Addis Ababa University
School of Graduate Studies
College of Natural Sciences
Department of Computer Science

Enhancing Information Security and Privacy of Health Information System: A case of OpenMRS

Selemawit Hadush Kidanu

A THESIS SUBMITTED TO THE SCHOOL OF GRADUATE STUDIES OF THE ADDIS ABABA UNIVERSITY IN PARTIAL FULFILLMENT FOR THE DEGREE OF MASTERS OF SCIENCE IN COMPUTER SCIENCE

April , 2015

Addis Ababa University
School of Graduate Studies
College of Natural Sciences
Department of Computer Science

Enhancing Information Security and Privacy of Health Information System: A case of OpenMRS

Selemawit Hadush Kidanu

Advisor: Dr.Dejene Ejigu and Berhanu Borena

Approved By

Examining Board:

Name	Signature
1. Dr.Dejene Ejigu, Advisor	_____
2. Berhanu Borena, Advisor	_____
3. _____	_____
4. _____	_____

Acknowledgement

I am humbly grateful to my God for guiding me and helping me all the way through. First and foremost, I would like to express my gratitude for Addis Ababa University for providing me opportunity to attend this program.

I would like to express my deep gratitude to my advisors, Dr.Dejene Ejigu and Ato Berhanu Borena for their firm support and guidance in directing my thesis. This work would not have been possible without the constant guidance of them. They taught me to think critically, they encouraged my ideas, and most importantly, they were there whenever I needed help.

I cannot end without thanking my family, none of this work would have been possible were it not for the support of my family. I want to thank them for their constant love, encouragement, patience, selflessness and sacrifice.

Finally, no words seem enough and appear weak and insufficient to define all sorts of help and strong support throughout the study. I would like to express my sincere gratitude to all who helped me and letting me follow my dreams through all ways.

Table of Contents

List of Figures

List of Tables

Acronyms

AES	Advanced Encryption Standard
ED	Emergency Department
EMR	Electronic Medical Record
HIAS	Health Information Access Control
HIE	Health Information Exchange
HINS	Health Information Network Security
HIS	Health Information System
HMIS	Health Medical Information System
IBAC	Identity Based Access Control
MRI	Medial Record Information
NEHTA	National E-Health Transition Authority
OpemEMR	Open Electronic Medical Record
OpenMRS	Open Medical Record System
OTHIS	Open and Trusted Health Information System
PBAC	Purpose Based Access Control
PCEHR	Personally Controlled Electronic Health Record
PHR	Patient Health Record
RBAC	Role Based Access Control
RSA	Ron Rivest, Adi Shamir, and Leonard Adleman
TT-RBAC	Team and Task Based Role Based Access Control

Abstract

Security is a vital part of daily life to healthcare organizations that need to ensure the information is adequately secured. The existing infrastructure lacks the structural security and privacy elements needed to support the evolving IT infrastructure, emerging legislative regulations, and ever increasing threats. The problem, then, is how we can maintain the availability of the right information at the right time and at the same time maintain the security and privacy of patient information.

This research took a broad approach into existing information security and privacy of healthcare domain with practical focus on Black Lion Hospital and Korean Hospital. The main theme of this thesis is that such major paradigm shifts or using/adopting new technologies demand a rethinking of the security and privacy aspects and solutions. The desire is to engage all parties, including the clinicians and patients, and understand what is acceptable and desirable before the coming generation of healthcare systems is deployed. There will certainly be tension between security and usability, between patient privacy and the clinician convenience. The point here is, therefore, to hit the balance between the two and come up with a system that satisfies both. Thus, to overcome the limitations and enable the complete protection of sensitive information this study reviews existing information security and privacy of health information system and the available open source software that can be enhanced with such service and used to improve the HIS.

We proposed and implemented a prototype that enhances information security and privacy of HIS using OpenMRS. The prototype's main security and privacy features includes confidentiality on the server side that is ensured by a carefully placed access control mechanism, encryption that protects the confidentiality during transfer of the data and at storage, anonymization of patient medical record and the use of log files. The proposed prototype meets all of our objectives. Finally, the prototype is tested using OpenMRS demo data and evaluated by health professionals in Black Lion Hospital and Korean Hospital. The result is encouraging and full deployment can be thought of.

Keywords: Information Security, Privacy, Health Information System, Electronic Medical Record, OpenMRS

Chapter 1

Introduction

1.1 Background

Security and privacy have become predominant concern of different stakeholders, users, governments, service providers, systems developers and systems administrators. These concerns are even growing more in health information systems [1]. Information system plays an important role in information processing in healthcare for the benefit of the hospital [2]. It has many advantages such as faster access, storage and retrieval of data, cost effectiveness, user friendliness, and more secure and involved less manpower [3].

Health Information System (HIS) support patients and also doctors, nurses, paramedical and other healthcare providers in diagnosing, treating and supporting patients [4]. Healthcare is not only a health but also a life and death issue. In such serious issue patients have to trust healthcare providers and both patients and healthcare providers depend on the trustworthiness of the information systems used. Unfortunately, privacy and security requirements are frequently expressed in vague, contradictory and complex laws and regulations. It is a major concern that requires new approaches in systems design. Trustworthy HIS need to provide effective, high quality support for providing the best care for patients but without compromising their privacy and security [4].

Information security in health sector refers to protecting personal health related records from unauthorized access, use, disclosure, disruption, modification or destruction. Patients fear that their personal medical information may influence their employers' decisions about promotions or downsizing or be made public in press reports or civil court actions. Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others [5].

Nowadays, many healthcare organizations are vulnerable to security attacks due to the fact that they contain sensitive patient information [6]. Patients are required to share information with their physicians to facilitate accurate diagnosis and treatment, especially to avoid adverse drug interactions. Patients trust their health providers if their information is kept private and secure. This leads them to be more willing to discuss their symptoms, conditions, and past and present

risk behaviors [6]. However, patient data can be hacked, manipulated, or destroyed by internal or external users and result for improper modification of diagnosis results that can threaten patient health or even his/her life [7]. Patient health information plays a major role in conducting medical research for improving healthcare quality. However, disclosure of health information for various reasons raises concerns of privacy [8].

Ensuring privacy and security of health information, including information in electronic Medical Records (EMR) is the key component to building the trust required to realize the potential benefits of electronic health information exchange. But, developing a secure and scalable architecture for healthcare information system is a difficult task due to the higher complexities within the healthcare environment [9].

To address the problems of HIS many free and open source HIS systems such as Open Medical Record System (OpenMRS), OpenEmr, ClearHealth and OpenVista are developed. However, all free and open source systems that are highly used in the developing world lack sufficient response in the architecture and implementation of security and privacy protection. This thesis work responds to such gap by architecting, implementing and testing security features to the free and open health information system OpenMRS as a case in Black Lion and Korean Hospital in Ethiopia.

1.2 Motivation

Health information systems (HIS) have become a crucial component for strengthening the health systems in developing countries. The usage of health data is extended not only for patient care and administrative purpose but also for planning and decision making in improving health service. HIS emergence has, therefore led to shifting from paper based to computer based processing of health information. This shift has increased the opportunities of manipulating patient data efficiently. However, currently, the vast majority of health records in Ethiopia are still in non electronic form or paper based, dispersed across many institutions, pressures related to Emergency Department (ED) overcrowding and cost containment make it increasingly important to characterize the patients we serve and analyze the work we do. But a lot of patient records are lost due to lack of security, there is no well documented privacy and security policy and procedures to be applied in hospitals. Above all well established information system does

not exist in many hospitals or are health posts. The technological complexity challenge in using the advanced tools of processing health data also raised this problem. Providing solution to such a problem is the motivation of the current research work.

Thus, privacy and security concerns would be major impediments to be dealt by electronic health information system. If they are not properly addressed or unless critical privacy and security problems are overcome, healthcare seekers will not feel comfortable in participating and healthcare professionals will face huge liability risks. This is especially true in countries like Ethiopia where healthcare system is just expanding.

1.3 Statement of the Problem

With the implementation of electronic patient records and the Internet and Intranets, medical information sharing among relevant healthcare providers is made possible. But the vital issue in this method of information sharing is security, patient privacy, as well as the confidentiality and integrity of the healthcare information system.

The privacy and security of health information is an important concern for all those delivering healthcare and is especially crucial for those who care for HIV/AIDS patients. Any inappropriate disclosure of such patient's information, state of disease, patient condition may yield serious consequences on the patient social life [10]. One of these social pressures that could result in the abandoning of the health service is stigma and discrimination. Stigma and discrimination can persist on patients and patients may continue to be disappointed in healthcare, housing, and the workplace. Fear of stigma and discrimination affects their decision to obtain care or go to health centers, as it may discourage them from seeking HIV testing and treatment [10].

Trust may not be established or incorrectly defined between different healthcare domains and patients because the privacy of personal medical records and health information is not protected well enough.

Since most of the healthcare systems use role based access, modification of information such as doctor notes and laboratory test results are done by unauthorized person.

We have visited different public and private hospitals or healthcare organizations such as Tikur Anbesa, Korean, Mentesnot, Yekatit 12, Kadisco, and St. Gebriel hospitals in Ethiopia. None of

the healthcare systems we visited have powerful security control mechanism capable of accessing all sensitive medical information.

In order to address this problem and to achieve high level of information security and privacy in HIS, this work examines customization architecture for the system. An open source HIS with lack of privacy and security mechanisms is selected to implement and evaluate the customization solution to meet privacy and security requirements focusing on the **Black Lion and Korean Hospitals.**

To address this research problem, the following research questions are forwarded:

- ✓ What are the available open sources that can be used in health information system?
- ✓ Which of those open source systems are appropriate for building secure HIS?
- ✓ What security architecture and implementation is suitable to safeguard patient information in HIS?

1.4 Objective

General Objective

The general objective of this work is to enhance and implement the security and privacy architecture of healthcare system in order to address the security and privacy requirements in health information system.

Specific Objectives

To achieve the above general objective, the following specific objectives are identified:

- Analyze the current system security and privacy protection architectures
- Identify key privacy and security questions that health information system must consider
- Examine current privacy and security policies, if any
- Design possible architecture that supports security and privacy of open source health information systems
- Implement and test the developed system.

1.5 Scope and Limitation

The scope of this thesis is to evaluate solutions that bridge the gap between usability, privacy and security in a way that will create a secure and scalable architecture for accurate information exchange and secure authentication and authorization to patients' medical records to assist in patient diagnosis and treatment. It includes features like protecting sensitive information at rest, in transit and in use, protecting access to sensitive information with strong authentication and improving security and privacy policy agreement. But, it does not include the development of detail patient information system such as patient registration, storage of patient history system.

1.6 Methodology

This section describes the methods used in this research. Our research is conducted through different phases using different research methodology. To attain the appropriate solution for our objectives we have chosen the flowing methods**:**

1.6.1 Selection of Study Unit

Tikur Anbessa (the English name of the hospital, Black Lion is used here after) Hospital from public and Korean Hospital from private have been selected for the proposed research work as a case for detailed study.

Black Lion and Korean hospitals were selected considering their capacity in serving large number of patients, largest and the oldest health training institution in the country, the facility they provide like HIV/AIDs and Cancer.

Black Lion hospital is a teaching and national referral hospital located at the center of Addis Ababa. It is one of the biggest Ethiopian hospitals and it aspires to become a center of excellence in the diagnosis, treatment and care of patients with cancer [11]. In addition to its comprehensive healthcare service, the hospital is hoping to develop a comprehensive cancer care program, including cancer registry, early detection, prevention, standard treatment and palliative care. By addressing the shortage of medications and meeting the growing demand for oncology trained doctors and nurses, hospital leaders are optimistic, that with the support of international partners such as INCTR, Black Lion Hospital can become a model cancer center and take the lead in improving Ethiopia’s response to its increasing cancer problem [11]. Unfortunately, the hospital

suffers from different challenges that emancipated from the paper based information management practice.

It is essential to take the potential doctors and patients views and suggestions regarding the current health information system to find the possibilities to introduce the proposed system for the improvement of security and privacy in health information system.

1.6.2 Fact Finding Method

All the necessary data from different data sources are collected by using different methods including:

- ✓ **Literature Review:** To identify the existing technologies and analyze the current situations and make the system feasible. We have read literature to obtain a better understandable of effective management of information of security in different areas. To explore properly how it is working, to what extent the healthcare system is satisfied within existing information security application and resources today. In addition, does the existing development fulfill the security requirements, standards and needs of healthcare organizations? Our research methodology was to conduct several interviews to know the existing information security approach in healthcare and whether it fulfills the security requirements of management. After analyzing the current information security structure of healthcare, we have proposed some recommendations, guidelines. Hopefully, the proposed suggestions will be able to enhance the information security to sensitive information of healthcare. High level of patient security would be possible to obtain in electronic based healthcare system while still effecting availability and accessibility.
- ✓ **Observation:** information that cannot be attained from the interview or fear of others, observation is used to acquire practical problems.
- ✓ **Interview:** We will have interview with healthcare givers (physicians and nurses), IT staff and manager of the hospital about security and privacy issues.
- ✓ **Questionnaires:** we will prepare and distribute questionnaires among the healthcare givers (physicians and nurses) in order to know the extent of patients' security and privacy concern from their point of view.

1.6.3 Development Tools

Different tools that are suitable to achieve the objective will be selected. After literature review and related works has been carried, based on the identified research problem and design of the architecture a prototype will be developed. Major activities performed in this stage includes: specifying the requirements of the prototype, choosing appropriate programming languages and technologies, algorithms needed for implementing the prototype. The developed prototype will tested for correctness using test data set. The outcome of the study was evaluated with the appropriate evaluation techniques to check whether the prototype is applicable and achieve our goals correctly or not.

By considering economically viable EMRS and security and privacy implementation capability as technical key component we use Open Medical Record System (OpenMRS). OpenMRS is popular internationally and in public health, with a very active open source development community. None of the open source tools we found on Git are that popular. Compared to other open source OpenMRS is selected for implementation because of its scalability, multi layered architecture, flexibility, uses standards such as HL7, use of encryption of data transmitted over the web using Secure Socket Layer (SSL) Protocol. But, other open source systems do not full fill all these features. Moreover, from a developer perspective the major advantage of OpenMRS is its modular software architecture. This allows separate components of software to “plug in” to the main system and allows additional functionalities to be added (and removed) without changing the core system.

1.7 Significance of the Work

Healthcare system is one of the major issues for developing countries and thus the information technology is becoming progressively more important nowadays. So, this thesis result will enable to establish greater public trust in HIS and hosting hospitals. It is applicable to:

- ✓ Minimize fear of stigma and discrimination
- ✓ Accurate patient identification
- ✓ Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the privacy regulations.

- ✓ Increase communication between healthcare providers

Generally, the system provides reliable, timely and high quality service for hospitals to provide reliable, timely and high quality product for Black lion hospital.

