, although physicians are increasingly adopting EMRs, their use is still not widespread. Evidences indicate that patients believe that EMRs improve care coordination but privacy of personal health information continues to be cited as a concern of both patients and providers. Recent developments have significantly increased the potential harms that can result when EMR systems are breached. For one, there has been a trend in recent years to gather and record more detailed information in

medical records. [11] For another, the ranges of uses to which EMR systems are put have expanded. The aggregated nature of EMRs facilitates secondary use indirectly related to patient care, such as clinical research; quality measurement, reporting, and improvement; public health; marketing; and managed care decision-making. [12, 13]

The potential for harm from a security breach may depend on several factors, including the intent of the perpetrators of the breach, nature of the information that was breached, and to whom the information was disseminated. Still, the detailed and complex patterns of collecting and using patient information in today's health care environment mean that the risk of harm to patients from security breaches is higher than ever before. [14, 15]

Medical identity theft can result not only in inconvenience, discrimination, or negative effects on a victim's credit rating, but can pose harms specifically related to health care in the form of improper exhaustion of insurance benefits, wrongful billing for the costs of the thief's health care, and the burden of proving that the victim isn't responsible for such charges and can adversely affect insurability. Of particular concern are the potential adverse effects of such theft on a victim's subsequent health care, notably inappropriate care based on erroneous entries in his or her record. [16,] Beyond this sort of material harm that may follow from inappropriate disclosure of a patient's personal health information are the dignitary harms that result.

The commitment to benefit the patient is a basic value of a physician's professional ethic.[17,18] Effective healing cannot take place without a patient-physician relationship that rests on the physician's competence, skills, and good will.[19]

The healing encounter is one in which the physician claims the necessary expertise and dedication to help and (implicitly) invites the vulnerable patient's trust. The physician is accountable to his or her patients in this relationship of fidelity in trust. [20] The commitment to benefit patients also entails respecting a patient's freedom to act in accord with his or her values and sense of self. [21] Inappropriate disclosure of a patient's personal information violates his or her right to (informational) privacy, a fundamental expression of autonomy.

2.4 Implications for Ethical Practice

Helping to restore a sense of control over health records to the patient is of great moral import. Indeed, studies consistently show that patients prefer to be informed of breaches of their health records or other medical errors. [22] Voluntarily disclosing to a patient that his or her information has (or may have) been inappropriately disclosed when the patient may otherwise be unaware of the breach respects the patient's dignity and supports his or her right to take appropriate steps to avert or minimize potential harms.

Beyond fulfilling the physician's obligation to be candid with patients, disclosing the incident and taking time to discuss possible harms and potential means of averting them may enhance trust. Conversely, the lack of disclosure may erode trust, especially if it leads to harm.

The material cost of adequately responding to a breach of security can be significant in terms of actual costs associated with the loss of patients, recruitment of new patients, and damage to the reputation of the physician, practice or institution. However, evidence has shown that litigation rates and related costs decrease when errors are promptly disclosed to patients and families. [23-25] It is also important to keep in mind that security measures and breach notice requirements should be practical and affordable so as to not hinder the ability of physicians to operate their practices and care for their patients.

A physician's responsibility to notify patients of an inappropriate disclosure and to take steps to help mitigate potential adverse consequences is not without limit.[26] A physician's ability to act may be limited by several factors, including what relationship the physician has with the affected patient or what his or her administrative authority is.

A physician who is not in a position to have personal knowledge that a breach has occurred or take effective action to prevent breaches for example, who works in a large health care institution whose EMR system is managed by others has relatively limited responsibilities.

Whatever the nature of the physician's involvement, in dealing with inappropriate disclosure of patient information the physician should place the interests of affected patients above the interests of their practices or institutions. The commitment to affected patients should be tempered only by potential harms of equal magnitude to other patients. Such patient advocacy

may take courage, but courage is implicit within a physicians' dedication to the well-being of their patients and their commitment to being trustworthy. [20]

Disclosure of a breach should occur as soon as practicable and in accordance with statutory timelines after the breach is known and should be carried out in a way that minimizes patients' distress and respectfully restores their control over their own privacy.

2.5 Challenges of Adopting EMR in Developing Countries

Information technology and its application to healthcare is a major global issue that has triggered a marked amount of research. There are sharp differences between barriers to adaptation and implementation in developing countries to that of developed countries. Implications of information technology for healthcare reform command much speculation [27]. Though health information technology promises benefits to healthcare, many problems exist. Despite years of research in the area of information technology, the progression in adaptation remains low.

Culture is a critical determinant of the successful implementation of EMR systems in developing countries. One particular issue is that of language. Since most EMR systems are designed in English, it becomes difficult to facilitate interaction between divergent cultural subsystems, preventing transfer of knowledge from one culture to another [28] for instance, the sub Saharan Africa region is notable for its incredible language diversity.

A well trained local data manager is fundamental in maintaining data quality. Like developed countries, issues of security of the information and confidentiality are significant but for many developing countries support for these concepts varies. Since most of the present EMR implementations in developing countries are centered on HIV/AIDS treatments, the issue of social stigma is something that needs to be considered while implementing EMR systems. Combinations of technical and human protocols have been advocated for use with these systems in developing countries [29].EMR system implementations are being carried out in phases [30]. These systems are fragmented and isolated – thus forming islands of users disconnected from each other.

Furthermore, most of these use proprietary standards which make them highly specific; hence interoperability is at minimal level. One initiative in place to overcome this issue is open MRS (openMRS). Since there are very low or slow returns on EMR systems in developing countries, these systems do not yet show up on the thrust areas of entrepreneurs in developing countries. [31]

Despite its advantages, many healthcare organizations have been slow to adopt this new technology. Cost is one barrier, but another concern is the negative impact it may have on doctor–patient communication [32].

In this article, we examine how EMR use influences doctor–patient communication by focusing on the nonverbal dimension of interactions. Understanding how the EMR influences communication during the medical interview is important because we know that better doctor–patient communication leads to improved healthcare outcomes [33-35].

A number of problems have been identified with the EMR, including increased provider time, computer down time, lack of standards, and threats to confidentiality. Studies at the institutions described above [36] have shown that electronic order entry increases the amount of time physicians spend entering orders. In the study at BWH (bates, boyle, & teich, 1994), residents required 44 more minutes per day using computerized order entry.

Confidentiality is concerned with keeping secrets. A professional secret is knowledge that, if revealed, will harm not only the professional’s client, but will do serious harm to the profession and to the society that depends on that profession for important services. [37]

The maintenance of strict confidentiality creates an environment that facilitates the privileged and unrestricted sharing of sensitive information between a physician and a patient. Any breach of privacy will irreparably damage this unique doctor-patient relationship. In the absence of confidentiality, patients might not fully disclose important facts; even worse, patients might avoid medical care entirely. [38]

Ensuring privacy and security of health information, including information in electronic health records (EHR), is the key component to building the trust required to realize the potential benefits of electronic health information exchange.

If individuals and other participants in a network lack trust in electronic exchange of information due to perceived or actual risks to electronic health information or the accuracy and completeness of such information, it may affect their willingness to disclose necessary health information and could have life-threatening consequences.[39]

Whatever the type of electronic health record decided upon the health information contained in it must be organized primarily to support continuing, efficient, and quality healthcare. It must also continue to meet legal, confidentiality, and retention requirements of the patient, the attending health professional and the healthcare institution/country. Among possible barriers of implementing EMR, concerns raised by healthcare professionals, patients and the general community are privacy, confidentiality and the quality and accuracy of electronically generated information (World Health Organization, 2006)

2.6 Potential safety benefits of EMR

Studies showing improved patient safety from EMR use in hospital and ambulatory care largely focus on alerts, reminders, and other components of CPOE.[40] CPOE makes information available to physicians at the time they enter an order for example, warning about potential interactions with a patient's other drugs. Once the order has been entered, the system can track the steps involved in executing the order, providing an additional mechanism for identifying and eliminating errors. In the longer term, CPOE provides the information needed to redesign the order execution process so that errors become even harder to make. To provide these benefits, CPOE must be an integrated component of a more comprehensive health care information system that is designed and used well. [41] safety benefits of CPOE are addressed by using models to extrapolate existing evidence to the national level and estimated separately the potential to reduce adverse drug events in inpatient and outpatient settings.

Realizing the benefits of prevention and disease management requires that a substantial portion of providers and consumers participate. Since, on average, patients comply with medication

regimens about half the time, it is plausible to assume that about half of the chronically ill would participate in disease management programs and, therefore, the health care system would reap about half of the estimated short term benefits, assuming that EMR systems and community-based connectivity were operational. [42]

EMR systems can be instrumental throughout the disease management process. Predictive modeling algorithms can identify patients in need of services. EMR systems can track the frequency of preventive services and remind physicians to offer needed tests during patients' visits. Condition-specific encounter templates implemented in an EMR system can ensure consistent recording of disease specific clinical results, leading to better clinical decisions and outcomes. [43]

EMR systems are currently amongst the prime transformers of IT based technologies in healthcare [44]. Healthcare users and consumers of EMR in countries like Kenya, India, and Haiti have been reaping the benefits for quite some time now. These systems, if compared with traditional manual systems provide basic benefits which can also be seen as potential benefits of EMR systems in other developing countries [45]. Such systems have been shown to provide greater accuracy, efficiency and cost benefits.

Studies on the impact of EMR list such benefits as efficient clinical management, improved diagnosis, reminders, and simple warning tools that help clinicians and patients reduce possible errors like drug incompatibility and interactions resulting in significant improvements in quality of care [46]. Networked EMR systems can enable laboratory data to be entered from remote locations. [47]

Other benefits to EHRs include: improved quality and patient safety, reduced lengths of stay (in acute care settings), increased efficiency and timeliness of care, avoidance of adverse events such as medical errors, improved treatment protocols, improved continuity of care, instant availability of charts, rapid and informed response to patients' telephone questions, refill requests, communication and education modules for enhanced patient understanding and satisfaction, accuracy and completeness of notes, and effective disease management by gathering

extensive data quickly and efficiently on patient populations. [48] An EHR does not just benefit the patients; it will benefit the main users by assisting and improving the duties and routines of physicians and health care institutions. [49]

2.7 SmartCare Ethiopia

SmartCare software development in Ethiopia happened in collaboration with the SmartCare team in Zambia and the United States. The SmartCare software application was adapted according to the recent Ethiopian HMIS reform conducted by the FMOH.

All customizations of the software are conducted by TUTAPE's Ethiopian software developers in collaborations with FMOH, Zambia's SmartCare team and consultants from the US.

SmartCare gained recognition as the Electronic Health System Application for Ethiopia followed by a presentation and live demo of the customized SmartCare EMR. The presentation was to the FMOH officials including Ministers, State Minister, Department/Agency Heads, Regional Health Bureau Heads, and other relevant stake holders.

SmartCare is designed to automatically and securely exchange data between different services in a facility. It allows communication among different clinical services, lab, pharmacy, and other networked units and offices. Whether installed in a small clinic or a hospital, it offers different options for data access and synchronizes data, eliminates redundancy of data entry. This integration includes patient demographics, provider notes, investigations, prescriptions and scheduling.

SmartCare has the feature to assist the user to use filtering criteria when searching a particular patient from the existing database. If the patient doesn't exist, the new name entered will be taken as a new client and SmartCare, will give you the option to register it or not. If there are similar names entered in to the database, which is most probably the case in most databases, a SmartCare window will pop with the list of similar names in the database; hence, the user can select the appropriate profile to continue.

2.8 Why does privacy matter?

Trust is clinically important and a key business asset. How your practice handles patient information is an important aspect of this trust. To help cultivate patients' trust, health care providers should carefully handle patients' health information to protect their privacy and keep the information in patients' individual records as accurate as possible. In medical practice, patients are unlikely to share sensitive information unless they trust that their health care provider will honor their confidentiality. Patients who trust their health information will be kept private and secure will be more willing to discuss their symptoms, conditions, and past and present risk behaviors. **(Building Trust in Health Information Exchange. (2011))**

Ensuring privacy and security of health information, including information in electronic health records (EHR), is the key component to building the trust required to realize the potential benefits of electronic health information exchange. If individuals and other participants in a network lack trust in electronic exchange of information due to perceived or actual risks to electronic health information or the accuracy and completeness of such information, it may affect their willingness to disclose necessary health information and could have life-threatening consequences. **(Building Trust in Health Information Exchange. (2011))**

2.9 Related Works

In Canada, surveys show that 11-13% of Canadians have held back information from a health care provider because they were afraid of who would see it and for what it would be used [50,51].

A survey of American citizens found that 15% of individuals were taking action to keep their personal medical information private by not seeking treatment, doctor-hopping, paying out of pocket, giving inaccurate or incomplete information, or asking their doctor to keep information out of their record. A 2005 survey of Americans found that 65% were very or somewhat concerned that people will not disclose sensitive but necessary information to doctors and other health care providers because of worries that it will go into computerized records. [52]

Approximately, 70% health care consumers in Australia were concerned about data leaks, medical information being shared without their knowledge, poor security, and increased medical errors [53]. Chanabhai et al. have shown in their EHR usability survey that 73.3% of participants were highly concerned about the security and privacy of their health records. the study indicated that consumers are ready to accept the transition to EHR systems, but only as long as they can be assured of their privacy [54].

In 1996 a research survey into GP and midwives attitudes to a shared electronic medical record system revealed a third of all respondents believed that some personal health care information should not be stored within an EMR. So if health care professionals are concerned about the use of shared EMR systems, then surely everyone should be asking the patient – after all, it is their personal health data that all these projects depend on. There appears to be minimal involvement of the patient in the planning and development of these projects. [55]

The privacy of personal information and of health information in particular, continues to be a burning issue. In one recent survey, 67% of respondents said they were concerned about the privacy of their medical records, with ethnic and racial minorities showing the greatest concern. When presented the possibility that there would be a nationwide system of electronic medical records, 70% of respondents were concerned that sensitive personal medical record information might be leaked because of weak data security, 69% expressed concern that there could be more sharing of medical information without the patient's knowledge and 69% were concerned that strong enough data security will not be installed in the new computer system [56].

Privacy or confidentiality is particularly important to adolescents who seek health care. When adolescents perceive that health services are not confidential, they report that they are less likely to seek care, particularly for reproductive health matters or substance abuse. These studies show that protecting the privacy of health information is essential to ensuring that individuals will obtain quality care [57].

Patients were less comfortable with sharing information about “sensitive” conditions such as mental health with researchers. Some were fearful that researchers would sell information to drug companies or other third parties. Although supportive of research, the majority of patients in these studies did not endorse the disclosure of their medical records for research without any

input from patients. Most patients expressed a desire to be consulted before their information was released for research [58]. A critical issue in the transition to EHRs is the privacy, confidentiality, and security of the information stored. This issue has made some patients and healthcare providers reluctant to accept electronic records [59].

In another study, Angst et al. (2006) investigated the divergence of perception among patients towards different types of personal health record systems (in an increasing order of technological advancement), including paper based, personal-computer-based, memory devices, portal and networked PHR. The study found that patients' relative perception of privacy and security concern increased with the level of technology, e.g., relative security and privacy concern for networked PHR is twice that of memory-device-based PHR. However, technologically advanced PHR systems were found to be favored by highly educated patients [60].

A significant body of research has examined the perception of privacy concerns from the viewpoint of a special class of patients, including mental health patients, seekers of HIV testing and adolescents. In a recent survey on healthcare confidentiality, it identified three overarching conclusions. First, patients strongly believe that their information should be shared only with people involved in their care. Second, patients do identify with the need of information sharing among physicians, though HIV patients are less likely to approve sharing of their health information. Third, many patients who agree to information sharing among physicians reject the notion of releasing information to third parties, including employers and family members.

Many researchers agree that the use of computerized EMRs is an issue that may have a negative effect on patient privacy [61]. Physicians doubt whether EMRs are a secure store for patients' information and records, and fear that data in the system may be accessible to those who are not authorized to obtain it. The consequent inappropriate disclosure of patient information might lead to legal problems. Furthermore, there is, in some countries, a lack of clear security regulations that could help ensure patient privacy and confidentiality. According to Simon *et al.* [62], physicians are more concerned about this issue than the patients themselves. Even among the physicians who do use EMRs, most believe that there are more security and confidentiality

risks involved with EMRs than with paper records [63]. This shows that concerns about the privacy and security of patient data are experienced as a barrier to EMR usage.

The majority of patients who have undergone genetic testing believe that patients should bear the responsibility of revealing test results to other at-risk family members [61]. If these concerns are not resolved before the widespread introduction of electronic health records, people will not trust EHR enough to reveal sensitive information, or to allow their doctor to record this sensitive information. This will be detrimental to the quality of care the patient receives and to the ability of other stakeholders to do their jobs [52].

A 2009 study on hospital doctors' understanding of ethics, including respect for patient privacy, revealed that there was a lack of proper and detailed knowledge of such duties among doctors. Shailaja Tetali commenting in the same journal states: as medical professionals, we generally do not give much thought to patients' feelings, especially with regard to their personal privacy. What could be the reasons for this apparent lack of sensitivity? Medical students in India are not formally taught about doctor-patient interactions. Ignorance among both doctors and patients about patient rights, and the asymmetry of information between them has ensured that patients do not have a voice of their own. [65]

CHAPTER THREE

METHODOLOGY

3.1 Study Area and Period

The study was conducted in Addis Ababa, which is the capital city of Ethiopia. Ethiopia is the second most populous nation in Africa, with over 82 million inhabitants. The population of Addis Ababa on January 1st 2011 is approximately 3,633,154. According to the head of the World Bank's Global HIV/AIDS Program, Ethiopia has only 1 doctor per 100,000 people. However, the World Health Organization's 2006 World Health Report gives a figure of 1936 physicians, which comes to about 2.6 per 100,000 population. Globalization is said to affect the country, with many educated professionals leaving Ethiopia for a better economic opportunity in the West. (World Bank's Global HIV/AIDS Program 2011)

There are 119 and 412 government owned hospitals and health centers in Ethiopia, respectively. Ethiopia has a relatively low average life expectancy of 45 years. Infant mortality rates are relatively very high, as over 8% of infants die during or shortly after birth, while birth related complications such as obstetric fistula affect many of the nation's women. HIV is also prevalent in the country. The government of Ethiopia and many organizations like World Health Organization (WHO), and the United Nations, are launching campaigns and are working aggressively to improve Ethiopia's health conditions and promote health awareness on AIDS and other communicable disease.

Inadequate health professional and resources, lack of technological advancements, traditional beliefs are the main reasons for health complications. Improper infrastructure for health records produces its contribution for low quality of health care. For example, e-health technologies which enable to connect all health care providers would help Ethiopia get the following advantages : it decreases repetition of information, information can be accessed by health care professional remotely, all health care providers will have the same up to date information, improves consistency of care, improves communication amongst health care providers.

Nowadays, in Ethiopia, electronic medical record (EMR) has been pilot tested in a hospital setting and is now ready for scaling up at the national level. In line with this, it is a must to study

health consumer's perception towards these technologies, especially related to privacy and confidentiality issues. Therefore, this study was conducted in Zewditu and Ras Desta Damtew Memorial Hospitals from Jan to June 2013. These are sites where EMR was fully implemented at the initial phase of this study

3.2 Study Design

A cross-sectional study was conducted using quantitative method. Data collection was conducted using structured and pre-tested self-administered questionnaire for health professionals and health managers and interview for patients.