1.8 Ethical Considerations

Medical ethics is a law that specifies how physicians are required to deal with ethical issues of the hospital with regards in patient care including their security, privacy and research. Preserving security and privacy of individual patient is one way of showing respect to them. Since individuals can have different privacy concerns, care must be taken by determining which personal information a patient needs to keep hidden and on which he/she is willing to share with others. Physicians have to act in the interest of patients while providing medical care since the reverse way might cause weakening the mental, moral and physical conditions of the patient. They are expected to be aware of their obligations under the data protection acts in relation to secure storage and eventual disposal of such information. Patients are eligible to get a copy of their own medical information. This right of access is provided by law [12].

There are also cases where medical information is required by health protection staff (Physicians, nurses, laboratory technicians) in order to protect the public. Clinical audit and quality assurance systems are important to provide good care and requires reliable patient data. Unlike in the clinical care, research works need the disclosure of medical records to the wider scientific community and the general public. In order to protect privacy of individuals, researchers must obtain consent from patients (research subjects) before using their medical information for research purpose. It is also true that the role of physicians and researchers with respect to the relationship they have with patients is different, even if the physician and researcher belong to the same person [13]. When medical information is used for clinical and/or educational purposes it may not be anonymised appropriately or impossible to be anonymised, so that patients should be aware of their medical information disclosure. If there is any objection of the disclosure, it must be respected. Physicians may also be requested by lawyers (legal representatives) or insurances for medical reports of a patient treated professionally. However the reports should not be prepared or given without the patient permission. Any kind of

recordings (Audio, visual or photographic) of a patient or any of his/her relatives should not be disclosed without their consent or should be kept secretly as part of their record [14].

Patient medical records should remain confidential even after death. If there is no clear consent made by the dead person about his/her information disclosure, they should consider how the disclosure might benefit or cause distress to the deceased's family or other patients. Individual decisions in this case might be limited by law [15]. Physicians should ensure that patient privacy is maintained at all times and compliance with data protection legislation. Even if the patient does not consent to disclose, the physician should respect except where failure to disclose would put others at risk of death or serious harm. Medical information disclosure may be mandated by law in certain limited circumstances such as: when there is an order by a judge in a court of law and when required by infectious disease regulations [14].

1.9 Organization of the Thesis

Including this Chapter the document has a total of Six Chapters, which are organized as follows: Chapter 2 discusses literature review on different issues of information security and privacy concern, free and open source software in health information system. In Chapter 3 review of related work is presented. It discusses some of the works conducted relevant to this work which have contributed concepts that are used as a basis for this work. Chapter 4 presents the detail architecture of the system. Chapter 5 deals with Implementation and experimentation in order to show the result of the developed system and the last chapter which is Chapter 6 presents a general conclusion, thesis contributions and possible future works.

Chapter 2

Literature Review

This chapter focuses on information security and privacy of patient information in Electronic Medical Records (EMR) used by healthcare providers. Initially, brief explanation of information security and privacy is done. Then the review proceeds on how to maintain the information security of EMR in healthcare organizations.

2.1 Security and Privacy Issues in Healthcare

Privacy and security in the healthcare system today must balance two competing social benefits. The first one is the need to appropriately access, share information to enhance care quality, safety and provide continuity of care, and the second one is the need to implement reasonable safeguards to maintain the privacy of personal health information. Balancing these two needs presents a challenge [16].

Despite their benefit, HIS can present problems that prevent their universal use in hospitals. The initial high cost of acquisition of the basic infrastructure of Health Information System (HIS) is an example. Privacy and Security are still big concerns in the healthcare industry and there is also concern about the privacy of patient data on computer systems and how to keep such information secure [16, 17]. Medical practitioners are generally slow adapters to Information technology [16, 17].

2.1.1 Security Concern of Health Information System

The emergence of Internet technologies has transformed the business model for customer oriented industries such as retail and financial services. The healthcare sector is also experiencing a tectonic shift in enablement of healthcare services through Internet and mobile technologies such as remote health monitoring, online consultation, e-prescription, e-clinical trials, patient information access and asset tracking among others [18]. Recent advances in web technology have enabled new approaches to patient information management such as Banking on Health or Health Bank [19]. The notion of a health bank, first conceptualized in [19], is a platform for storage and exchange of patient health records patterned after a personal banking

system where consumers could deposit and withdraw information. Recent launches of Microsoft Health Vault and Google Health are examples of such health banking systems.

However, HIS faces security threats ranging from intentional/unintentional disclosure or manipulation of information through insiders or outsiders over user errors, maintenance errors, software failures, or hardware failures to environmental threats [20, 21]. The following examples illustrate potential damage of HIS use:

HIS can have access to information with low sensitivity like user's height, weight, or common past illnesses and treatments like a cough or broken bones [22, 23]. On the other hand, HIS can have access to information with high sensitivity like abortions, mental illness, sexually transmitted diseases, HIV status, substance abuse, or genetic predispositions to disease [22, 23, 24]. Disclose of such information can cause potential damage to users through socio economic repercussions [25], embarrassment or damage of reputation, social stigma [26], loss of affection or respect of family members, monetary repercussions through fraud or medical identity theft, more expensive insurance coverage or problems to obtain insurance coverage Secure Provision of Patient Centered Health IT Services [22, 23, 26].

Furthermore, information manipulation can cause harm to users because erroneous information might be added to their information due to medical fraud, medical identity theft or other threats [24, 25]. Consequentially, treatment might be based on erroneous information, which could impact patients quality of care, cause harm to health or death, or might impede later efforts to obtain medical, life, or disability insurance [23, 25, 26, 27]. Similarly, loss of information can lead to situations where important information required for patients care is no longer available [22, 26, 28].

Information accessible by health HIS can also be of valuable to third parties, which makes infringements of information security or privacy more likely because infringements are more rewarding to third parties. Information like insurance policy, government identity numbers, date of birth, or social security numbers is for instance valuable to third parties if it can be used for medical identity theft (obtainment of medical services with a faked medical identity) or medical fraud (billing for treatments never rendered) [24,27].

Nowadays, a growing body of research is focused on developing mechanisms to address these privacy and security concerns related to healthcare applications. Some of them are described in [29, 30, 31, 32, 33].

2.1.2 Privacy Concern of Health Information System

The term "privacy" bears many meanings depending on the context of use. Common meanings include being able to control the release of information about oneself to others and being free from intrusion or disturbance in one personal life. To receive healthcare one must reveal information that is very personal and often sensitive. We control the privacy of our healthcare information by what we reveal to our physicians and others in the healthcare delivery system. Once we share personal information with our caregivers, it is very difficult to have a full control over our privacy. In this sense, the concept "privacy" overlaps with "confidentiality" or the requirement to protect information received from patients from unauthorized access and disclosure [34].

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 of past research on healthcare confidentiality, four overarching conclusions were made [34]. First, patients strongly believe that their information should be shared only with people involved in their care. Second, patients do identify the need of information sharing among physicians, though HIV patients are less okay 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. Lastly, 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. This extensive body of research has primarily focused on the use of identifiable or potentially identifiable information by others outside of immediate health providers, such as employers, families and third parties. However, very limited research has examined patient's perceptions of sharing anonymised health records (perhaps with the exception of more recent studies that examine patient perceptions about permission for data use) [35, 36].

A research by Bansal et al. [35] developed a set of constructs based on utility theory and prospect theory as antecedents of trust formation and privacy concern that impact user personal disposition to disclose their health information to online health websites. In particular, they reported that user current health status, personality traits, culture, and prior experience with websites and online privacy invasions play a major role in users trust in the health website and their degree of privacy concerns. On the other hand, in a mail based survey with adult patients in England, Campbell et al. [36] found that about 28–35% of patients are neutral to their health information such as age, gender, ethnicity, reason for treatment, medical history, personal habits impacting health, type of treatment obtained, side effects of treatment being used by physicians for other purpose. Only about 5–21% of patients, however, expected to be asked for permission to use their information by their physicians. Similarly, only about 10% of the patients expected to be asked for permission if their doctors used their health information for a wide variety of purposes, including combining data with other patient data to provide better information to future patients, sharing treatment outcomes with other physicians, teaching medical professionals and writing research articles about diseases and treatments [36].

Another study by Angst et al. [37], 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 Patient Health Record (PHR). The study found that patient relative perception of privacy and security concern increased with the level of technology. 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.

2.2 Security and Privacy Related Problems of HIS

Many hospitals are moving away from paper based medical records to use electronic healthcare records. Specialized software and electronic diagnostic tools are offering a new level of patient care. The move towards electronic based systems provides streamlined automated processes and specific applications that can help doctors with diagnosis and treatment of patients. The introduction of these technologies raises privacy risks with regards to patient information. A malicious person trying to compromise many patient records will be able to collect large amounts of data easily if these records are available electronically [38].

Here are some common technical security vulnerabilities that affect most healthcare related businesses:

- ✓ Weak or nonexistent security and privacy policies and plans
- ✓ Lack of ongoing security and privacy and compliance assessments
- ✓ Lack of back up encryption mechanism
- ✓ Weak operating system, application and database passwords
- ✓ Lack of content filtering and audit logging
- ✓ Insufficient malware controls for viruses, Trojans, spyware and root kits
- ✓ Disclosure of personal health information
- ✓ Lack of responsibility and accountability

Many different solutions have been developed over the years but the questions still remain as to whether the data in HIS are secure enough. The National E-health transition authority (NEHTA) is the Australian authority dedicated to developing better ways of electronically collecting and securely exchanging health information. In their newest venture, the development of the personally controlled electronic health record (PCEHR) system, they have identified that privacy and security are major issues that need to be addressed properly in order for the proposed model to be well received [39].

Access control is one of the main safeguards against improper data access which ultimately controls who has access to patient information and how they are allowed to handle that information should be centralized to work in large, distributed environments such as modern healthcare organizations. Without it, authorization and authentication for each application and resource is fragmented, likely to produce security gaps and burdensome to IT personnel and end users. Historically, applications have been designed to scale to Internet requirements and provide role based functional access. Today, however, regulations and privacy laws require limited access to application data, even by the database administrator and especially from ad-hoc tools that can be used to bypass the application. Furthermore, determining, implementing and enforcing appropriate and effective access control program for access to patient record and other sensitive information can become highly problematic under these conditions [40].

Despite the access control, secure data storage and secure data transmission are essential to ensure data confidentiality, privacy and integrity. Encryption is one of many techniques used to protect data from unauthorized use, whether it is on disk the database and applications, in development environments, in transmission or on backup media [41].

Database encryption encrypts data as it is written to (and decrypts data as it is read from) a database. By doing so, database encryption protects data while it is in use by the database system, as well as while it is in storage. Database encryption protects the data both within the database management system and also within the storage media. However, currently database encryption technology is less commonly used in healthcare to protect patient information (in large measure because of the cost of the software and the high performance hardware needed to support it) [41].

Another is lack of secure audit service to record significant privacy and security related events in an event log. Audit trails can serve a useful role in recreating a security incident and determining the extent of a security breach. This will in turn allow the covered entity to respond and report appropriately. For example, good audit trails can help identify the number of individual records affected by a breach. This accurate data can affect the number of individuals who must be notified and affect the impact of civil penalties. When a covered entity does not have good audit trails, the entity is at greater risk of having to notify all individuals because the entity does not know how many records were accessed or leaked during a breach [42].

Generally, all of these vulnerabilities could put sensitive healthcare records in harm.

2.3 Open Source Software in Health Information System

Open source technology is the philosophy of developing and improving software through open and public forums by sharing the source code [43]. Today, open source community in healthcare is more energized and has more of a track record on which to build. Health industry leaders are showing renewed interest in open source solutions. Among the highly visible projects gaining momentum nationally and internationally are Open Vista, a patient information system in the United Sates , Care2X, an integrated practice management solution in Europe and Health info way, a patient data exchange venture in Canada [43].

The potential advantages of open source software in healthcare are many. Anyone can use or modify the software with few restrictions, the cost for customers is minimal because developers generally volunteer their time, and revenues derive from services such as implementation and support rather than licensing, which means healthcare providers are more likely to gain direct value. In addition, the fact that no single vendor owns the software gives providers more options, enables them to customize software for their own particular needs, promotes public and foundation funding of software development and ensures correct and timely implementation of standards, as there are no proprietary limitations. The creation of technology standards that define how information is structured, defined and exchanged is critical because successful healthcare exchange will depend on them [44].

By facilitating the adoption of standard electronic medical record, open source software may contribute to the creation of regional health information networks, which exchange data and patient records. Access to source code will allow each region to adapt the software to its specific requirement without having to develop an entire software suite from scratch and open source software is increasingly likely to become the dominant model for creating software to improve the quality of care in a cost effective way [44].

According to the findings, open source EMR systems have been wildly welcomed by source limited regions around the world, especially in Sub Saharan Africa and South America. Argentina, Australia, Chile, Ecuador, Ethiopia, Germany, Ghana, Haiti, Jordan, Kenya, Lesotho, Malawi, Malaysia, Mali, Mexico, Mozambique, Netherlands, Nigeria, Pakistan, Peru, Rwanda, Senegal, Sierra Leone, South Africa, Sweden, Tanzania, Thailand, Turkey, Uganda, USA and Zimbabwe are among countries, which used open source EMR to enhance the healthcare quality. The results indicated that many countries especially developing countries demand to use an interoperable and cost efficient EMR system, which is flexible enough to modify and improve [45].

Ethiopia is a hugely populated country in Africa. The majority of hospitals and clinics still maintain patient diagnosis and treatment records manually. Some of the private and few of public sector hospitals have implemented electronic medical records and hospital computerization which is helpful to handle many patients within short time. Black Lion Hospital is one of the biggest referral hospitals in Ethiopia. According to IT staff we interviewed from

Black Lion hospital, the hospital uses different open source such as HMIS and J2. But these software don't address the above security and privacy related problems. In addition to that different departments use different open sources separately.

Open source systems make opportunities for advanced innovation in the health information sector of low income countries. However, cost efficiency seems to be the most important reason for utilization of open source systems in many countries [46]. Despite the enormous financial investment to Ethiopia HIS, we believe that the reduction in duplicated efforts will reduce the total expenses of an Ethiopian HIS.

Generally, the adoption of health information systems is seen world wide as one method to mitigate the widening healthcare demand and supply gap. But they still have security and privacy problems.

Implementing security and privacy plans and technologies to protect electronic medical records system is a paramount health data security problem today. This implication is backed up by the report of the editorial staff of information security media group, with the assistance of members of the healthcare information security board of advisers, which includes leading healthcare information security and IT experts in 2013 entailed "Healthcare information security today". The conclusion of the report is summarized as follows in Figure 2.1:

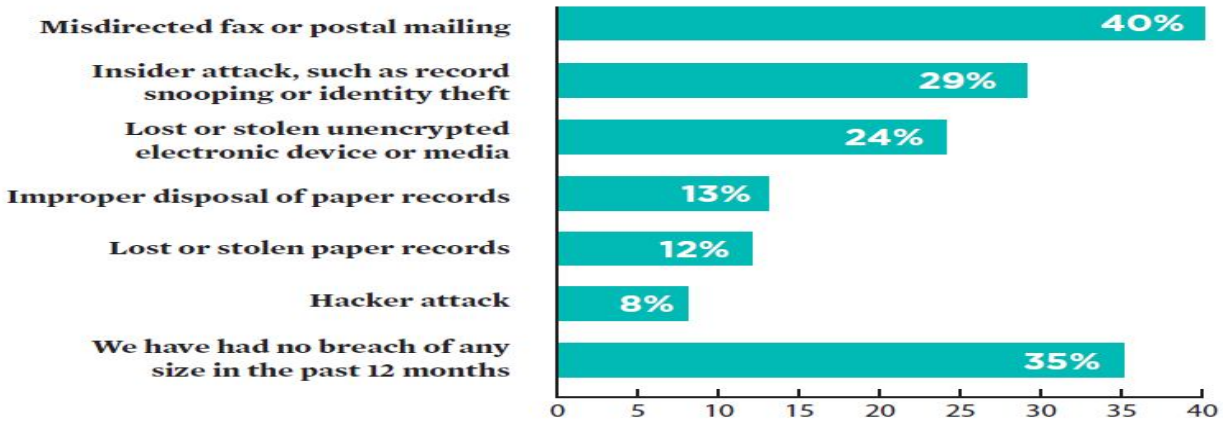


Figure 2.1: Type of health information breach in 2013[47]

Summary

We believe that the use of open source solutions benefits individual healthcare providers and large organizations by offering lower cost solutions, resulting in increased deployment and use of health information systems. The overall result of the increasing use of enhanced systems will improve patient safety and quality of care. The open source path seems to lead to greater standardization and better security more rapidly and comprehensively than going down the proprietary path. Finally, the growing complexity of questions of health and disease now requires an unprecedented growth of collaborative research efforts. The open source approach has demonstrated its potential many times over, as the work environment and programming culture best suited for large scale, ongoing distributed collaborations.

Nevertheless, there are some challenges or concerns regarding open source solutions that must be addressed. An organization should be established to ensure adequate software testing is conducted and to assure users of the quality of the software before widespread acceptance and use of a particular product should be encouraged.

Chapter 3

Related Work

Privacy and security of patient health information is crucial to developing systems and structures that support the exchange of information among healthcare providers, payers, and consumers using Health Information Exchanges (HIE) and to assure confidentiality and trust of the physician patient relationship. If patients do not have the confidence that their privacy will be maintained, or that reasonable security safeguards will be in place to protect their information, they may do things to protect their privacy on their own (such as refrain from disclosing critical information, refuse to provide consent to use personal health information for research purposes, or not seek treatment). This can have direct effect in assuring treatment of dangerous illnesses like AIDS, TB and Hepatitis that require early treatment which depends on the initiative and openness of patients. Thus to bring solution for such problem, starting with security architecture is important. The security architecture design process will be able in conducting the exchange of health information in general, as well as when initiating and establishing health information exchange (HIE) [48].

3.1 Identity Based Authentication System (IBA)

The author proposed secure communication services, an identity based authenticated broadcast encryption system [49]. This scheme allows each sender to dynamically broadcast messages to its group members using a polynomial function constructed with secret keys of the members. However, it does not provide the mechanism of verifying the signature or integrity of the message. Later on, Byun etal. [50] propose purpose based access control (PBAC). PBAC is based on the notion of relating data objects with purposes [51]. These purposes can determine for what reason data is collected and what they can be used for. Much research has been done in this area and most have identified that greater privacy preservation is possible by assigning objects with purposes [50, 51]. However, according to Al-Fedaghi [52], purpose management introduces a great deal of complexity at the access control level.

3.2 Cryptographically Enforced Access Control Scheme

Some HIS suggest use of cryptographically enforced access control scheme. This type of system usually allows patients to encrypt their PHR data and distribute corresponding decryption key to

authorized user. A typical example of cryptography based system is iHealthEMR [53]. It implements a self protecting electronic medical records (EMRs) using attribute based encryption. In that system, patient can encrypt each node in the XML based EMR file with an automatic generated access policy before exporting it to cloud system. PHR users' access rights are defined by the attributes within their private key. However, it does not solve practical problems such as key revocation and key delegation. Nevertheless, the actual implementation is limited since the encrypted XML file contains malformed metadata and, therefore, cannot be accepted by the third party.

3.3 Role Based Access Control (RBAC)

Several models have been proposed to address the access control requirements of distributed applications. Role based access control (RBAC) [55] has rapidly emerged in the 1990s as a technology for managing and enforcing security in large scale systems [54]. Most security researches in healthcare systems [56, 57, 58] have been based on role based access control (RBAC). In fact, RBAC is the most common access control model, and is considered to be particularly well-suited to healthcare systems. An access control system designed to operate in the healthcare scenario should be flexible and extensible. The basic opinion of RBAC is that the permissions are organizationally associated with roles, and users are administratively assigned to appropriate roles. RBAC ensures that only authorized users are given access to certain data or resources [55]. This simplifies the management of authorization while providing an opportunity for flexibility in specifying and enforcing enterprise-specific protection policies [56]. In RBAC, a role is a function within the context of an organization with an associated semantics regarding its authority and responsibility [55]. User is defined as a human being, a machine, a process, or an intelligent autonomous agent, etc [55]. Permission is an access mode that can be exercised on objects in the system. Both objects and access modes are domain dependent [55]. System administrators can create roles, grant permissions to those roles, and then assign users to the roles on the basis of their specific job responsibilities and policy. Hence, role permission relationships can be predefined, making it easy to assign users to the predefined roles [54]. RBAC really helps to determine efficiently which permissions are authorized for what users in a large enterprise system.

Figure 3.1 shows the mapping relationships among users (A, B, C, D, E, etc), roles (R1, R2, R3, R4, R5, etc.), and permissions (P1, P2, P3, P4, P5, etc) in an RBAC model. Every user has one or more roles. Every role can be assigned to one or many users. They are one-to-one, one-to-many, or many-to-one relationship. Every role has one or many permissions, and permission can be assigned to one or many roles according to the policy. Here the author chooses the tables (T1, T2, T3, T4, T5, etc) of the database as the particular data or resources for access. Permission gives the right to do an action (such as read or write) on a table in a database.

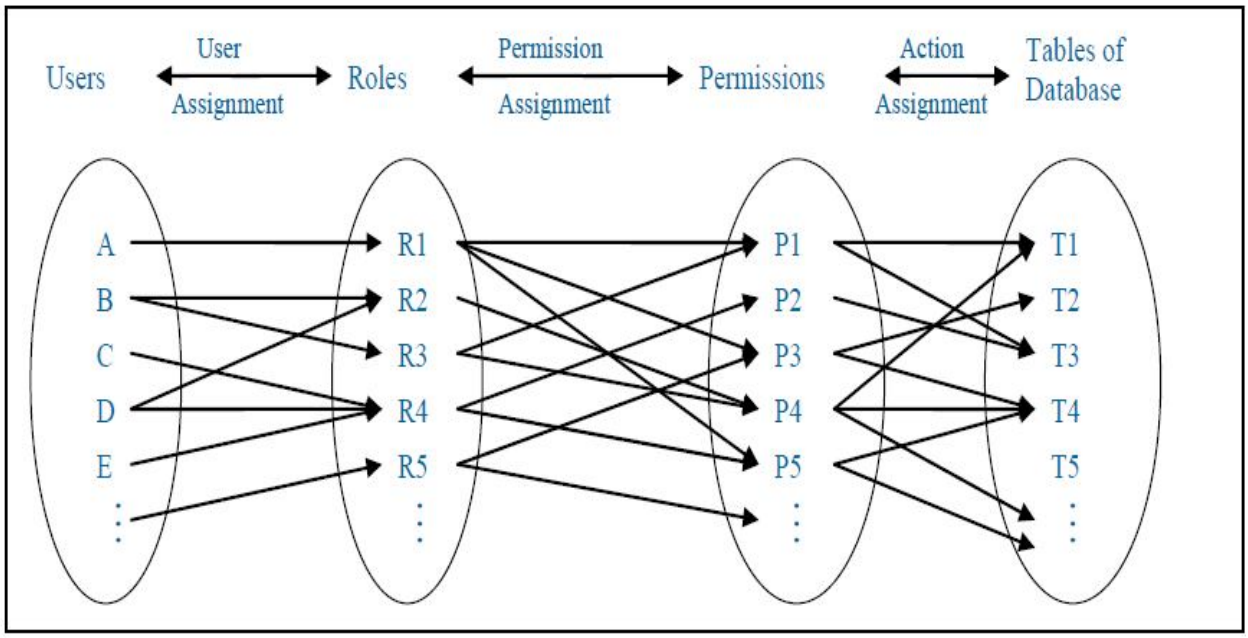


Figure 3. 1: Mapping relationships among users in RBAC[56]

However, RBAC has several weaknesses. Firstly, the nature of role is static, so RBAC lacks flexibility and responsiveness to the environment in which they are used. Secondly, RBAC does not encompass the overall context associated with any collaborative activity [57]. So, it is a passive security system that serves the function of maintaining permission assignments. Thirdly, RBAC lacks the ability to specify a fine grained control on individual users in certain roles and on individual object instances [59]. So, it is not enough for collaborative environments.

3.4 Open and Trusted Health Information Systems (OTHIS)

The goal of OTHIS is to address privacy and security requirements at each level within a modern HIS architecture to ensure the protection of data from both internal and external threats. OTHIS

also has the capability of providing conformance of any HIS to appropriate regulatory and legal requirements. Its primary emphasis was on the Australian health sector [60].

OTHIS describe appropriate data security management which involves the protection of data in storage, during processing, and during transmission. The proposed HIS structure consists of three distinct modules: Health Informatics Access Control (HIAC), Health Informatics Application Security (HIAS), and Health Informatics Network Security (HINS).

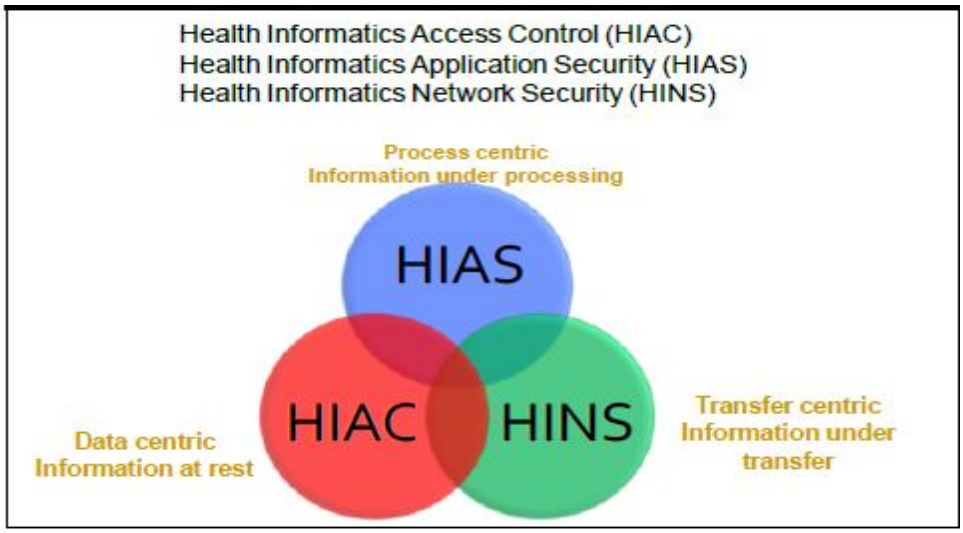


Figure 3. 2: Modularized Structure of OTHIS [60]

However, they don't consider ensuring that a patient's health information is adequately protected, the "non-exchange" portions of the data usage, including collection and storage. They use Discretionary Access Control. But this model is no longer valid for modern HIS.

Organizations also need to consider the security of backups of stored information and it require development of other modules within the proposed OTHIS structure with the ultimate goals of maximum sustainability, flexibility, performance, manageability, ease-of-use and understanding scalability in the healthcare environment. In addition to that the OTHIS/HINS project is currently under development.

3.5 Agent Based Security Architecture

Current health information system in [61] described a security architecture that can support web based distributed systems, focusing on authentication and authorization issues in a multiple security policies environment (interconnection of different security domains). The focus of the

work was on designing and developing the security agent and the SSP web services, as well as on the definition and implementation of a formal policy representation language.

However, this security is architecture mainly designed for providing authentication and authorization services in web based distributed systems and it doesn't focus on privacy issue. The architecture has been based on a role-based access scheme and on the implementation of an intelligent security agent per site (i.e. healthcare unit). This intelligent security agent:

A. Authenticates the users, local or remote, that can access the local resources

B. Assigns, through temporary certificates, access privileges to the authenticated users in accordance to their role; and

C. Communicates to other sites (through the respective security agents) information about the local users that may need to access information stored in other sites, as well as about local resources that can be accessed remotely.

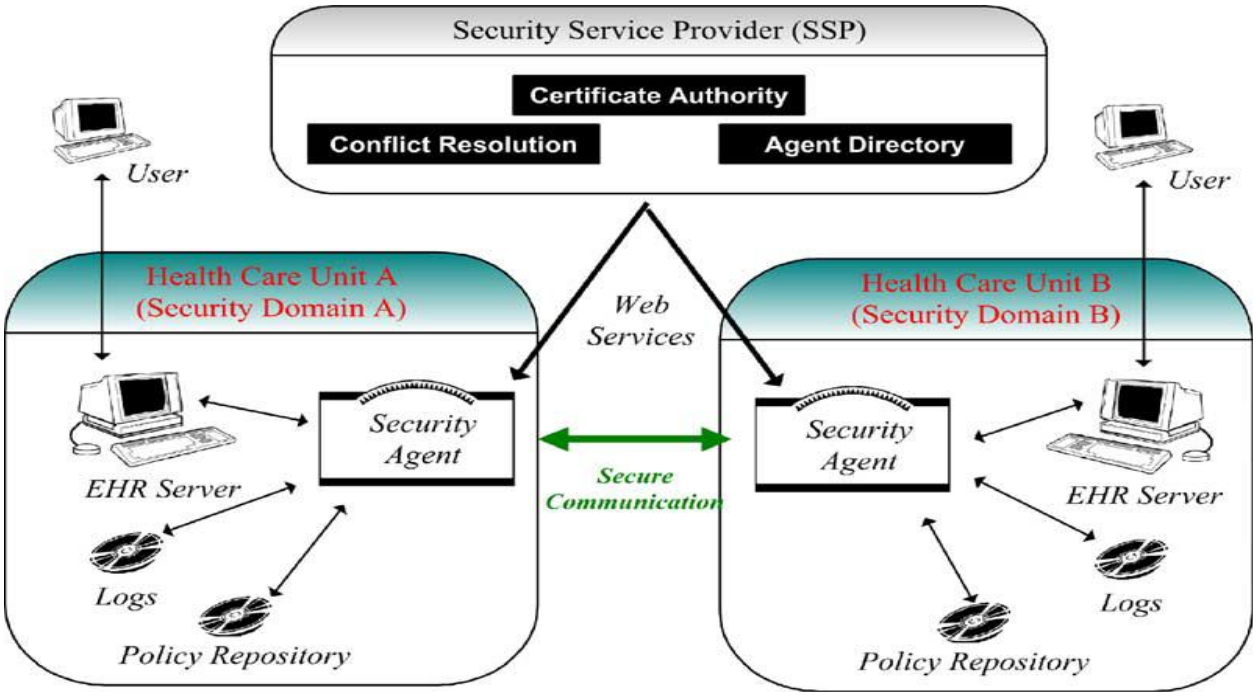


Figure 3. 3: Security architecture for HIS [62]

3.6 Privacy Issues in Healthcare System

The focus of this thesis work [62] is on managing personal privacy of patient in Ethiopia black lion hospital, Ethiopia. The system deals with active monitoring of the human immune system in

both HIV patients and individuals who are regarded as at risk. The author described that the existing system of patient medical information management in black lion hospital is manual and is prone to security and privacy threat.