3.3 Study Population

A research population is a well defined collection of individuals or objects known to have similar characteristics. This study comprises a population of all healthcare providers, health managers, patients.

3.4 Inclusion Criteria

- All health professionals, medical directors, health managers and patients
- Well communicable/conscious patients for interview

3.5 Exclusion Criteria

- Age below 18 years, patients who are critically ill and those who were not volunteer to participate in the study are not included

3.6 Sampling Procedure

Sampling is concerned with the selection of a subset of individuals from a population to estimate characteristics of the whole population. The total sample was allocated to both health facilities based on the number of health professionals and patient flow. The sampling procedure of this study encompasses from health professionals, patient and health managers who are working in Zewditu and Ras Desta Memorial Hospital. Equal proportions of respondents were allocated to both Zewditu and Ras Desta Damtew hospitals based on the information obtained from each hospital. Samples were selected bearing in mind that they represent well the entire population.

All health care professionals and health managers who are working in both hospitals are included under the study. 115 patients are also interviewed. The study considered 10% non response rate.

3.7 Sample Size Determination

This study has managed to select health professionals, health managers and patients, as respondents for the questionnaire distributed. Single population proportion formula was used to estimate sample size and it was calculated with the assumption of significance level of 95%, 5% margin of error, and 50% population proportion perceive risks of privacy and confidentiality issues.

$$n = \frac{Z_{\alpha/2}^2 p Q}{d^2} = \frac{(1.96)^2 (.5 \times .5)}{(0.05)^2} = 384 + \text{Non- respondents} = 10\%, = 422$$

Where: -

n = Sample size required

$Z_{\alpha/2}$: Standard normal distribution corresponding to 95% confidence interval (1.96)

d= desired level of precision/Marginal error 5% (0.05).

P=Proportion with concerns of risks in the target population. Q = 1-P

Non- respondents = 10%,

According to the formula and 10% non response rate a total of 422 cases were recruited. This sample size ensures that the responses are sufficiently reliable to get the necessary and genuine data from the health professional, health managers and patients.

3.8 Data collection procedures

Structured self administered and interview questionnaires were developed to be filled by health professionals, managers and patients respectively. Both questionnaires were pre-tested in Yekatit 12 hospital prior to the survey. Respondents were selected randomly.

3.9 Data quality management and analysis

The collected data was checked first for completeness and internal consistency. Then the data was entered and analysis was done with SPSS version 16.0 statistical packages. Proportions, percentages, frequency and tables, were used to summarize the data accordingly. Findings of the three groups of respondents were presented separately and compared.

3.10 Ethical consideration

Initially, a letter of Ethical clearance was obtained from AAU School of Public Health and School of Information Science and Addis Ababa Regional Health Bureau. A formal letter of cooperation was obtained from Addis Ababa Regional Health Bureau. Before starting the actual data collection the purpose of the study, the right to participate and refuse was told to the study subjects. Verbal consent from the study subjects was sought. Confidentiality of the information was also guaranteed.

3.11 Dissemination of Results

The findings of this research will be presented to Addis Ababa University School of Public Health and Information Science as part of the fulfillment for the degree of Masters of Science in Health Informatics. In addition, it will be distributed to Addis Ababa Regional Health Bureau and Federal Ministry of Health.

3.12 Operational Definitions

- **Health Consumer:** Anyone who needs health care services in addition to Patients
- **User:** Health professionals or Data clerks who are using the EMR
- **Perception :** an attitude or understanding of health professionals, managers and patients towards privacy **and confidentiality of electronic medical records**
- **Patients:** All individuals who seek health care at the time of data collection

- **Health Managers:** Medical directors and case team leaders
- **Privacy:** is the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others
- **EMR:** Computerized legal medical records tend to be a part of health information system, allowing for the storage, retrieval and manipulation of records.

CHAPTER FOUR

RESULTS

4.1 Socio-demographic characteristics

Of 422 respondents selected for the study, 402 respondents returned the questionnaire, yielding a response rate of 95.3 %. Among 402 respondents, 287 were health professionals and health managers and 115 were patients.

4.1.1 Socio-demographic characteristics of health professionals and health managers

Out of the total respondents, 157 (54.7%) and 130(45.3%) were male and female respectively. Among age ranges of the respondents 95(33%) and 89(31%) were aged between 31-35 and 26-30 respectively. Concerning their religion, 177(61.7%) were orthodox Christians, 56(19.5%) Muslims, 41(14.3%) protestant and the rest 13(4.5%) were Catholics and others. Occupational category of the respondents were 111 (38.7%) Nurses, 53 (18.5%) physicians, 25 (8.7%) Data Clerk, Pharmacy 23 (8%), 14 (4.8%) Laboratory technician and 57(19.8%) were others. (Table 1)

4.1.2 Socio-demographic Characteristics of patients

Out of 115 respondents, 63(54.8%) were male and 52(45.2%) female. Age categories of participants were 24(20.8%) 18-28, 32(27.8%) 29-38, 43(37.4%) 39-48, 11(9.6%) 49-58 and 5(4.4%) were above 59 years old. Most respondents i.e. 78(67.8%) were Orthodox, 20(17.5%) Muslim, 9(7.8%) Protestant and 8(6.9%) were Catholic and other followers. When we are assessing their educational status, 17(14.8%) were illiterate, 41(35.7%) read and write, 23(20%) attended between 6-12 grades and 34(29.5%) were above 12th grade. (Table 2)

Table 1 Socio-demographic characteristics of health professionals and managers in Zewditu and Ras Desta Damtew Hospitals, A.A, May, 2013.

Variable	Number (287)	Percent
Sex		
Male	157	54.7
Female	130	45.3
Age		
21-25	39	13.6
26-30	89	31
31-35	95	33
36-40	45	15.7
41-45	7	2.4
46-50	7	2.4
51-55	3	1
56-60	2	0.7
Religion		
Orthodox	177	61.7
Muslim	56	19.5
Protestant	41	14.3
Catholic	8	2.8
Others	5	1.7
Occupational Category		
Nurse	111	38.7
Physician	53	18.5
Pharmacist	23	8
Data clerk	25	8.7
Laboratory technician	14	4.8
Others	57	19.8

Table 2 Socio-demographic Characteristics of Patients in Zewditu and Rasdesta Damtew Hospitals, May 2013, A.A

Variable	Number (115)	%
Sex		
Male	63	54.8
Female	52	45.2
Age		
18-28	24	20.8
29-38	32	27.8
39-48	43	37.4
49-58	11	9.6
>59	5	4.4
Religion		
Orthodox	78	67.8
Muslim	20	17.5
Protestant	9	7.8
Catholics & others	8	6.9
Educational status		
Illiterate	17	14.8
Read and write	41	35.7
6-12	23	20
>12	34	29.5

4.2 Knowledge of Health Professionals about electronic medical records

Almost all 281(97.9%) professionals used paper based medical records to keep their patients data previously. When they are asked about electronic medical record systems, 273 (95.2%) know the presence of computerized ways of keeping patient information but 14(4.8%) of respondents said they don't. Beyond their knowledge 229 (79.8 %) are trained to use the electronic medical record by an NGO, the Government, or are self trained. The rest 58 (20.2%) were never trained. Amongst 229 trained respondents 34(14.8%) of them have been using the EMR for more than 24 months.

Trained respondents were also asked about how adequately the training prepared them to keep their patients privacy. About 66 (28.8%) replied the training prepared them fully, 120 (52.2%) mostly prepared, 41(17.9%) somewhat prepared and the rest 2 (0.7%) said not at all. (Figure 1) From this point it is not difficult to see the presence of some gaps not to ensure privacy of patient information. There is no means to control over who can access patient data among employees because 48 (21%) of the respondents have no individual Log in Id and passwords. They have no other option to enter their patients data other than sharing others passwords. This condition may pose breaches of confidentiality and facilitates patient information to theft. So appropriate privacy protections must be incorporated in the design stages of EMR because it is difficult or impossible to establish effective privacy protections in implementation stages and restoring public trust is much more difficult than building it at the start. (Table 3)

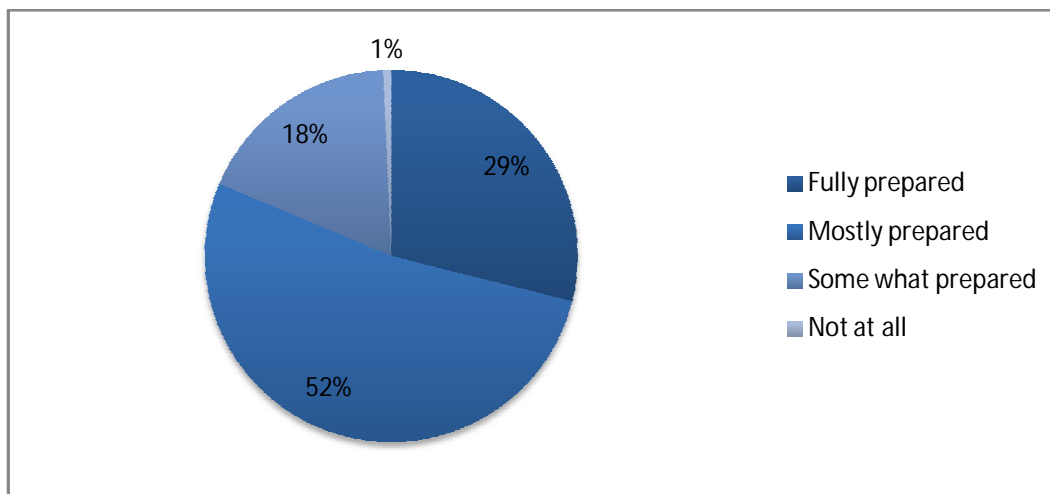


Figure 1. Adequacy of EMR training among health professional to keep patient privacy in Zewditu and Ras Desta Damtew memorial hospitals, May 2013.

Table 3. Knowledge of health professionals about medical record systems in Zewditu and Ras Ddesta Damtew hospitals, May 2013, A.A

Variables	Number (287)	Percent
Have you used paper based medical records before?		
Yes	281	97.9
No	6	2.1
Do you know about electronic medical records?		
Yes	273	95.2
No	14	4.8
Who trained you to use the EMR system?		
NGO	85	29.6
Gov't	85	29.6
Self trained	59	20.6
Was never trained	58	20.2
How long have you been using the EMR?		
Less than 6 months	71	24.7
6-12 months	84	29.3
13-18	30	10.5
19-24 months	22	7.7
Above 24 months	34	11.8
Never	46	16
How adequately did the training prepare you to keep patient privacy?		
Fully	66	28.8
Mostly	120	52.2
Somewhat	41	17.9

Not at all	2	0.7
------------	---	-----

4.3 Knowledge and attitudes of patients towards EMR System

Patients from all health care departments were included under the study i.e. waiting rooms, outpatient department, laboratory rooms, wards, pharmacy, antenatal care and family planning rooms. Among participants 96(83.5%) of them know the presence of computerized ways of keeping medical records. Whereas 19(16.5%) of patients even don't know that their health data will go into computerized method.

In this study, patients who are relatively literate showed concerns of privacy issues but illiterate patients didn't know risks and benefits of computerized medical record. For the question they are asked, which method they prefer to keep their health record 103 (89.5%) of them said EMR whereas 7(6%) paper based and 5(4.5%) said whichever it doesn't matter. Most patients gave more attention to physical data lost due to negligence, fire, flood rather than privacy and confidentiality. This study tried to assesses the level of awareness of patients to EMR, 65(56.5%) of respondents have significant concerns about the privacy of their medical records.

88(76.5%) of patients have complained data loss is common in record rooms and the rest 27(23.5%) mentioned is vulnerable to loss in laboratory, OPD, Wards and in other areas. About 104(90.5%) of interviewed patients said that they believe electronic medical record system will keep their sensitive medical information. Patients were also asked about their concerns in a move to computerized method 19 (16.5%) data leaks, 12 (10.4%) poor security, 84 (73%) have no concerns and none of them mentioned medical errors will happen because of EMR.

All respondents said patients who are in poor health status and those with HIV/AIDS, Youths using drugs, patient with mental problems are categorized as need more privacy and confidentiality. 21(18%) of respondents faced problems of data loss in record room previously and they believed these problems may be solved by this EMR method. 108(94%) of them said the most beneficiaries are patients, 6(5.2%) government and less than 1% of them said development partners

All respondents agreed that health consumer involvement is crucial before adopting any technologies. This study shows some patients are unaware of how their health data is kept and

analyzed. No patient is told by his provider about his diagnosis and treatment results will be stored electronically. Majority of respondents said not all medical records should be stored electronically. All participants said they wish they could be informed before their medical information is taken for research or other purpose. Lastly, they were also asked their overall satisfaction 19 (16.5%) are mostly satisfied 89 (77.4%) somewhat satisfied, 7 (6.1%) never satisfied by the existing EMR system. This means about 94% of interviewed patients are satisfied by the existing electronic medical record systems.

4.4 Health Professional Perception towards EMR

Protecting privacy is important not just to avoid harm, but because good health care depends on accurate and reliable information. There is widespread confusion among respondents about the scope of current health privacy laws. 98.2 % of respondents said there should be strong protections for privacy and security in the healthcare system otherwise patients will withhold information from health providers due to worries about how the medical data might be disclosed. Almost all respondents said, now in the early stages Federal Ministry of Health and all concerned stakeholders need to begin immediately to implement and enforce a comprehensive privacy and security framework.

Concerning physical security of patient data or loss of data by fire, flood, collapse or other disasters, two third or 188 (65.5%) of respondents said they are comfortable with the system because data can be retrieved by backup methods which is totally impossible in paper based systems. But still concerns of data loss because of viruses or worms were raised. 51(17.8%) of participants said both Paper and Electronic methods are about the same. 48(16.7%) still prefer paper based systems.

Among areas which are mentioned patients privacy is at greater risk are registration rooms 87 (30.3%), outpatient department (OPD) 83(28.9%), laboratory rooms 33(11.5%), 38(13.2%) in other areas including wards, imaging, ART and family planning clinics. Related to this point 120 (41.8%) of participants don't trust the software not to reveal sensitive health data because they have concerns that sensitive information will be shared because of poor security and data leaks.

Regarding sources of concern 107 (37.3%) sensitive information may be shared for clinical purpose even though it is for better treatment, 57(19.9%) poor security, 54(18.8%) mentioned Data leaks and 41(14.3%) of respondents said it doesn't concern me.

It is clear that all patients need privacy especially those who are in poor health condition have higher levels of concern about the privacy of their personal medical records to protect themselves from stigma or discrimination, 249(87%) respondents said there are no adequate privacy protection policies in Ethiopia regarding EMR. People living with HIV/AIDS, adolescents using drugs, people with mental problems and Family planning clients are groups who, are listed by participants, need more privacy and confidentiality.

Study participants were further asked for which systems do they prefer to keep their patients data. Most of them noted that computer-based records, with appropriate security, are potentially more secure than paper based records. 227 (79.1%) of participants still prefer Electronic medical records, 41 (14.3%) paper based and 19(6.6%) said any doesn't matter.

This figure indicates that greater than 20% of participants are not comfortable with EMR and still prefer the traditional way. This shows privacy and security concerns are major obstacles that can hinder the progress to electronic health. If they are not properly addressed, health care seekers will not feel comfortable in participating and health care professionals will face huge liability risks.

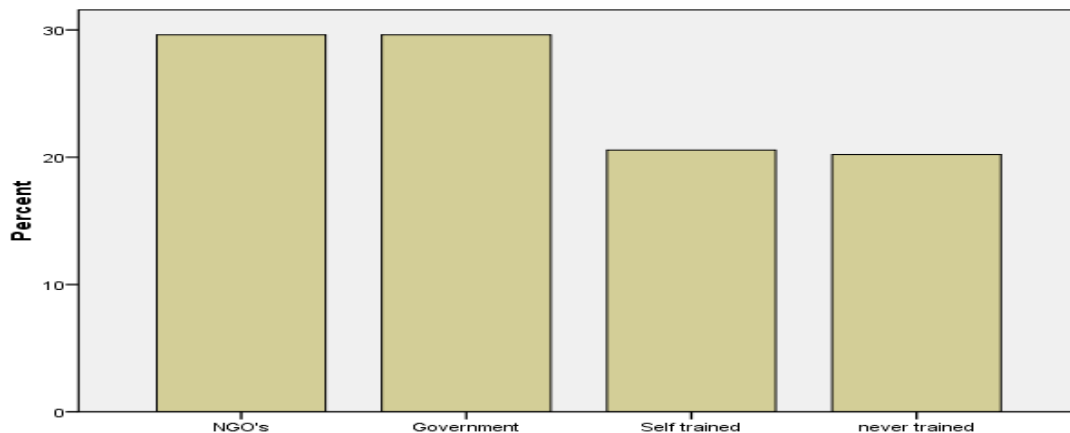


Figure 2 EMR training Status of Users in Zewditu and Ras Desta Dantew, A. A, May 2013

4.5 Practice of electronic medical records

From the analysis it was found that, 249(86.8%) of respondents said electronic medical records speed up access to a patient's health information. While 38(13.2%) replied the opposite. 105(36.6%) of them said pledge of confidentiality is now challenged by computers rule and health information falls into many hands.

Participants were also asked whether they have faced problems associated with the system, 11(3.8%) of them identified passwords being shared with those who have no private log in id, loss of patient data by virus or worm attack, breaking of passwords, taking personal information by other to make reports. The computerization of personal health information in the absence of strong privacy and security magnifies the risk to privacy. The unauthorized sharing of sensitive health information may result in a wide range of undesirable outcomes. This increases the danger of compromising the security and privacy of individuals.

Almost all patients are not well aware of both the benefits and the risks of computerized ways of keeping medical records. The analysis of the responses shows only 155(54%) of health professionals tell their patients about sensitive information will go in to computerized records. While 132(46%) of them didn't tell the issue because of fear that if they are aware they may hinder important information. 26(9%) of health professionals used patient data for research and other purposes without gaining consent from their patient. For the question they are asked about who is beneficiary in a transition from paper based record to electronic medical record 51(17.8%) said patient, 25(8.7%) development partner, 17(5.9%) Federal Ministry of Health and the remaining 177(61.7%) said multiple answers of the above alternatives.

Nearly all participants 273(95.1%) said health consumer involvement is important before adopting new technologies and 13(4.5%) said it has no value. Respondents were also asked about poor adoption and utilization rate of electronic medical record system. The reasons given are 145(50.5%) lack of training, 66 (23%) consumes time, 44(15.3) changes the usual work flow, 29(10.1%) poor patient involvement and 3(1%) said it is of no value.

In addition 161(56.1%) of respondents said some sensitive personal information should not be stored within an EMR while 126(43.9) said no matter if stored within an EMR. Even 43(15%) of them didn't believe information that is shared as a result of clinical relationship is confidential and protected.