The author used various privacy protecting techniques during communication and sharing of medical information among the physicians, patients and other stakeholders. Techniques used to protect personal privacy of patients are obscuring information flow, user access rights management, user access policy management, granularity awareness, constraints and permissions, data persistence control and classification of resources. The information flow should be obscured by encryption techniques. The end users of medical information should access patients' information based on the access rights given by the owners of the information. The system grants or denies access rights to the medical information end users according to the policy set by the owners of medical information. Patients' information is grained down in order make to the anonymity set by the patients be according to the level of their need [63].

However, the system is mainly applicable to HIV patients, doesn't focus on the security issue and the work is developed for pervasive environment.

3.7 OpenMRS in Central Africa

This work presents a study conducted to improve healthcare in central Africa by customizing OpenMRS [63]. The focus of the work is to define, develop and implement health enterprise architecture for Rwanda. We use the work as starting point for most part of our investigation and try to enhance the drawback of their work and continue with their future works.

Open Medical Record System (OpenMRS) was formed in 2004 as a open source medical record system framework for developing countries. To date, OpenMRS has been implemented in several African countries, including South Africa, Kenya, Rwanda, Lesotho, Zimbabwe, Mozambique, Uganda, and Tanzania. OpenMRS is supported in part by organizations such as the World Health Organization (WHO), the Centers for Disease Control (CDC) [64].

Open Medical Record System (OpenMRS) is a collaborative open source project to develop software to support the delivery of healthcare in developing countries [65]. It is a common platform in developing countries. The system is based on a conceptual database structure which

is not dependent on the actual types of medical information required to be collected or on particular data collection forms and so can be customized for different uses. OpenMRS is based on the principle that information should be stored in a way which makes it easy to summarize and analyze, i.e., minimal use of free text and maximum use of coded information [66].

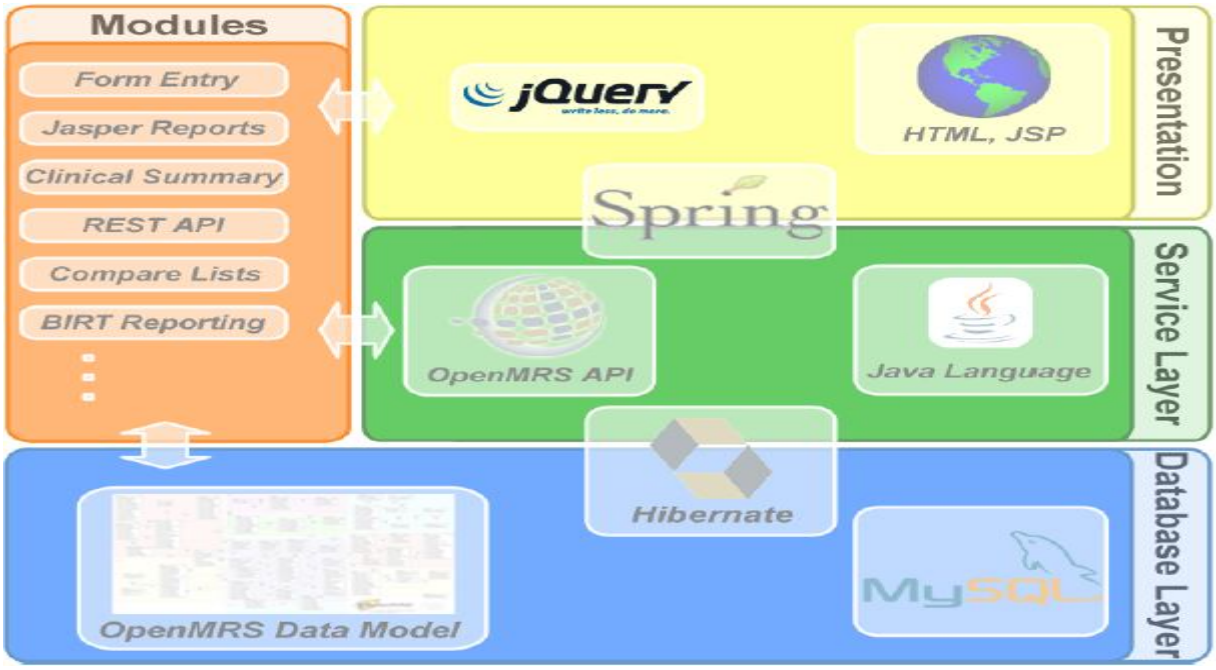


Figure 3.4: Architectural components of the OpenMRS[http://go.openmrs.org]

However, OpenMRS cannot address some critical security and privacy issues like access control, encryption and emergency situation.

Access Control: Role Base Access Control is implemented in OpenMRS. The limitation of RBAC is that it is impossible to configure a policy that permits access to a specific object. It only supports course grained access policy which restricts access at the level of classes rather than objects. For example if the roles of Doctor and patient are introduced with the privileges that the Doctor role is allowed to both view and modify patient records and the patient role is allowed only to view a medical record. With the RBAC, Doctors are allowed to view and modify any patient's record rather than only their own patients. Similarly, implementation of RBAC allows patients to access any other patient's record. It shows that RBAC model is not fine grained enough to fulfill the requirement of access control. That means what OpenMRS cannot do is "User X can only view/edit Patient Y".

Encryption: Disk/database encryption of the data are actually left as exercises for the user. But securing the database from illegal access, theft and forging becomes a big challenge for different organizations. In addition to that Backup data exposure is an important threat that needs to be taken care of. Since backups on tapes, DVD or any external media are exposed to high risks. They need to be protected from attack such as theft or destruction.

Emergency Situation: is not considered but based on the interview from black lion hospital security in emergency case becomes a big issue in the hospital. for Example, if the user like a nurse, who is not authorized to view a critical data, needs to view a critical field during emergency then how does OpenMRS handle the situation is not under consideration. Which means there is no way the nurse can access the patient's critical information at that time.

Summary

Based on the research works reviewed we have summarized all health services need to benefit from the rapid development in digital electronics to improve their performance through implementation of electronic information systems in order to meet their patient needs, satisfaction and in order to meet the expectations of the health authority by providing high quality services at an acceptable cost. A lot of research works have been done which can be applied to healthcare to increase privacy and security of patient information. But, the related work we review shows security and privacy of information in healthcare system remains one of the major issues. Based on this observation, we select OpenMRS to enhance information security and privacy in health information system. OpenMRS is one of these open sources which represents a collaborative effort to develop an open source EMR for developing countries in the fight against HIV/AIDS, multi-drug resistant tuberculosis, malaria, and related health crises.

One of the main challenges and problems in health services is protecting information and many security issues are related to the use of patient information or record. Another privacy aspect is not only protecting the data from unauthorized access but also from unauthorized modification. Ensuring proper access control is essential. Most healthcare security architectures regulate authorization through role based access control or role based security. But this security model brings challenges to use the patient record accurately and securely. In addition to that encryption is needed to ensure the security of the data and help prevent eavesdropping and skimming. Thus,

without proper authentication and encryption unauthorized personnel can without any difficulty take patient data.

Other problem identified in the related work is the lack of developing a secure and scalable architecture for accurate information exchange is not easy task due to the complexities within the healthcare environment. This problem complicates the process for developing and establishing appropriate patient information security policy, access control, encryption methods and auditing. Information security in Black Lion hospital is relatively new and is progressing slowly. The hospital lacks a clear information security policy for patient information.

Generally, healthcare information system in Ethiopian is mainly in paper form. There is no coordination and information and communication technologies are rarely implemented and current interest and investment in PHRs are usually motivated by goals of efficiency, increasing patient empowerment, or improving disease management. However, patient's greatest concern about PHR, as well as other healthcare system, is security and privacy. This thesis addresses the above issues by implementing a secure HIS.

Chapter 4

The Proposed Security and Privacy Enhanced MRS

In this Chapter, we have discussed the empirical work for our thesis that explains what we propose as a solution and how we arrive at the solution. We have conducted several interviews with different healthcare personnel, who are working in Black Lion and Korean hospitals. Before conducting the interview, we have planned to choose the appropriate personnel who have relevant experience and expertise about the management of information security of electronic health records or patient information.

4.1 Consider the Environment

To carry out this research work and to answer the research question presented in Chapter One, review of necessary literature and existing similar system in different hospitals which are stated in Chapter 2 and 3 is done. Depending on the gathered data from literature review a plan to carry out the research was set. Accordingly, the next step for this research is data collection. In this phase we studied existing healthcare system in Ethiopia, and various articles from different journals and conference papers.

Attitude and perception of employees towards security has been discovered through the results of questionnaire. Appendix A shows the questionnaire prepared to solicit the status and requirements of security in hospitals. The questionnaire served also to trigger detail interview conducted.

4.1.1 Discussion of the Questionnaire and Interview

We began interviews by talking about the research in general, and we started the interviews with a background check we wished to know what the interviewee's position in healthcare was as well as more specifically what they work with. Furthermore, we wanted to find out how the process of employment was carried out when the interviewees were employed as well as how patients are identified in the organization. We then moved on to different questions for different job types. During the interviews with doctors we focused on education in information security, transferring information between healthcare units and log keeping. When interviewing IT personnel, we assumed that we did not need to ask about computer experience, instead asking

about management of user registrations, authorization tools, and then log keeping. Finally, when interviewing the directors and nurses we asked about policies in the organization positive aspects and negative aspects regarding the work with information and patient security today and what requirements will be needed in the near future. All interviews were concluded by asking the interviewees where the main focal point should be in the near future, concerning patient security, privacy and safety. After all questions were asked, we asked if the participants wished to remain anonymous in our report, but all participants turned down that offer, claiming that they had not said anything that could harm anyone.

The first interview was carried out with the hospital IT department personnel in order to explore the use of patient record within the hospital and the hospital IT strategy. The IT personnel indicated clearly that they have introduced electronic patient record system. The hospital uses HMIS open source in card room. The interviewed IT personnel stressed that the system is installed and used only in the card room staff as part of the hospital strategy to improve hospital performance and the care system within the hospital. Two of the IT personnel stated in this regard:

> *"Yes, the hospital introduced electronic system to improve the hospital performance and saving time and effort. We currently store and process patient records electronically. But it is in card room. and we need to extend The record start from the time patient enters the hospital till he/she leaves the hospital."*
>
> *(IT Staff from Black lion hospital)*
>
> *"The patient electronic records are still in the process of development. There are several items need to be added to the electronic record such as the clinical testing. The hospital is still using paper based recording system"*
>
> *(IT Staff from Black lion hospital)*

One of the main focuses of this research is EMR access control policy. Access control policy issues were explored in all of the interviews and discussed in some detail. The main aim was to identify Who, What and How to access EMR. The interviews indicated that the EMR access differs from one staff member to another depending on his or her role and responsibility. The interviews indicated that the information department staff of the hospital has no restriction in accessing EMR. The main explanation provided for accessing EMR was ICT staff role and responsibility. One of the ICT administrators stated:

"I have the right to access patient records; in fact there is no restriction on my team on the access rights".

(IT administrator from Korean hospital)

The ICT administrator also indicated and agreed that there is no need for them to access EMR. They expressed that there is no need for such access. EMR is not related to their job role and responsibilities.

The hospital physicians also have no restriction in accessing the EMR. It was clear all the physicians are given permission to access patient record. It is part of the physician responsibilities as one of the physicians stated:

"I have no restriction in accessing patient record. In fact I am using the access to EMR as part of my job responsibilities in the hospital. I believe and understand that all the hospital physicians have access to the patient record"

(Physician from Korean hospital).

On the other hand, medical staff such as most of the hospital nurses has no full access to the EMR. The nurse interviewees' respondents have explained that. They stated that most of their work is carried out manually using the traditional paper based recording forms. The nurses believed that the main reasons behind this denial of full access to most of the nurses are lack of clear policy and the technical skill to design the access control. Some nurses stated:

"*I have right to access EMR but not in full. The hospital is still using paper based recording system"*

(Nurse from Black lion hospital)

"*Nurse needs to access patent personal details to ensure she is dealing with the right patient and not mixing up with other patient, patient allergies and current diagnosis as examples"*

(Nurse from Black lion hospital)

The medical staff can be classified into two main groups for accessing EMR. The first group is the physicians, medical consultants who have open access to EMR. On the other hand, most of the nurses and the patients of the hospital were denied full or partial access to patient record.

Information security policy was explored in the interviews, aiming to establish whether the hospital has a clear policy and to identify any gap in the policy. The interviewees believed that the hospital has an information security policy but there is no well documented policy. They

stressed that all the hospital staff are not given a copy of the hospital security policy. However, the physician stressed the need to improve and update the current policy due to changes in patients' rights and to avoid any unauthorized access to the patient record. One of the physicians stated:

> *"The hospital has certain rules and procedures for security policy. but I don't have the document*
>
> *(Physician from Black lion hospital).*
>
> *"Medical record department is addressing any security issues and deal with it accordingly. However, handling patient records manually can be source of privacy concern to patients especially in emergency room medical records can be destroyed and privacy concern of patient is a critical issue. In addition to that there is no clear policy and or strategy on security policy"*
>
> *(Black lion hospital director/ leader)*

However, currently the hospital has a certain policy regarding patient information security. The hospital security policy document is not distributed to the medical staff.

> *"There is no clear statement regarding the patient record security. There is a need for clear policy regarding use of patient record"*
>
> *(Physician from Black lion hospital).*
>
> *"Medical record department is addressing any security issues and deal with it accordingly.*
>
> *However, there is no clear policy and or strategy on security policy"*
>
> *(Physician from Black lion hospital)*

Summary

Generally, according to the black lion and Korean hospitals the patient is the most important actor in healthcare. The aim of the hospitals is to deliver citizens with good health safety and secure information. Furthermore it must be based on respect for the patient self determination and privacy and promote good relationships between the patients and the healthcare actors.

Black lion hospital work for the future aims to involve EMR as a support for good and efficient information management within healthcare. One main aim of the hospital, as mentioned above is to achieve both patient security and patient privacy to provide the patient with the best care based on care decisions resulting from the right information at the right time. But based on what we

have learned from these ongoing conversations there are different security and privacy breach in the hospital. Some of them are:

- ✓ There is no well established privacy and security policies for employers who have access to PHI
- ✓ There is no well established and clear policies, procedures, guidelines, and approaches governing patient consent
- ✓ Inappropriate access of patient information by unauthorized users
- ✓ Disclosure of patient health information or otherwise used for other than a specified purpose without consent of the individual or legal authority.
- ✓ Some patients may refuse to reveal their information to their physicians
- ✓ There is no backup, to secure from fire, flood, or other events and save records or recover.
- ✓ Psychological distress, loss of trust in healthcare team and system, and reduce adherence to treatment and care
- ✓ Theft/ Stealing, loss, damage, unauthorized destruction of patient records

Table 4.1 shows hospital access rights for reading from and writing to the EMR based on the interview main outcomes. The table classified access to the EMR into three main access categories.

Table 4.1: User access right to patient record

Subject	Access	Type of Access
Hospital Manger	Open	R/W
Medical Doctors and Consultants	Open	R/W
Nurses	Partially	R/W -Partially
Pharmacists	Partially	R only
Administrator	Partially	Partially R/W

4.1.2 Data/ Information Flow

To better understand and find the main difficulty for the implementation of security and privacy architecture of health information technology, we have studied and analyzed the general healthcare data exchange scenario and how patient data flow with in a hospital. The hospital health information allows recording, storage, processing and access of data by various departments. Department that perform specific functions may use data entered by another department. Patients are required to share information with their physicians to facilitate correct diagnosis and determination of treatment, especially to avoid adverse drug interactions.

Patient health records could serve a range of purposes apart from diagnosis and treatment provision. For example, information could be used to improve efficiency within healthcare system, drive public policy development and administration at state and federal level, and in the conduct of research to advance medical science. Patient medical records are also shared with payer organizations such as insurance to justify payment of services rendered by physicians. Healthcare providers may use records to manage their operations, to assess service quality, and to identify quality improvement opportunities. Furthermore, providers may share health information through a regional health information organization to facilitate care services. Medical information of patients is also used for common good through federal and state government interventions regarding public health management, hospital accreditation, medical research, and for managing social and welfare systems.

The generalization can be represented graphically as shown in Figure 4.1 based on the data collected from relevant stakeholders in the Black lion and Korean hospitals using interview.

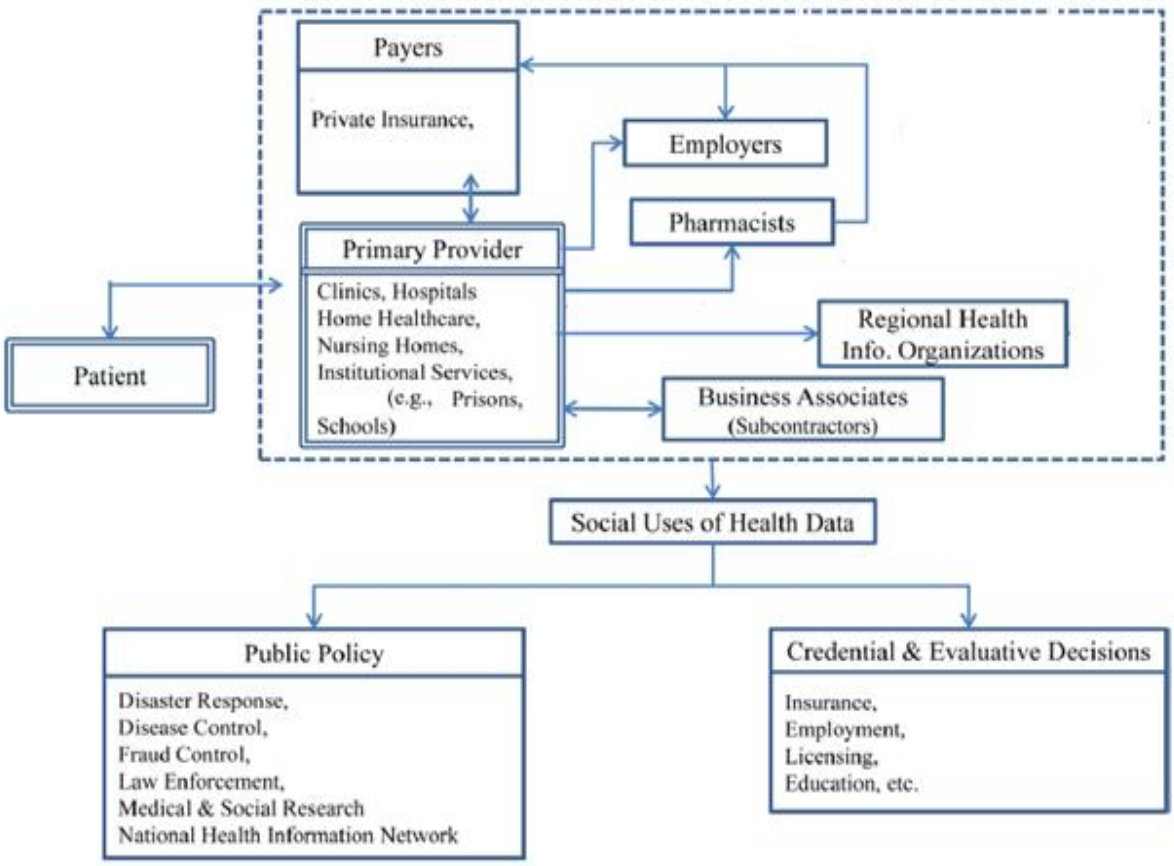


Figure 4.1: Graphical view of information flow in the existing healthcare system

4.2 System Architecture

After analyzing the current HIS and its information security structure, we proposed solutions that enhance the information security and privacy to sensitive information of a healthcare system. High level of patient security and privacy would be possible to obtain in electronic based healthcare system through systematic approach and component based modular architecture. The proposed architecture contains three main component namely system users, security and privacy control and health record. The entire list of system components for information security and privacy architecture is shown in Figure 4.2.

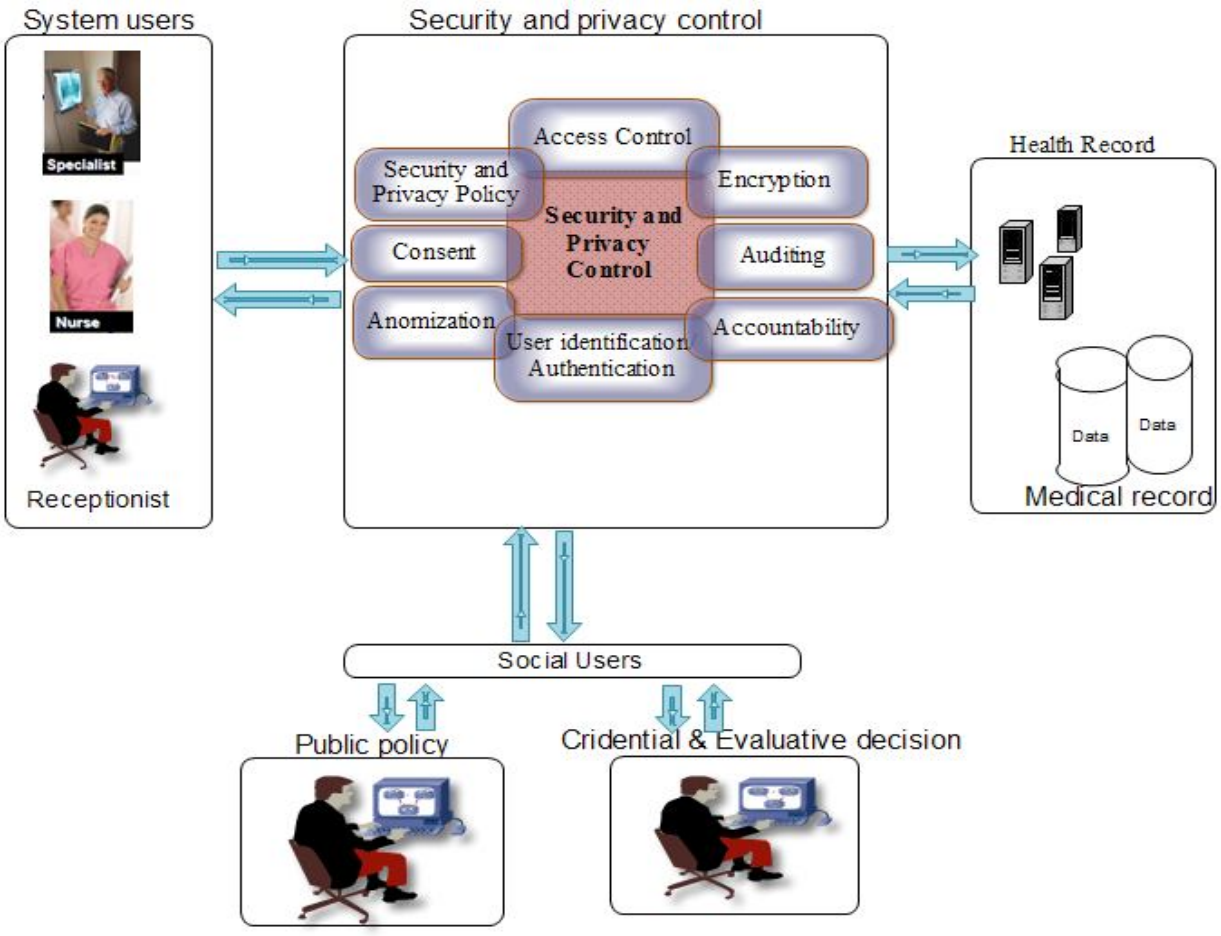


Figure 4.2: Security and privacy enhanced architecture for health information system

4.2.1 Users

Users contains two type of users which are system users and social users of health data in the hospital. System users are the main actors in handling, transferring, controlling and accessing the patient information. System users contain all healthcare workers such as doctors, nurses, pharmacists, receptionist and diagnostic laboratory technologists. All these users are required to sign a confidentiality agreement before they have access to any patient data. There are users outside the hospital like insurance company, medical and social research, employment, licensing, and drug company and law enforcement bodies. This category of user can be named social users.

4.2.2 Security and Privacy Control

This component describes several mechanisms used to protect the individuals and collective sensitive information from vulnerabilities. This section answers the question: **What are information security and privacy requirements of patient information?**

Access Control: defines rights, privileges, and mechanisms to protect information from access or loss [68]. It also includes identification of users during registration, their subsequent authentication during log in, and their authorization prior to being granted access to services and data. Access control is intended to prevent unauthorized access to information systems, ensure the protection of services, detect unauthorized activities and ensure information security. The essence of access control is in determining what access privileges a given user can exercise in a given context. Can a person look up a specific patient EMR? Can she/he view the entire record or just of portion of the record? Can he/she update the record? Can he/she enter or update consent on behalf of this patient? Can she/he search for records matching some search criteria she/he specifies? Can she/he place orders (e.g. for a lab test) through the EMR? Some of these questions have been answered for any user depending on the access control mechanisms we have used. We use TT-RBAC to answer the above questions and to ensure that no one may access confidential records unless specifically authorized to do so. Even authorized individuals may use confidential records only for authorized purposes.

Consent: Consent plays an important role in maintaining patient privacy. It is permission to use or disclosure PHI [69]. This ensures health that information is collected, accessed, used, or disclosed only with a patient's consent.

Anonymization: Privacy is one of the biggest concerns in sharing patient data because without appropriate protection, personal information is vulnerable to misuse. The goal is to make information accessible to secondary users of healthcare data (healthcare researchers) without breaching on patient privacy.

Encryption: The sensitivity of the data logically determines the need for the use of encryption. To maintain data confidentiality and integrity of patient information we implement encryption of EMR data within databases and plain stored data such as backup files using hybrid encryption algorithms: AES and RSA algorithm.

Accountability: It is essential that all providers be responsible and accountable for the care that they provide and for the well being of the patient. As clinical leader, the physician should be responsible for the clinical oversight of an individual patient care.

Secure Audit: Audit trail/audit log is a chronological sequence of audit records, each of which contains evidence directly pertaining to and resulting from the execution of a business process or system function [70]. This allows to record significant privacy and security related events in an event log. Audit logs will be reviewed frequently to allow detection of unauthorized events before a significant loss has occurred.

4.2.3 Health Record

Health record describes patient information which has been collected and exchanged during regular checkups by doctors, pharmacists, and other staffs in hospitals. Data stored, processed, and transmitted through a computer system must be protected. Data is often the most valuable asset possessed by an organization and it is the main target of intentional attacks. When data is processed properly, this should improve the security of the data and the application. Healthcare organizations and other participants in generating health data have to follow and adopt the best practice to ensure privacy and security of personal health information.

4.3 Detail on Security and Privacy Control

This sub-chapter describes information security and privacy control in detail. The security and privacy control architecture (Figure 4.3) is designed in such a way that it can be easily integrated in any existing infrastructure and its scalability characteristics being heavily taken into consideration.

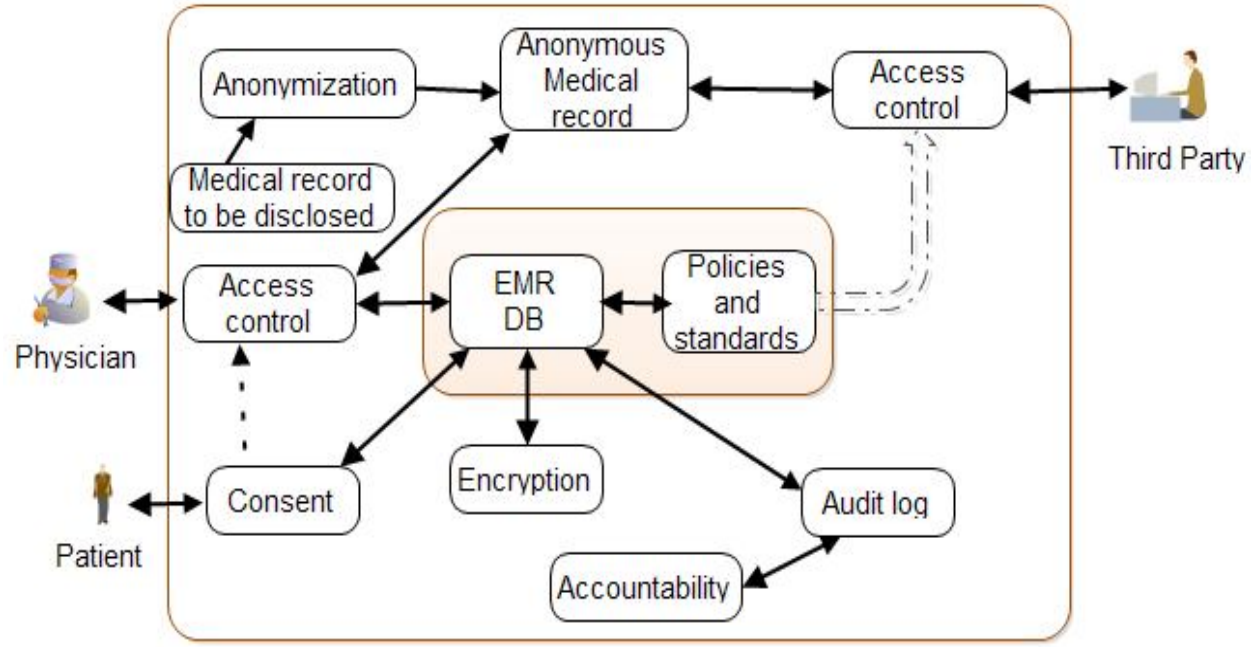


Figure 4.3: Information security and privacy control architecture

4.3.1 Standards and Policies

The objective of a security and privacy standard and policy is to provide management direction and support for information security and privacy in accordance with business requirements and relevant laws and regulations [67]. This requirement addresses the need to accept responsibility for security and privacy within organisations. Some practical rules governing medical record use or user responsibilities towards the information they collect, use, access or otherwise process. This includes standards and policy regarding access control, security management, auditing and monitoring, consent and notification and patent information flow in the hospital.