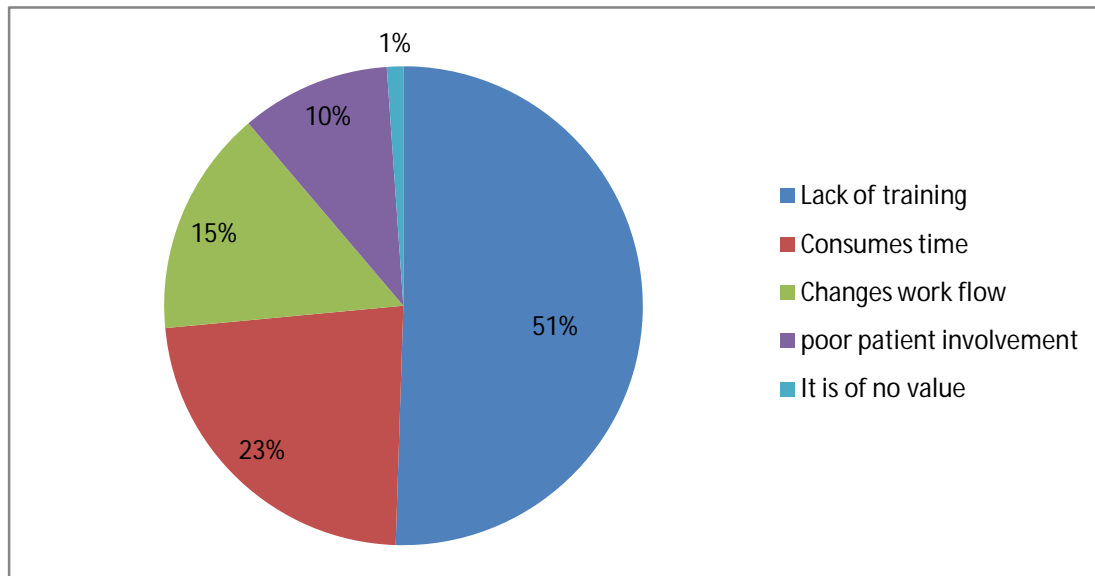


Figure 3. EMR users perception about poor adoption and utilization rate in Zewditu and Ras Desta Damtew Hospitals, A.A, May 2013.

The respondents were also asked to which organization privacy law should allow to use patient data without a patient's knowledge or consent. Their response were 50(17.4%) researchers, 47(16.4%) law enforcement 12(4.2%) pharmaceutical companies, 117(62%) to none of the above organizations unless the patient is informed and consent is gained. Overall satisfaction with the EMR system was also analyzed. 151(52.6%) of them are mostly satisfied, 110(38.3%) somewhat satisfied, and 26(9.1%) not at all satisfied. From this point almost 91% of respondents are satisfied by the existing electronic medical record system and they mentioned the technology improved health care quality and efficiency, but a lot has to be done by the federal levels and policy makers to empower consumers to play a greater role in their own care. All respondents agreed on while the software can help improve overall quality of health care delivery, the benefits of the technology must be balanced with the privacy and security concerns of the user.

4.6 DISCUSSION

Because IT in health care is an emerging field, adequate studies are not done locally to compare with this study. Therefore this study may give important information regarding health consumer's perception towards privacy and confidentiality issues of electronic medical records. In this work, I tried to assess the level of awareness of patients to EMR, 65(56.5%) of respondents have significant concerns about the privacy of their medical records. This figure is nearly consistent with study done in Australia, in which 73.3% of participants were highly concerned about the security and privacy of their health records. [54]. On the other hand, a national survey of conducted in 2005, 65% of respondents were "somewhat" or "very concerned" about the privacy of their personal medical records. [52]

In this study, among patient participants 96(83.5%) of them know the presence of computerized ways of keeping medical records. Whereas 19(16.5%) of them even don't know that their health data will go into computerized method. Similarly, survey data shows that Americans are well aware of both the benefits and the risks of health IT. A large majority of the public wants electronic access to their personal health information – both for them and their health care providers – because they believe such access is likely to increase their quality of care. [64]

All patients and EMR users mentioned their concerns in a move to computerized method. 27% of patients said data leaks and poor security. On one hand, 41.8% of health professionals and data clerks don't trust the EMR because they have concerns that information will be shared because of poor security and data leaks. On the other hand all EMR users and interviewed patients agreed that computerized ways of record keeping might speed up access to private data. But this concern is much higher in Australia, 70% health care consumers were concerned about data leaks, medical information being shared without their knowledge, poor security, and increased medical errors [53].

In this study, 98.2 % of EMR users said there should be strong protections for privacy and security in the healthcare system otherwise patients will withhold information from health providers due to worries about how the medical data might be disclosed. This point agrees with a survey of American citizens that 15% of individuals were taking action to keep their personal

medical information private by not seeking treatment, doctor-hopping, paying out of pocket, giving inaccurate or incomplete information, or asking their doctor to keep information out of their record. [52]

In this study 56.1% of EMR user respondents said some sensitive personal information should not be stored within an EMR. Similarly a research done in Massey university into GP and Midwives attitudes to a shared electronic medical record system revealed a third of all respondents believed that some personal health care information should not be stored within an EMR [55].

4.7 Strength and Limitation of the Study

Strength

- A high response rate of 95.3 %
- This is the first work which focuses on perception and level of awareness of EMR users and patients

Limitation

- All respondents might not give genuine answers to the questions they were asked. This might underestimate the degree of privacy concerns
- This study was done only in Zewditu and Ras Desta Damtew Memorial Hospital and in a short period of time.
- Presence of very limited studies for comparison purpose could be considered as a constraint factor for the study

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

5.1 CONCLUSIONS

In this study, all interviewed patients and EMR users agree that EMR system is likely to increase the quality of care. At the same time, they have significant concerns about the privacy of their medical records.

The study also showed that there is no means to control over who can access patient data among employees. Most respondents are obliged to share passwords because they have no individual Log in Id and passwords.

Patients who are relatively literate have higher concerns of privacy issues but illiterate patients didn't know risks and benefits of computerized medical record. All respondents said patients who are in poor health status and those with HIV/AIDS, youths using drugs, patient with mental problems are categorized as need more privacy and confidentiality

This study clearly revealed that patients who are in poor health condition have higher levels of concern about the privacy of their personal medical records. No patient is told by his health care provider about his diagnosis and treatment results will be stored electronically.

Only 66 (28.8%) of EMR users replied that the training they took to use EMR prepared them fully to keep patient privacy. In addition to this some users have no private Log in ID. This shows the presence of some gaps not to ensure privacy of patient's medical information. There is no adequate privacy protection policy

5.2 RECOMMENDATIONS

Based on the findings of the study the following recommendations are made:

1. Even though respondents are comfortable with the EMR system, privacy concerns are still there. Because the quality of health care depends on accurate information, patients should be free of any concerns related to their privacy. It is difficult to build public trust after full implementation of the EMR system. Therefore, government and other responsible bodies should implement and enforce strategies to strengthen privacy in this early stage.
2. In this study some EMR users identified that the training they took didn't prepare them fully to keep patient privacy and even have no individual log in ID and password. Therefore, these problems must be resolved by FMOH, the hospitals or by responsible bodies as quick as possible.
3. In this study patients said they have never told how their health data is being stored and processed. Health care providers should inform to their patients in order to avoid confusion and build public trust.
4. All patients and users need to be included before adopting new technologies. Therefore, the federal ministry of health should communicate patient associations to empower consumers to play a greater role in their own care.
5. This study is done only on EMR software in Zewditu and Ras Desta Damtew hospitals within a short period of time. This might not be representative of the whole privacy issues of E-health. Therefore, study needs to be conducted to further investigate ways of rapid adoption of health IT and realization of its potential benefits.

REFERENCES

1. ICT applications and cyber security division, implementing e-health in developing countries, September 2008, Geneva
2. Privacy Rights Clearing House, Medical Records Privacy: Fears and Expectations of Patients towards an Electronic patient Record, 1996, Australia.
3. Michael Smit et al, Privacy of Electronic Health Records: Public Opinion and Practicalities, 2006 , Canada
4. Laurinda B. Harman, PhD et al , Electronic Health Records: Privacy, Confidentiality, and Security,
5. Win K.T., Croll P., Cooper J., Alcock C. (2001), “Issues of Privacy, Confidentiality and Access in Electronic Health Record”, Journal of Law and Information Science, vol. 12, is. 1, pp 24-45
6. Gaithersburg I. V. (2000), “Electronic Medical Records and Patient Privacy”, The Health Care Manager, March, pp 63-69
7. Rindfleisch T.C. (1997), “Confidentiality, Information Technology and Health Care”, Communications of the Association of Computing Machinery, vol. 40, pp 93-100
8. Songini M.C., Dash J. (2000), “Hospital confirms hacker stole 5,000 patient files: attack points to need for standards for patient records”, Computer World, vol. 34, iss 51, pp 7
9. Carter M. (2000), “Integrated electronic health records and patient privacy: possible benefits but real dangers”, The Medical Journal of Australia, vol. 172, pp 28-30
10. Puplick C. (2003), “The privacy implications of the revolution in health technologies”, Australian Financial Review 5th Annual Health Congress
11. Etzioni A. Medical records: Enhancing privacy, preserving the common good. Hastings Cent Rep. 1999;29(2):14-23
12. National Center for Vital and Health Statistics. Enhanced Protections for Uses of Health Data. Washington, DC: Department of Health and Human Services; 2007.
13. Chilton L, Berger JE, Melinkovich P, et al. Privacy protection and health information: Patient rights and pediatrician responsibilities. Pediatrics. 1999; 104:973-977.