Access Control: Each identifiable clinical record shall be marked with an access control list naming the people or groups of people who may read it and append data to it. The system shall prevent anyone not on the list from accessing the record in any way.

Security Management, Auditing and Monitoring: It is vital that there should be a continuous management of the security issues as new techniques and uses of new systems take place. All these changes need to be monitored for their effect on the security provided to the Healthcare Establishments. The existing security measures need to be monitored to ensure that they reach adequate levels of compliance and that they remain effective.

Consent and Notification: The responsible clinician must notify the patient of the names on his record's access control list when it is opened and whenever responsibility is transferred. His consent must also be obtained, except in emergency or in the case of statutory exemptions.

4.3.2 Access Control

It ensures the protection of services, prevent unauthorised computer access, detect unauthorised activities and ensure information security and privacy when using EMR in the hospital. Access control includes identification of users during registration, their subsequent authentication during log in, and their authorisation prior to being granted access to services and data.

All communications with the databases and other system objects are according to the policies and controls defined in access control. This makes sure that no interference occurs by any attacker neither internally nor externally and thus, protects the databases from potential errors that can make impact as big as stopping firm operations. Access control also helps in minimizing the risks that may directly impact the security of the database on the main servers.

Among access control schemes Team and Task based RBAC (TT-RBAC) access control is preferred in this study. This extends the RBAC model through adding sets of two basic data elements called teams and tasks. TT-RBAC insure balancing the competing goals of collaboration, security and privacy in collaborative systems or hospitals which is targeted towards making people, information, and resources available to all who need it.

In a physician practice, the nurse and the receptionist, for example, have very different tasks and responsibilities (as shown in Figure 4.4). Therefore, they do not have access to the same information. Hence, designating user privileges is a critical aspect of medical record security. All users have access to the information they need to fulfill their roles and responsibilities and they must know that they are accountable for use or misuse of the information they view and change.

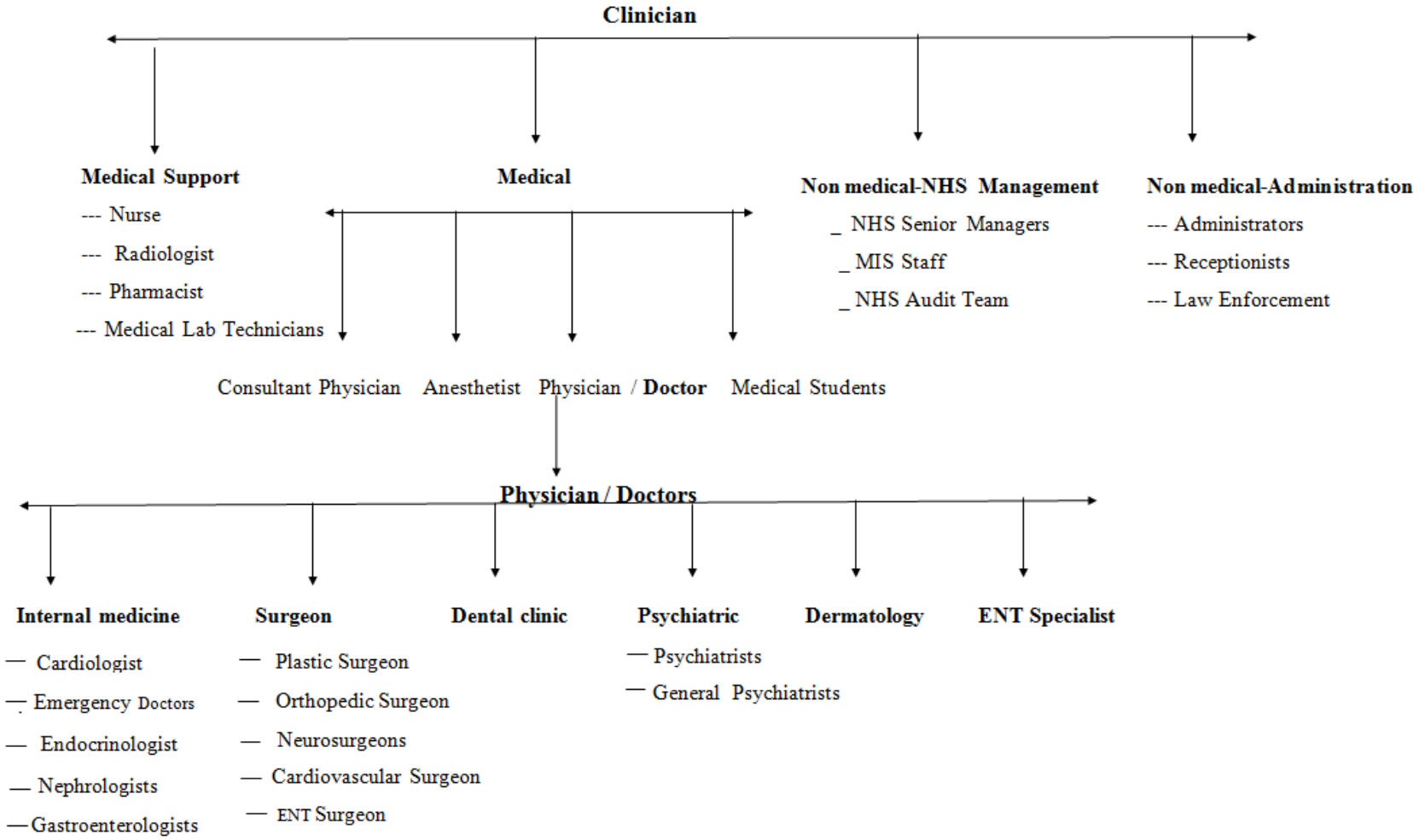


Figure 4.4: Type of clinician in Black lion hospital

Team and Task-based RBAC (TT-RBAC): We use the TT-RBAC model that extends the RBAC model through adding sets of two basic data elements called teams and tasks. TT-RBAC is the concept of team relations, through which users, roles and tasks are connected together. Through the relations of user-team assignments, role-team assignments and task-team assignments, users, roles and permissions are introduced into a team, respectively. Thus, the team defines a small and specific RBAC application zone through which we can preserve the advantages of scalable security administration that RBAC style models offer and yet offers the flexibility to specify fine grained control on individual users in certain roles and on individual object instances. This characteristic enables a team to organize a collection of users with different privileges collaborating together to complete some specific tasks assigned to the team.

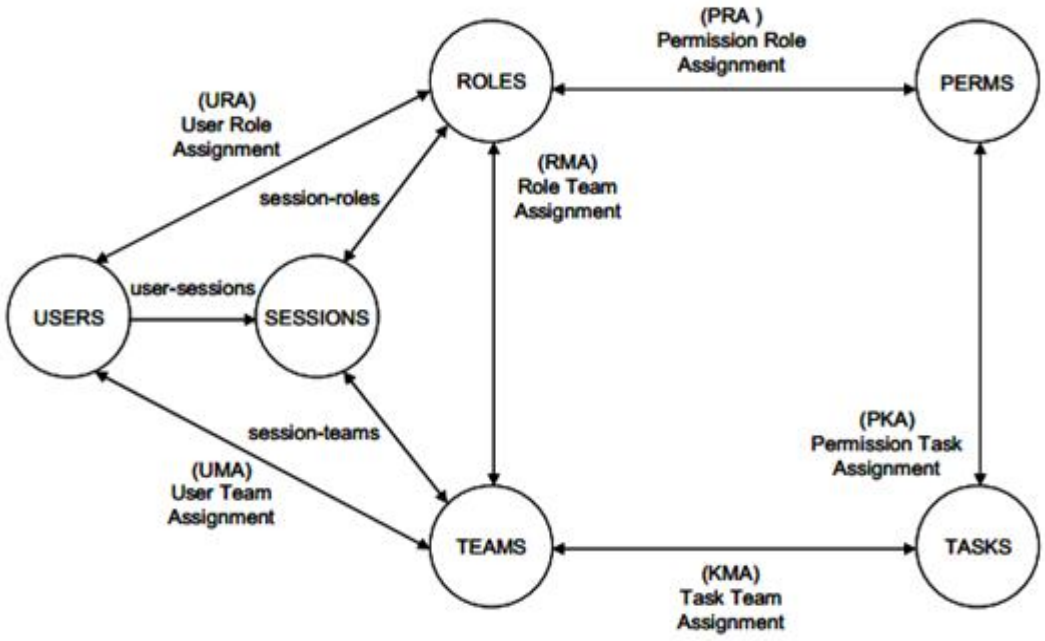


Figure 4.5: TT-RBAC

A team encapsulates a collection of users in various roles and a set of roles with the objective of accomplishing specific tasks.

4.3.3 Consent

This enables to ensure that patient information is collected, accessed, used or disclosed only with a patient's consent. Electronic patient record systems should allow only authorized people involved in care to have access to a patient record and to have access only to those parts of the record that are needed for care.

Patient is fully informed of the implications of their medical status information and permit access to or the collection of their health information. The consent directives service would enable healthcare providers to confirm that patient has consented to the specific clinical trial, provided authorization for data use, and authorization for organizational access. Looking for consent is also a matter of common courtesy between healthcare professionals and patients. Patients also have a fundamental legal and ethical right to determine what happens to them. Then access control mechanisms can maintain the confidentiality of the patient health information according to the patient consent.

4.3.4 Accountability

Limiting user access to the minimum necessary can be challenging. Therefore we implement audit controls and warnings for holding users accountable for their actions.

Individual users are responsible for ensuring that others do not use their system privileges. In particular, users must take great care in protecting their usernames and passwords from eavesdropping or careless misplacement. Passwords are never to be 'loaned.' Individual users must be responsible for any security violations associated with their usernames and password. Operations staff is responsible for reviewing the audit logs and identifying potential security and privacy violations. If the operations staff believes a security incident has occurred, they will immediately notify their management. Management will assess the potential implications of the incident and take any remedial and necessary action.

4.3.5 Security Audits

It defines and identifies security and privacy relevant events and the data to be collected and communicated as determined by policy, regulation, or risk analysis to support identification of those security and privacy relevant events [70]. A secure audit service is the basic EMR system

component responsible for creating and managing details of system and application events. It records significant privacy and security related events.

System Administrator/ authenticated person reviews a file that is generated by the HIE enabling system on a daily basis. The Audit Trail enabling service generates a record of the users who have accessed what files and when. The enabling service also records any attempts to access the system from an unauthorized terminal, the use of an expired username or password, unusual numbers of password attempts and other potential attempted violations of security and privacy policies. The System Administrator may take appropriate action to ensure that future attempts at gaining unauthorized access are unsuccessful.

The audit log service will create a secure audit record each time a user:

a) Accesses, creates or updates PHI of a patient/person via the EMR

b) Overrides the consent directives of a patient/person via the EMR

c) Accesses, creates or updates registration data on an EMR user.

The log file consists of:

- ✓ Time stamp
- ✓ Document ID
- ✓ User ID of the accessing user
- ✓ Document type
- ✓ Activity or the function performed by the accessing user
- ✓ the role the user is exercising
- ✓ IP address

Because logs contain records of system and other sensitive information, they need to be protected from breaches of their confidentiality and integrity. Generally, performing of periodic reviews of audit logs may be useful for:

- ✓ Detecting unauthorized access to patient information
- ✓ Establishing a culture of responsibility and accountability
- ✓ Reducing the risk associated with inappropriate accesses (Note: Behavior may be altered when individuals know they are being monitored)

- ✓ Providing forensic evidence during investigations of suspected and known security incidents and breaches to patient privacy, especially if sanctions against a workforce member, business associate, or other contracted agent will be applied
- ✓ Tracking disclosures of Patient Health Information (PHI)
- ✓ Detecting new threats and intrusion attempts

4.3.6 Anonymization

Patient health information (PHI) plays a major role in conducting medical research purposes for improving healthcare quality. Universities, government agencies, and private healthcare entities also use such data for measuring effectiveness of medical treatments, tracking contagious diseases, support decision making and for other development and marketing purposes. However, disclosure of health information to researchers raises concerns of privacy violations [71].

We implement anonymization service that takes PHI representing an identifiable individual and then removes all personal identifiers. The goal is to make information accessible to secondary users of healthcare data (healthcare researchers, public health, administrators or other reasons that do not benefit the data subject directly) without violating patient privacy. Anonymization can be accomplished by removing the data or replacing each data element. Our anonymization process performs the following functions:

- ✓ Deletes the unique patient identification number (UPN)
- ✓ Deletes the patient full name
- ✓ Deletes the patient address like telephone number, FAX numbers, Email addresses
- ✓ Rounds the patient date of birth
- ✓ Deletes medical record numbers
- ✓ Deletes full face photos and comparable images
- ✓ Deletes any unique identifying number, characteristic or code

The only identifier that remains is the internal database primary key which is a simple integer value. We cannot identify individual patients from this identifier alone. We use anonymization by using **k-anonymity** algorithm (Figure 4.6).

Definition: (k-anonymity) A table is said to be k-anonymized with respect to a set of identifier(I) if and only if each record (sample) of a table is identical to at least k-1 other records. Identifier (I) is an attribute in the table that uniquely identifies individuals such as address, name phone number and gender.

The main purpose of k-anonymization is to de-identify table through generalization or suppression. Eliminate unsafe combinations by generalizing attributes and cell suppression.

Generalization: Conversion of any value to a more general form is the process of generalization. Example, male and female can be generalized to Person. Generalization can be applied at the following levels:

Attribute (AG): Generalization is performed at the level of column. A generalization step generalizes all the values in the column.

Cell (CG): Generalization is performed on single cells as a result a generalized table may contain, for a specific column, values at deferent generalization levels. Example,. generalizing date, month and year form different levels of generalization.