14. Dixon P. Medical identity theft: The information crime that can kill you. World Privacy Forum. 2006.
15. Hamilton BA. Medical Identity Theft Environmental Scan. Department of Health and Human
16. Blumenthal D, DesRoches C, Donelan K, et al. Health Information Technology in the United States: Where We Stand. Robert Wood Johnson Foundation;2008.
17. ABIM Foundation Medical Professionalism Project. Medical professionalism in the new millennium: A physician charter. *Ann Intern Med.*2002;136(3):243-246.
18. AMA Council of Ethical and Judicial Affairs. Code of Medical Ethics of the American Medical Association. 2008-2009 ed. Chicago, IL: American Medical Association; 2008.
19. Goold S, Lipkin M, Jr. The doctor-patient relationship: Challenges, opportunities, and strategies. *J Gen Intern Med.* 1999;14 (S1):S26-S33.
20. Pellegrino ED. The internal morality of clinical medicine: A paradigm for the ethics of the helping and healing professions. *J Med Philos.* 2001;26 (6):559-579.
21. Beauchamp T, Childress J. Principles of Biomedical Ethics. 6th ed. New York: Oxford University Press; 2009.
22. Whetten-Goldstein K, Nguyen TQ, Sugarman J. So much for keeping secrets: The importance of considering patients' perspectives on maintaining confidentiality. *AIDS Care.* 2001;13(4):457-465.
23. Wood, D. Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown. Government Accountability Office; 2007.
24. Kraman SS, Hamm G. Risk management: Extreme honesty may be the best policy. *Ann Intern Med.* 1999; 131(12):963-967.
25. Annual Study: Cost of a Data Breach: Understanding Financial Impact, Customer Turnover, and Preventative Solutions. Ponemon Institute; 2006.
26. Fischer J. Recent work on moral responsibility. *Ethics.* 1999; 110 (1):93-139.

27. Fraser, H.S. F., Biondich, P., Moodley, D., Choi, S., Wamlin, B. W., Szolovits, P. (2005), Implementing Electronic Medical Record systems in developing countries, *Informatics in Primary Care*, 13,83-95.
28. Katzenstein, J. & Chrispin, B. (2005). Effect of culture on the design of a Telemedicine System in Tanzania(abstract), *The fifth International Conference on Diversity in Organizations, Communities and Nations*, 30 June - 3July, 2005, Beijing, China.
29. Singh, K. (2006). Planning a hospital information system implementation, presented at *Global eHealth and Telemedicine Conference*, New Delhi (17-21 August, 2006).
30. Straub, D. W. Loch KD (2002). Toward a Theory Based Definition of Culture. *Journal of Global Information Management*, 10(1): 13-23.
31. Bates D W, Ebell M, Gotlieb E, Zapp J, Mullins H C, A proposal for electronic medical records in U.S. primary care. *Journal of the American Medical Informatics Association* 2003; 10; 1–10.
32. Cegala D J, Marinelli T, Post D M, The effect of patient communication skills training on treatment compliance in primary care, *Archives Family Medicine* 2000; 9; 448–57.
33. Stewart M A. Effective physician–patient communication and health care outcomes: a review. *Canadian Medical Association Journal* 1995; 152; 1423–33.
34. Ong L M, dehaes J C, Hoos A M, Lammes F., Doctor–patient communication: a review of the literature, *Social Science & Medicine* 1995; 40; 903–18
35. Bates, Kuperman, & Teich, 1994; Tierney et al., 1993
36. Garrett TM, Baillie HW, Garrett RM. *Health Care Ethics: Principles and Problems*, 4th edition. New Jersey: Prentice Hall; 2001.
37. Mandl KD, Szolovits P, Kohane IS. Public standards and patients’ control: how to keep electronic medical records accessible but private. *BMJ*. 2001;322(7281):283-287
38. National coordinator for HIT, *Guide to Privacy and Security of Health Information*, Version 1.2 060112, USA, 2004
39. Suh, R. (2006). *Health Information Technology 2006: Current Status and Future Directions*. Annual Meeting of the American College of Preventive Medicine

40. D.W. Bates et al., "Effect of Computerized Physician Order Entry and a Team Intervention on Prevention of Serious Medication Errors "Journal of the American Medical Association 280, no. 15 (1999): 1311-1316.
41. Koppel et al., "Role of Computerized Physician Order Entry Systems."
42. R.B. Haynes, H.P McDonald, and A.X. Garg, "Helping Patients Follow Prescribed Treatment: Clinical Applications," Journal of the American Medical Association 288, no. 22 (2002): 2880-2883.
43. B. Kaplan, Evaluating Informatics Applications—Clinic Decision Support Systems Literature Renew," International journal of Medical informatics 64, no. 1 (2001): 15-37
44. Tang, D., & Lansky, D, (2005). The Missing Link: Bridging the patient provider health information gap. Health Affairs, 24 (5), 1290-1295.
45. Tomasi, E., Facchini, L. A. & Maia, M. S (2004). Health information technology in primary health care in developing countries: a literature review, Bulletin of the World Health Organization, 82 (11), 867-874.
46. Chaudhry, B. (2006). Systematic Review: Impact of health information technology on quality, efficiency and costs of medical care. Annals of Internal Medicine, 144(10), 742
47. Fraser, H.S. F., Biondich, P., Moodley, D., Choi, S., Wamlin, B. W., Szolovits, P. (2005), Implementing Electronic Medical Record systems in developing countries, Informatics in Primary Care, 13,83-95
48. Health Information Management Systems Society HIMSS, 2003
49. National Center for Vital and Health Statistics. Enhanced Protections for Uses of Health Data. Washington, DC: Department of Health and Human Services; 2007.
50. Angus Reid, National Angus Reid omnibus survey for the Canadian Medical Association, 1998. Canada
51. Canadian Medical Association. Press release: Canadians highly value the privacy and confidentiality of their health information, 1999, Canada
52. Princeton Survey Research Associates, Medical privacy and confidentiality survey, 1999, USA
53. Goldman J., Protecting privacy to improve health care. Health Affairs 17, 6 (1998)

54. P. Chhanabhai and A. Holt. Consumers are ready to accept the transition to online and electronic records if they can be assured of the security measures. *Medscape General Medicine*, 9(1):8, 2007.
55. Health consumer attitudes to electronic medical records, Dr Inga Hunter, Massey University, September 2002.
56. The Importance and Value of Protecting the Privacy of Health Information, Joy L. Pritts, 1998
57. John Markoff, *Growing Compatibility Issue: Computers and User Privacy*, 1999, New York.
58. Michael Robling et al., *Public Attitudes towards the Use of Primary Care Patient Record Data in Medical Research without Consent: A Qualitative Study*, 2004
59. Michael Smit et al, *Privacy of electronic health records: public opinion and practicabliteis* , 2006, Canada
60. Angst et al. (2006), *Privacy and security in public health: maintaining the delicate balance between personal privacy and population safety*, Miami
61. Menachemi N and Langley A. The Use of Information Technologies Among Rural and Urban Physicians in Florida. *Journal of Medical Systems* 2007, 31(6):483-488
62. Loomis G. & Ries S. If Electronic Medical Records Are So Great, Why Aren't Family Physicians using them? , *Journal of Family Practice* 2002, 51(7):636-641.
63. Simon SR, Kalshal R & Cleary PD, *Physicians and Electronic Health Records "A Statewide Survey*, *Archives of Internal Medicine* 2007
64. National Consumer Health Privacy Survey 2005, California HealthCare Foundation (November 2005)
65. Tetali S. The importance of patient privacy during a clinical examination. *Indian Journal of Medical Ethics*, 2007, 4(2):66.
66. Higgins G. The history of confidentiality in medicine: the physician-patient relationship. *Canadian Family Physician*, 1989, 35:921–926.
67. Policy Engagement Network. *Electronic health privacy and security in developing countries and humanitarian operations*. London School of Economics and Political Science, 2010

ANNEXES

Annex 1 Consent Form

I, the undersigned, confirm that, as I give consent to participate in the study with a clear understanding of the objectives and conditions of the study and with recognition of my right to withdraw from the study if I change my mind.

Ido hear by give consent to DR/Mr./Miss.....to include me in the proposed research. I have been given the necessary information about the research. I have also been assured that I can withdraw my consent at any time without penalty or loss of benefits .The proposal has been explained to me in the language I understand.

Name of the participant: _____

Participant's signature: _____

Name of Dr/Mr./Miss:_____

Dr/Mr./Mrs./Miss signature: _____

Date: _____

Witness: _____ Date:_____

Annex 2 Questionnaires for EMR Users

ADDIS ABABA UNIVERSITY

SCHOOL OF PUBLIC HEALTH AND SCHOOL OF INFORMATION SCIENCE

I. English questionnaires

Structured English questionnaires to assess the privacy and confidentiality issues of electronic medical record application: users, health managers and patients' perception in Zewditu and Ras Desta Damtew hospitals.

01. Code Number -----/-----
02. Hospital _ 1. Zewditu 2. Ras Desta Damtew

Greeting

Hello! My Name is; _____. I am interviewing patients, health professionals and health managers. We would like to ask you a few questions in order to assess the existing electronic medical records. You do not have to answer any question that you do not want to answer and you may end this interview at any time you want to; however your honest answer to these questions will help us to the better understanding of the conditions.

Verbal consent and confidentiality

All information given by you will be strictly confidential. Your name will not be recorded in this form and will never be used in connection with any information you are telling us. We greatly appreciate your cooperation in responding to this study. Would you be willing to participate? If yes, proceed. If no, thank you and stop here.

(Signature of the interviewer certifying the informed consent has been given verbally by respondent _____.)

Thank you. Let's begin.