Suppression: Removing any value completely from a data table is the process of suppression. Suppression can be applied at the following levels:

Tuple (TS): Suppression is performed at the level of row. A suppression operation removes a whole tuple.

Attribute (AS): Suppression is performed at the level of column. A suppression operation obscures all the values of a column.

Cell (CS): Suppression is performed at the level of single cells, as a result a k-anonymized table may wipe out only certain cells of a given tuple/attribute.

Anonymization algorithm

Input: *Private table PT (tale to be anonymized). identifier I = (A1,....,An)*
K constraints
Output: *Anonymized Table AT*
Method:
freq <---- frequency list contains distinct sequences of values of PT(I)
Along with the number of occurrences of each sequence
while there exists *sequences in freq occurring less than k times*
That account for more than k tuples ***do***
let *Aj be attribute in freq having the most number of distinct values*
freq<-- *generalize the values of Aj in* ***freq***
freq<-- *suppress sequences in freq occurring less thank times*
freq<-- enforce k requirement on suppressed tuples in ***freq***
Return AT <-- *construct table from* ***freq***

Figure 4.6: Algorithm for K-Anonymity

4.3.7 Encryption

Encryption maintains data confidentiality using cryptography. To maintain data confidentiality and integrity of EMR, we implemented encryption of EMR data within databases and encryption of stored data/backup files.

4.3.7.1 Database Level Encryption

Such approach provides an important layer of security to sensitive data. Database level encryption allows securing data as it is written to and read from a database. By doing so, database encryption protects data while it is in use by the database system, as well as while it is in storage. It is deployed at the column level within a database table (and hence is sometimes referred to as column encryption) to encrypt individual columns in a data table so that they can only be seen by authorized users or user groups. When coupled with database security and access controls, database encryption provides a secure means of preventing unauthorized access to PHI.

The security of the database and communication is provided through hybrid (RSA and AES) algorithm. Each sensitive data element is encrypted and then stored in the database and only the authenticated users can see any required data. User is authorized to access the data depending upon permitted user access level.

4.3.7.1.2 Hybrid Encryption Algorithm

When we look at the efficiency of both AES and RSA, AES is faster than RSA for encryption and decryption of large messages while RSA is suitable for key management as it is based on the difficulty of factoring large numbers [72]. Taking into account the advantages of both AES and RSA and avoiding their shortcomings, hybrid encryption algorithm based on AES and RSA has been proposed in which AES is used for encryption of data and RSA is used to encrypt the AES key. This hybrid encryption algorithm can be used in health information system to avoid the current risks. The entire hybrid encryption process is as follows:

Process of Encryption

Hybrid encryption is recommended for large data as it improves the encryption/decryption. First, the content is symmetrically encrypted with a generated random initialization vector (IV) and a generated AES key. Then, these two encryption parameters are asymmetrically encrypted with the RSA public key. During the process of storing encrypted data, the random number generator produces 256-bit AES key only once, it encrypts the plaintext to produce cipher text.

Process of Decryption

During the decryption of hybrid encryption algorithm, first the function fetches the saved encrypted key and IV then these key are decrypted by RSA algorithm. Using the AES key K and initialization vector IV it then decrypts the cipher text from database and fetches to the form.

4.3.7.2 Backup Data Encryption

The use of encryption is essential to the secure backup of EMR data containing PHI. This module provides a user interface for the backup procedure. Only administrator is allowed to backup the database and during the backup process the backup is encrypted by using some key and the system/database administrator uses the key to restore the database or share it to some authenticated user if needed. Furthermore, administrator is allowed to restrict which tables would be included in the backup.

Chapter 5

Implementation and Discussion

This Chapter presents the various tools used during the implementation of the system and the prototype of the proposed system and discussion.

5.1 Development Environment

We used different tools and technologies for the implementation of the prototype. Some of them are listed below:

Hibernate is an object relational mapping tool used to map database records to Java objects (Object relational mapping). The Spring Framework was designed to simplify the development of Java programming by addressing complexities introduced by the J2EE architecture. Spring web applications follow the Model View Controller (MVC) design pattern for web development. Apache Tomcat version 6.0.37 for HTTP web server environment is used in order to run the java servlet codes. MySQL database server version 5.0.2 is used to store detail medical information of patients and privacy protection related information of patients. MySQL Connector/JDBC version 5.1.25 is used for native java driver which converts JDBC (Java Database Connectivity) calls into the network protocol used by the MySQL database.

5.2 Implementation of the Prototype

The aim of this prototype implementation is not only to bridge the gaps in information security and privacy of health information system but also to test and enhance the newer technologies in solving community problems in other words proof our concept prescribed in this study.

We used OpenMRS as the platform to develop an electronic health information system to support all services of health information system in Black lion hospital. OpenMRS also existed in a range of deployment sizes from small clinics and large hospitals. In addition, OpenMRS was quickly able to be customized to support not only patient based data management but also insure information security and privacy of health information system.

The design of OpenMRS offers security features. These are use of standards such as HL7 for medical data transfer and encryption of data transmitted over the web using Secure Socket Layer

(SSL) Protocol. OpenMRS did not provide auditing of all required items for the study. All the security and privacy features we described in chapter 4 are integrated in to the OpenMRS source code.

The implementation of OpenMRS source code is divided into three main components. These are the User Interface, Service, and Data Access layers. This layering isolates various system responsibilities from one another to improve both system development and maintenance.

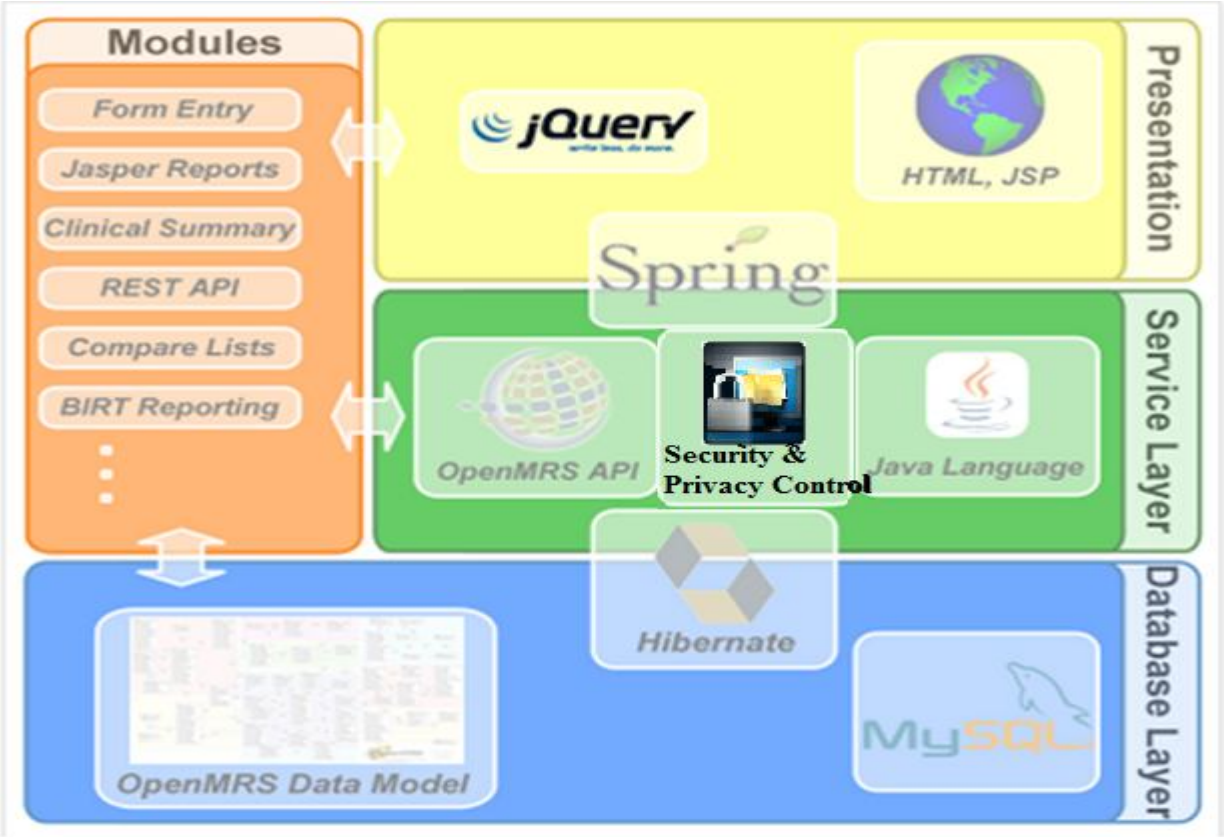


Figure 5.1: Component of the prototype

5.2.1 Data Access Layer

The data access layer is an abstraction layer from the actual data model and its changes. It uses Hibernate as the Object Relational mapping tool, and Liquibase to manage relational database changes in a database independent way. The relationships between our domain objects and database tables are mapped using a mixture of Hibernate annotations and XML mapping files. The data access layer is exposed to the service layer through interfaces, thereby shielding it from implementation details such as which object relational mapping tool is being used.

5.2.2 Service Layer

The service layer is responsible for managing the business logic of the application. It is built around the spring framework. The OpenMRS service layer classes make extensive use of the Spring framework for a number of tasks including the following:

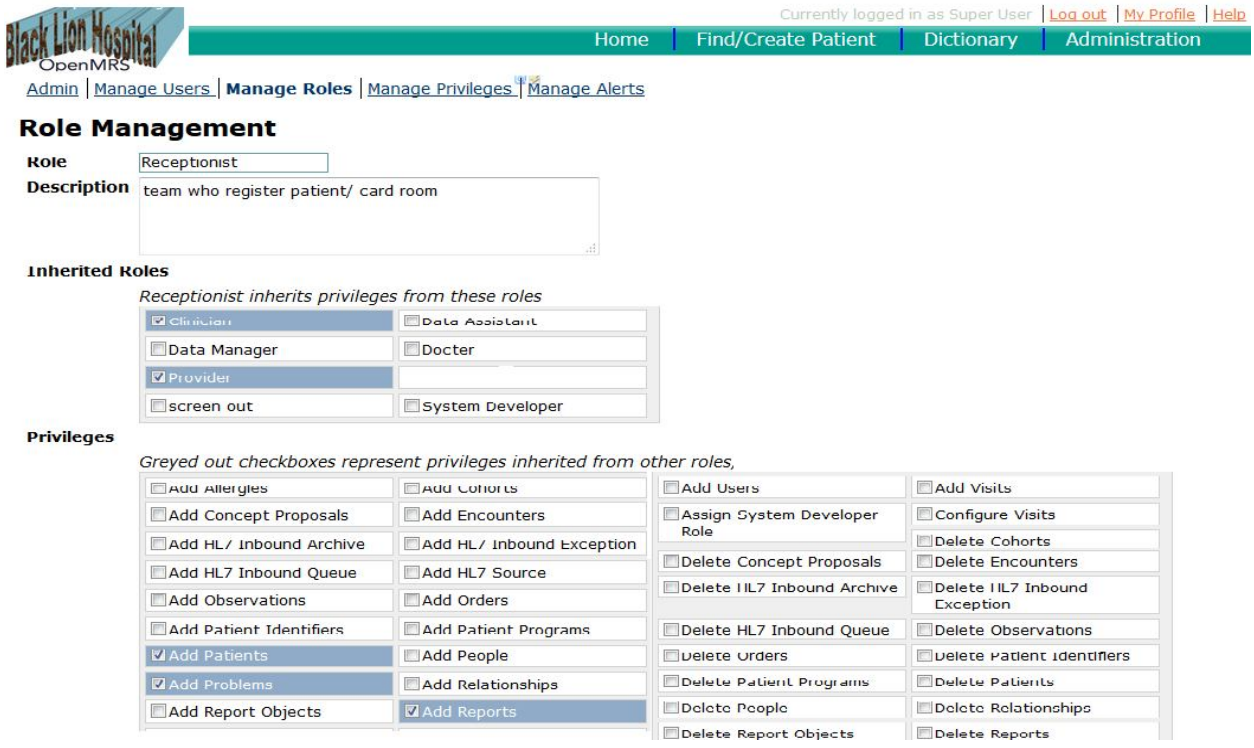
Spring Aspect Oriented Programming (AOP) is used to provide separate cross cutting functions (for example: authentication, logging).

Spring Dependency Injection (DI) is used to provide dependencies between components. Spring is used to manage transactions between service layer classes.

5.2.2.1 User Management and Access Control

This restrict direct access to specific types of sensitive data (e.g., mental health records, HIV results, etc.). To implement our fine grained access control, we use TT-RBAC. To provide access to users first we create a team and role is assigned to the team. For each user, the exact privilege he/she obtains from a team is determined by his/her roles and the current activity of the team. In addition, TT-RBAC model includes a set of sessions where each session is a mapping onto an activated subset of roles and an activated subset of teams that are assigned to the user.

Roles and Privileges are controlled through the Administration page, under the Manage Users section.