Date of interview ____/ ____/ ____

Beginning time -----

Section -1- Background Characteristics

S/N	Questions	Response	Skip
1.1	Sex	Male <input type="checkbox"/> Female <input type="checkbox"/>	
1.2	Age	-----	
1.3	Religion	Orthodox <input type="checkbox"/> Catholic <input type="checkbox"/> Muslim <input type="checkbox"/> Other <input type="checkbox"/> Protestant <input type="checkbox"/>	
1.4	Occupational category	Nurse <input type="checkbox"/> Data clerk <input type="checkbox"/> Clinician <input type="checkbox"/> Manager <input type="checkbox"/> Pharmacist <input type="checkbox"/>	
1.5	In which health care service are you assigned currently?	OPD <input type="checkbox"/> Laboratory <input type="checkbox"/> Pharmacy <input type="checkbox"/> Imaging <input type="checkbox"/> Ward <input type="checkbox"/>	

Section -2- Knowledge about Electronic Medical Records

2.1	Have you used paper based medical records before?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
2.2	Do you know about Electronic medical records?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
			<input type="checkbox"/>

2.3	Who trained you to use the EMR system?	By NGO <input type="checkbox"/>	Self trained <input type="checkbox"/>	
		By other <input type="checkbox"/>	Was never trained <input type="checkbox"/>	
2.4	How long have you been using the EMR?	Less than 6 months <input type="checkbox"/>	19-24 months <input type="checkbox"/>	
		6-12 months <input type="checkbox"/>	Above 24 months <input type="checkbox"/>	
		13-18 months <input type="checkbox"/>		
2.5	How adequately did the training prepare you to keep patient privacy?	Fully <input type="checkbox"/>	Not at all <input type="checkbox"/>	
		Mostly <input type="checkbox"/>	Not applicable <input type="checkbox"/>	
		Somewhat <input type="checkbox"/>		
2.6	Is there a means to control over who can access patient data among employees in your hospital?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
2.7	Do you have individual log in ID and password?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
Section -3 - Perception towards Electronic medical records				
3.1	Which one is more secured between the EMR and Paper based records?	EMR <input type="checkbox"/>		
		Paper form <input type="checkbox"/>		
		Both are about the same <input type="checkbox"/>		
3.2	In which is the information about patients safer? (Privacy)	EMR <input type="checkbox"/>		
		Paper form <input type="checkbox"/>		
		Both are about the same <input type="checkbox"/>		
3.3	Where do you think patients Privacy is at risk? (Multiple answers are possible).	Registration room <input type="checkbox"/>		
		OPD <input type="checkbox"/>		
		Laboratory <input type="checkbox"/>		
		Wards <input type="checkbox"/>		
		Imaging <input type="checkbox"/>		

3.4	Do you trust EMR not to reveal sensitive health data?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
3.5	What concerns you in a move to electronic medical records?	Data leaks <input type="checkbox"/>	Sensitive information will be shared <input type="checkbox"/>	
		Poor security <input type="checkbox"/>	Increased medical errors <input type="checkbox"/>	
		It doesn't concern me <input type="checkbox"/>		
3.6	Is there any privacy protection policy that is supposed to ensure public's confidence?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
3.7	If your answer is yes, are they adequate to protect patients' privacy?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
3.8	Which patients do you think need more privacy and confidentiality of EMR?	People with HIV <input type="checkbox"/>	Adolescents using drugs <input type="checkbox"/>	
		People with mental problems <input type="checkbox"/>	STI and Family planning pts <input type="checkbox"/>	
		All <input type="checkbox"/>		
3.9	How has the EMR changed your patients' privacy?	Decreased significantly <input type="checkbox"/>	Decreased a little <input type="checkbox"/>	
		Not changed <input type="checkbox"/>	Improved a little <input type="checkbox"/>	
		Improved significantly <input type="checkbox"/>		
3.10	Which system do you prefer to keep your patients privacy?	EMR <input type="checkbox"/>	Paper based <input type="checkbox"/>	
		<input type="checkbox"/>		

		Any (doesn't matter)	
Section -4-Practice and sources of concern regarding the potential negative impacts of EMR's			
4.1	Do you think Electronic medical records will speed up access to a patient's health information?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
4.2	Do you think pledge of confidentiality is now challenged by computers rule and health information falls into many hands?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
4.3	Have you ever encountered problems of loss of privacy?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
4.4	If you encounter problems please elaborate	----- -	
4.5	Did you tell your patient about sensitive but important information will go into computerized records?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
4.6	Have you ever used patient information for research or other purpose?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
4.7	If your answer is YES to the above question have you gained consent from your patient?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
4.8	Who do you think will be beneficiary in transition from paper based to EMR?	Patient <input type="checkbox"/>	Development partners <input type="checkbox"/>
		FMOH <input type="checkbox"/>	All of the above <input type="checkbox"/>
		None of them <input type="checkbox"/>	

4.9	Do you think health consumer involvement is important before adopting new technologies?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
4.10	What do you think about poor adoption rate and poor utilization of EMR? b/s	Poor patient involvement <input type="checkbox"/>	Consumes time <input type="checkbox"/>	
		Changes the usual work process <input type="checkbox"/>	Lack of training <input type="checkbox"/>	
		It is of no value <input type="checkbox"/>		
4.11	Do you think all health care information should be stored within an EMR?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
4.12	Do you think the information that is shared as a result of a clinical relationship is confidential and protected?	Yes <input type="checkbox"/>	No <input type="checkbox"/>	
4.13	If your answer is NO to the above question, what is your option to ensure confidentiality of your patients' data?	----- ---		
4.14	To which organization, you think, should privacy law allow to exploit patient data without a patient's knowledge or consent?	Pharmaceutical companies <input type="checkbox"/>	Researchers <input type="checkbox"/>	
		Law enforcement <input type="checkbox"/>	All <input type="checkbox"/>	
		Insurance providers <input type="checkbox"/>	None of them <input type="checkbox"/>	
4.15	Overall, are you satisfied with the EMR system?	Always satisfied <input type="checkbox"/>	Somewhat satisfied <input type="checkbox"/>	
		Mostly satisfied <input type="checkbox"/>	Not at all satisfied <input type="checkbox"/>	

That is the end of our questionnaire. Thank you very much for taking time to answer these questions. We very much appreciate your help.

Time at the end of interview _____

Annex 3 Questionnaires for Patients

ADDIS ABABA UNIVERSITY

SCHOOL OF PUBLIC HEALTH AND SCHOOL OF INFORMATION SCIENCE

I. English questionnaires (patients)

Structured English questionnaires to assess the privacy and confidentiality issues of electronic medical record application: users, health managers and patients' perception in Zewditu and Ras Desta Damtew hospitals.

01. Code Number -----/----- 02. Hospital _ 1. Zewditu 2. Ras Desta Damtew

Greeting

Hello! My Name is; _____ I am in the research team of Addis Ababa University in the collaboration with Addis Ababa Regional Health Bureau. We are interviewing patients, health professionals and health managers. We would like to ask you a few questions in order to assess the existing electronic medical records. You do not have to answer any question that you do not want to answer and you may end this interview at any time you want to; however your honest answer to these questions will help us to the better understanding of the conditions.

Verbal consent and confidentiality

All information given by you will be strictly confidential. Your name will not be recorded in this form and will never be used in connection with any information you are telling us. We greatly appreciate your cooperation in responding to this study. Would you be willing to participate? If yes, proceed. If no, thank you and stop here.

(Signature of the interviewer certifying the informed consent has been given verbally by respondent _____.)

Thank you. Let's begin.

Date of interview ____/ ____/ ____

Beginning time -----

Section one Background Information

S/N	Questions	Response	Skip
1.1	Sex	Male <input type="checkbox"/> Female <input type="checkbox"/>	
1.2	Age	-----	
1.3	Religion	Orthodox <input type="checkbox"/> Catholic <input type="checkbox"/> Muslim <input type="checkbox"/> Other <input type="checkbox"/> Protestant <input type="checkbox"/>	
1.4	Educational status	Illiterate <input type="checkbox"/> Grade 7-10 <input type="checkbox"/> Read and Write <input type="checkbox"/> Grade 11-12 <input type="checkbox"/> Grade 1-6 <input type="checkbox"/> Above grade 12 <input type="checkbox"/>	
1.5	Which service you received with this visit?	Family planning <input type="checkbox"/> ART <input type="checkbox"/> Abortion care <input type="checkbox"/> Other specify -----	

Section -2- Knowledge

2.1	Do you know about EMR?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
2.2	Which one is more secured between the EMR and Paper based records?	EMR <input type="checkbox"/> Paper form <input type="checkbox"/> Both are about the same <input type="checkbox"/>	
2.3	In which is the information about patients safer? (Privacy)	EMR <input type="checkbox"/> Paper form <input type="checkbox"/> Both are about the same <input type="checkbox"/>	
2.4	Where do you think patients Privacy is at risk?	Registration room <input type="checkbox"/> OPD <input type="checkbox"/> Laboratory <input type="checkbox"/> Imaging <input type="checkbox"/> Wards <input type="checkbox"/>	
2.5	Do you trust EHR not to reveal sensitive health data?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
2.6	What concerns you in a move to electronic medical records?	Data leaks <input type="checkbox"/> Sensitive information will be shared <input type="checkbox"/> Poor security <input type="checkbox"/> Increased medical errors <input type="checkbox"/> It doesn't concern me <input type="checkbox"/>	

2.7	Which patients do you think need more privacy and confidentiality of EMR?	People with HIV <input type="checkbox"/> Adolescents using drugs <input type="checkbox"/> People with mental problems <input type="checkbox"/> STI and Family planning pts <input type="checkbox"/> All <input type="checkbox"/>	
2.8	Between paper based record and EMR, which system do you prefer to keep your privacy?	EMR <input type="checkbox"/> Paper based <input type="checkbox"/> Any (doesn't matter) <input type="checkbox"/>	
2.9	Have you ever encountered problems of loss of privacy?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
2.10	If you encounter problems please elaborate	-----	
2.11	Who do you think will be the most beneficiary in transition from paper based to EMR?	Patient <input type="checkbox"/> All <input type="checkbox"/> Donors <input type="checkbox"/> None <input type="checkbox"/> FMOH <input type="checkbox"/>	
2.12	Do you think health consumer involvement is important before adopting new technologies?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
2.13	Do you think all health care information should be stored within an EMR?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
2.14	Do you need to be consulted before your medical record information is released for research purpose?	Yes <input type="checkbox"/> No <input type="checkbox"/>	
2.15	Overall, are you satisfied with the EMR system?	Always satisfied <input type="checkbox"/> Not at all satisfied <input type="checkbox"/> Mostly satisfied <input type="checkbox"/> Please explain ----- Somewhat satisfied <input type="checkbox"/>	

That is the end of our questionnaire. Thank you very much for taking time to answer these questions. We very much appreciate your help.

Time at the end of interview _____

Annex 4 Amharic version questionnaire for patients

በአዲስ አበባ ዩኒቨርሲቲ የህክምና ፋኩልቲ የህብረተሰብ ጤና ት/ት ክፍል በኮምፒውተር የታገዘ የህመማን መረጃ አያያዝን በተመለከተ የህመማንና የጤና ባለሞያዎችን አመለካከት ለማጥናት የተዘጋጀ መጠይቅ ፤

መግቢያ

ሰላምታ። ስሜ -----ይባላል። በአዲስ አበባ ዩኒቨርሲቲ የህክምና ፋኩልቲ የጥናት ቡድን አባል ነኝ። የዚህ ጥናት አላማ በኮምፒውተር የታገዘ የህመማን መረጃ አያያዝን በተመለከተ በአዲስ አበባ ጤና ቢሮ ስር ከሚገኙ ሆስፒታሎች መካከል በተወሰኑት ላይ የህመማንና የጤና ባለሞያዎችን አመለካከት ለማጥናት ነው።

የእርስዎ በዚህ መጠይቅም ሆነ ጥናት መሳተፍ በሙሉ ፍላጎትዎ ላይ የተመሰረተ ነው። ለመመለስ የማይፈልጉት ጥያቄ ካለ ያለመመለስ መብትዎ የተጠበቀ ነው። ቢሆንም ለሚያደርጉልን ቀና ትብብር ምስጋናዬ ከፍ ያለ ነው። ግልጽ ያልሆነልዎ ጥያቄ እንዲብራራልዎ መጠየቅ ይችላሉ። መመለስ የማይፈልጉት ጥያቄ ካለ በፈለጉበት ጊዜ ማቆም ይችላሉ። በመጨረሻም እርስዎ የሚሰጡትን መልሶች ከማንኛውም አካል በሙሉ ሚስጥርነት አንደሚጠበቅና የእርስዎ ስም በመጠይቁ ላይ አንደማይመዘገብ እገልጻለሁ።

ስለዚህ በመጠይቁ ለመሳተፍ ፍቃደኛ ነዎት?

- አዎ----- 1
- አይደለሁም----- 2 አቁም

ተጠያቂው የቃል ስምምነት ማድረጉን የሚያሳይ የቃል መጠይቁ አቅራቢ ፊርማ -----

የቃል መጠይቁ አቅራቢ ኮድ _____

ስም _____

ፊርማ _____

ቃለ መጠይቁ የቀረበበት ቀን _____

ክፍል አንድ፡ ማህበራዊ እና ስነ ህዝባዊ				
ተ.ቁ	ጥያቄዎች	አማራጭ ምላሾች	ወደ ተ.ቁ	ኮድ
1.1	ጾታ	ወ <input type="checkbox"/> ሴ <input type="checkbox"/>		
1.2	እድሜ	-----		
1.3	ሀይማኖት	ኦርቶዶክስ <input type="checkbox"/> ሙስሊም <input type="checkbox"/> ካቶሊክ <input type="checkbox"/> ፕሮቴስታንት <input type="checkbox"/> ሌላ <input type="checkbox"/>		
1.4	የት/ት ደረጃ	ያልተማረ <input type="checkbox"/> ማንበብና መጻፍ <input type="checkbox"/> ከ 1-6 ኛ ክፍል <input type="checkbox"/> ከ6-12 <input type="checkbox"/> ከ 12 በላይ <input type="checkbox"/>		
1.5	በዚህ ጉብኝትዎ ያገኙት አገልግሎት	የቤተሰብ ምጣኔ አገልግሎት <input type="checkbox"/>		

	የትኛውን ነው;	የውርጃ አገልግሎት <input type="checkbox"/> የኤች አይ ቪ ኤድስ አገልግሎት <input type="checkbox"/> ሌላ (ይጠቀስ) -----		
ክፍል 2: ስለ ህመማን መረጃ አያያዝ በተመለከተ				
2.1	በኮምፒውተር የታገዘ የህመማን መረጃ አያያዝ ዘዴ መኖሩን ያውቃሉ?	አዎ <input type="checkbox"/> አላውቅም <input type="checkbox"/>		
	የህክምና ውጤትዎ ከወረቀት ፋይል በተጨማሪ ወደ ኮምፒውተር እንደሚገባ ያውቃሉ?	አዎ <input type="checkbox"/> አላውቅም <input type="checkbox"/>		
2.2	የህመማንን ሚስጥር ከመጠበቅ አንጻር የትኛው ዘዴ የተሻለ ነው ብለው ያምናሉ?	በኮምፒውተር የታገዘ <input type="checkbox"/> በወረቀት/ፋይል <input type="checkbox"/> ልዩነት የላቸውም <input type="checkbox"/>		
2.3	ጎርፍ ፤ ቃጠሎና መሰል አደጋዎችን ከመቋቋም አንጻር የትኛው ዘዴ የተሻለ ነው ብለው ያምናሉ?	በኮምፒውተር የታገዘ <input type="checkbox"/> በወረቀት/ፋይል <input type="checkbox"/> ልዩነት የላቸውም <input type="checkbox"/>		
2.4	የህመማን የህክምና ውጤትና ሚስጥር በየትኛው ክፍል ይበልጥ የተጋለጠ ነው ብለው ያምናሉ?	ካርድ ክፍል <input type="checkbox"/> ላብራቶሪ <input type="checkbox"/> በተመላላሽ ህክምና ክፍል <input type="checkbox"/> በአስተኝቶ ማከም ክፍል <input type="checkbox"/> በራጅ ክፍል <input type="checkbox"/>		
	በኮምፒውተር የታገዘው የህመማን	<input type="checkbox"/>		

2.5	መረጃ አያያዝ ዘዴ ሚስጥራን ሙሉ ለሙሉ ይጠብቅልኛል ብለው ያምናሉ?	አዎ <input type="checkbox"/> አይደለም <input type="checkbox"/>		
2.6	ከወረቀት ወደ ኮምፒውተር ዘዴ ባለው ሽግግር ላይ ምን ስጋት አለዎ?	የመረጃ መንጠባጠብ <input type="checkbox"/> የመረጃ ደህንነት ማኅስ <input type="checkbox"/> የህክምና ስህተት <input type="checkbox"/> ምንም አያሰጋኝም <input type="checkbox"/>		
2.7	የየትኞቹ ህሙማን ሚስጥር የበለጠ መጠበቅ አለበት ብለው ያምናሉ?	የኤች አይ ቪ ህሙማን <input type="checkbox"/> ዕጽ ተጠቃሚ ወጣቶች <input type="checkbox"/> የአእምሮ ህሙማን <input type="checkbox"/> የቤተሰብ ምጣኔ አገልግሎት ተጠቃሚዎች <input type="checkbox"/> የሁሉም ህሙማን <input type="checkbox"/>		
2.8	የእርስዎ የህክምና ውጤት በየትኛው ዘዴ ቢቀመጥልዎ ይመርጣሉ?(ሚስጥራዊ)	በኮምፒውተር የታገዘ <input type="checkbox"/> በወረቀት/ፋይል <input type="checkbox"/> በማንኛውም <input type="checkbox"/>		
2.9	ከዚህ በፊት የህክምና መረጃ አያያዝ በተመለከተ ችግር አጋጥሞት ያውቃል?	አዎ <input type="checkbox"/> የለም <input type="checkbox"/>		
2.10	ካጋጠሞት እባኮን ያብራሩልን	-----		
2.11	ከወረቀት ወደ ኮምፒውተር ዘዴ	ህሙማን <input type="checkbox"/> <input type="checkbox"/>		

	በሚደረገው ሽግግር ይበልጥ ተጠቃሚው አካል የትኛው ነው ብለው ያምናሉ?	እርዳታ ድርጅቶች ጤና ጥበቃ ሚኒስቴር <input type="checkbox"/> ሁሉም <input type="checkbox"/>		
2.12	አዲስ ቴክኖሎጂ ከመቀበል በፊት ከህመማን ተወካይ ጋር ውይይት ማድረግ አስፈላጊ ነው ብለው ያምናሉ?	አዎ <input type="checkbox"/> የለም <input type="checkbox"/>		
2.13	ሁሉም የምርመራ ውጤቶች በኮምፒውተር መመዘገብ አለባቸው ብለው ያምናሉ?	አዎ <input type="checkbox"/> የለም <input type="checkbox"/>		
2.14	የምርመራ ውጤት ለጥናት ከመወሰዱ በፊት ፈቃደኝነት እንዲጠየቁ ይፈልጋሉ?	አዎ <input type="checkbox"/> የለም <input type="checkbox"/>		
2.15	በአጠቃላይ በኮምፒውተር በሚያዘው የህመማን መረጃ ደስተኛ ነዎት?	በእጅግ <input type="checkbox"/> በመጠኑ <input type="checkbox"/> በጭራሽ <input type="checkbox"/>		

ይህ የጥያቄዎቻችን መጨረሻ ነው። እነዚህን ጥያቄዎች በመመለስ ጊዜ ወስደው ላደረጉልን ትብብር በጣም እናመሰግናለን።

ቃለመጠይቁ ያበቃበት ሰዓት _____

ፊርማ _____