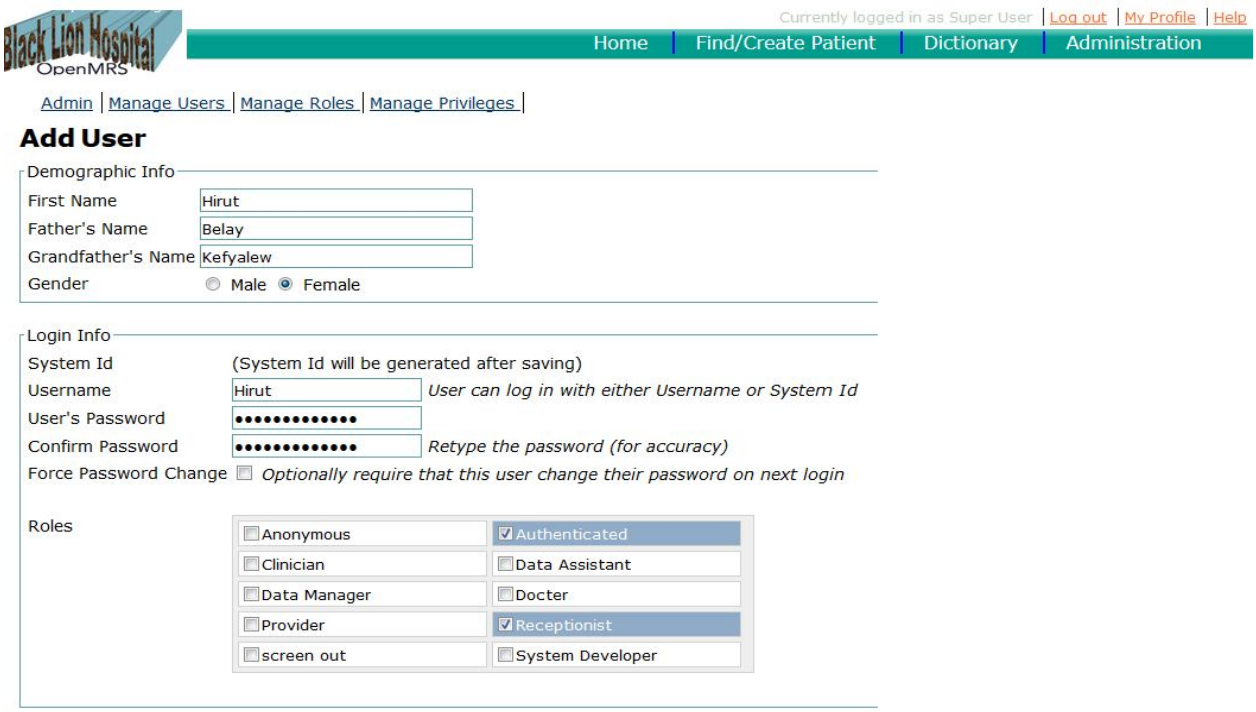


Figure 5.2: Screen shot for the implementation of user management and access control

5.2.2.2 Encryption of Database

This class provides the functionality for encryption and decryption of sensitive data in database to ensure security of the data. Encryption is performed when the data is written to database using AES key. After that when the data is needed by authenticated person it decrypted and return to the user. The AES key and the init vector are encrypted using RSA key and saved in the runtime property as shown below:

```
#Auto generated by OpenMRS initialization wizard
#Tue Jan 06 01:41:50 PST 2015
encryption.vector=OBw/2qmtLEauhUUb50eA7Q\=\=
connection.url=jdbc\:mysql\://localhost\:3306/openmrs?autoReconnect\=true&sessionVariables\=storage_engine'
module.allow_web_admin=true
connection.username=openmrs_user
auto_update_database=false
encryption.key=CWEv3/JkuziQ4GavrtAGPg\=\=
connection.password=9OVXiO^c|\#~J
```

5.2.2.3 Audit

To establish trust and accountability only authorized users (like doctors) have access to patient data and all accesses are logged, so any inappropriate access can be audited. Log4j is designed to be usable as an audit logging framework. The main components of log4j are sown in Figure **5.3**

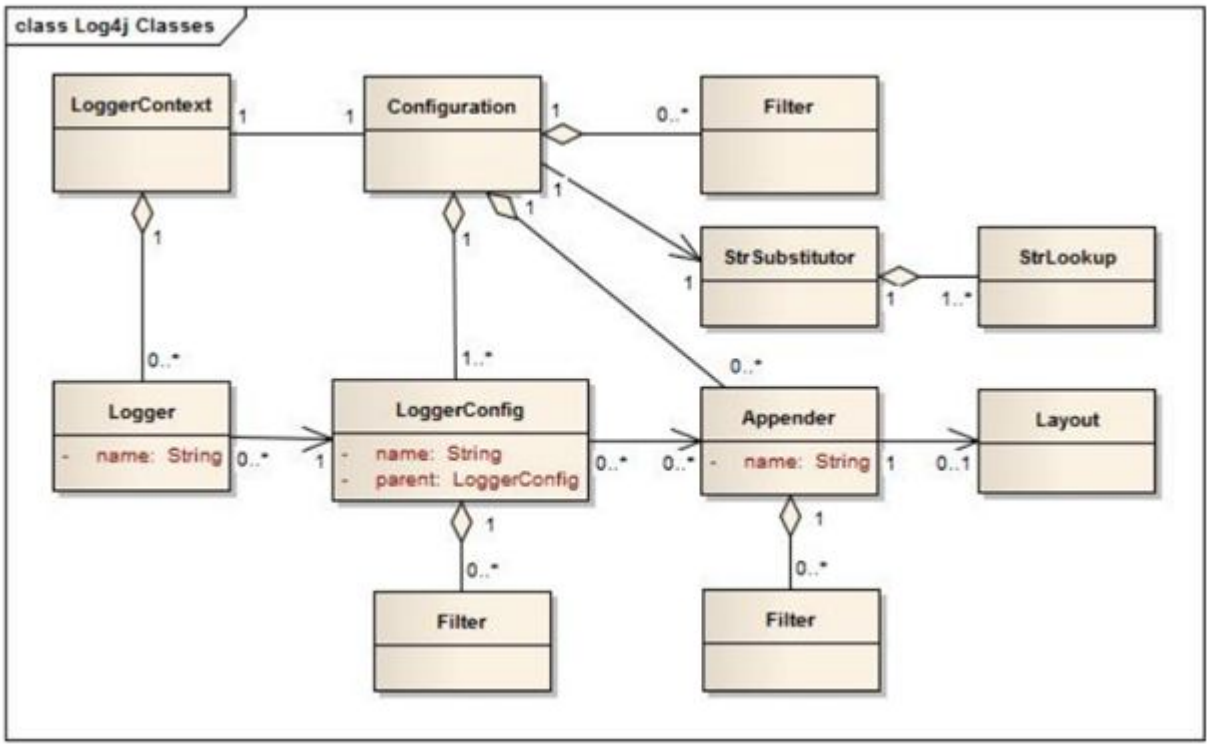


Figure 5.3: Components of Log4j

LoggerContext is the anchor point for the logging system. This class is used for tracking existing loggers and creating new ones on request. **Configuration** is Part of the core API which represents a parsed configuration to be used with one or more LoggerContexts. **LoggerConfig** is another part of the Core API which represents the logger elements in the configuration file. Links one Configuration to an arbitrary number of Loggers and Loggers pass along their logged messages to their respective LoggerConfig.

Appender is used for routing log messages to a physical destination. It contains a Layout object for LogEvent objects. **Layout** configures the output format of log events. Layout is responsible for formatting the LogEvent according to the user wishes, whereas an appender takes care of sending the formatted output to its destination. Pattern configure what relevant log event data (message, method/location, thread name, date/time) to output. Usually used with a

PatternLayout. The PatternLayout, part of the log4j distribution, lets the user specify the output format according to conversion patterns. **Filter** selects which log events should be logged or not. **Lookup** provides property variables for configuration files.

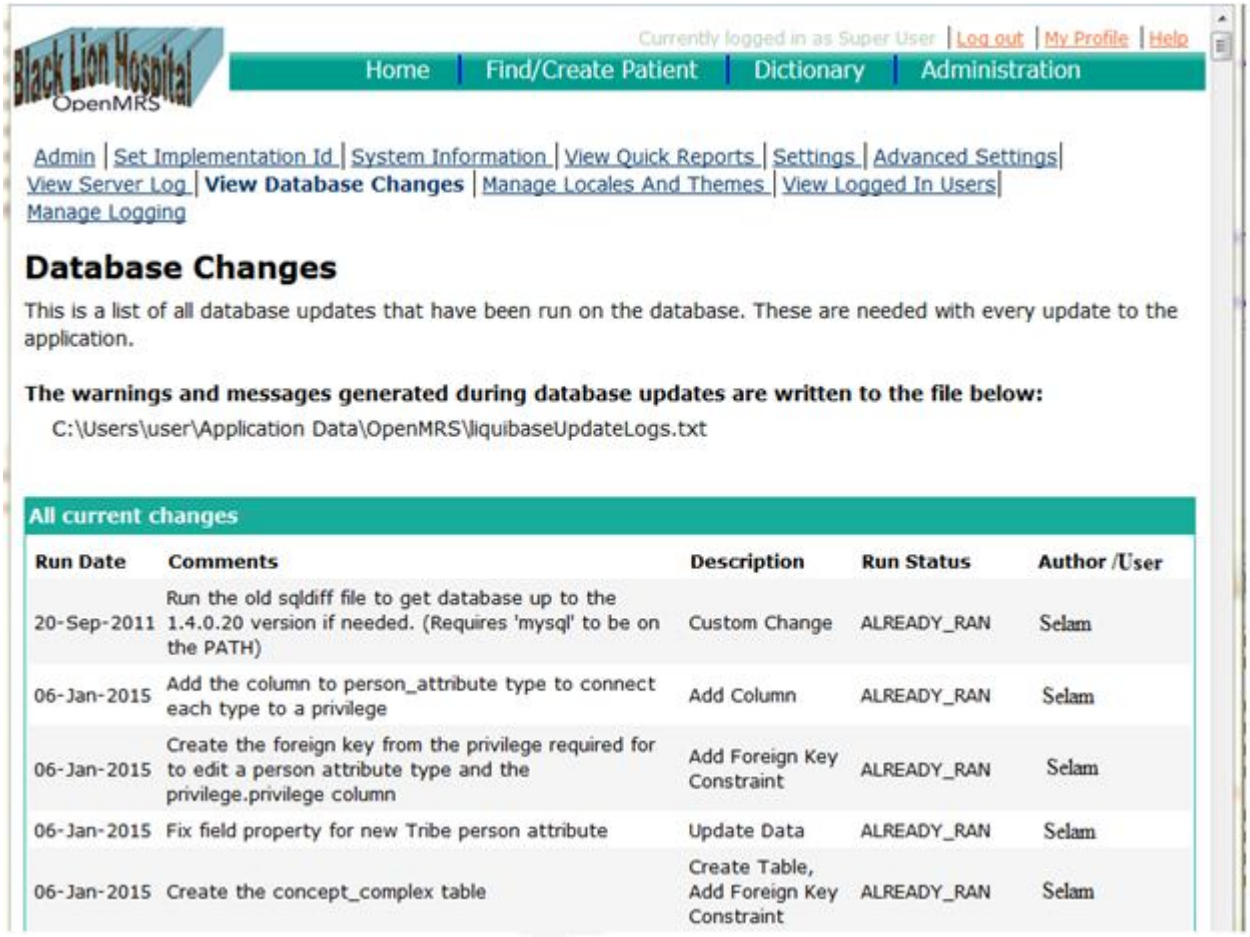


Figure 5.4: Screen shot for the implementation of the database change log scenario

5.2.2.4 Anonymization

In order for the recipient of the data not to be able to compromise patient privacy, we implement anonymization. Sensitive raw data like identifiers, names, addresses and the like should be modified or trimmed out from the original database.

Orginal Database To Be Disclose

ID	NAME	GENDER	YEAR OF BIRTH	TEST RESULT	PHONE NUMBER
1	Abebe Teka	male	1959	+ve	+251910558700
2	Grum Bekele	male	1962	-ve	+251910432115
3	Almaz Enku	female	1955	-ve	+251912513467
4	Dereje Grma	male	1959	-ve	+251913678011
5	mulualem Belay	female	1942	-ve	+251914559109
6	Abebech Mola	female	1975	-ve	+251941559288
7	Alem Eshetu	female	1966	+ve	+251910559333
8	Helen Melese	female	1987	-ve	+251911559421
9	Dawit Dereje	male	1975	-ve	+251927559572
10	Abrham Teferi	male	1978	-ve	+251927559631
11	Blen Bezabeh	female	1964	-ve	+251945559701
12	Alemu Samson	male	1959	+ve	+251916559877
13	Saron Sehalu	female	1975	-ve	+251933559902
14	Admasu Gebru	male	1967	-ve	+251941056004

Anonymization

ID	GENDER	DATE OF BIRTH	TEST RESULT
1	male	1950- 1959	+ve
2	male	1960-1969	-ve
4	male	1950-1959	-ve
6	female	1970- 1979	-ve
7	female	1960- 1969	+ve
9	male	1979- 1979	-ve
10	male	1970- 1979	-ve
11	female	1960- 1969	-ve
12	male	1950- 1959	+ve
13	female	1970-1979	-ve
14	male	1960- 1969	-ve

Disclosed (K-Anonymized) Database

Figure 5.5: Anonymized data using K-anonymity algorithm

5.2.3 User Interface Layer

The user interface layer is built upon spring MVC, Direct Web Remoting (DWR), JSP and JavaScript. DWR is used for AJAX functionality and it provides the mapping between our Java objects and methods to JavaScript objects and methods respectively. JQuery is used to simplify the interactions with Javascript and the browser. Spring MVC is used to provide the Model View Controller design pattern.

In addition to the security and privacy consideration the user interfaces are customized according to Black lion hospital forms (e.g. Figure 5.6).

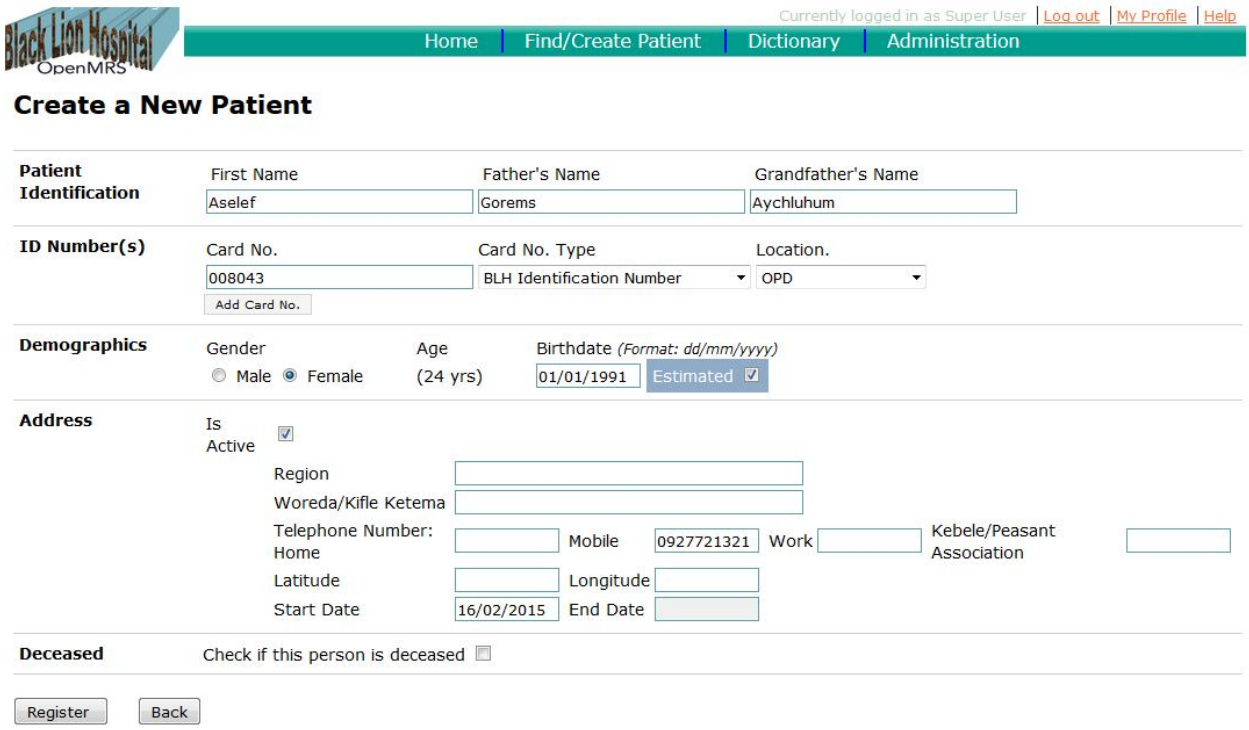


Figure 5.6: Screen shot for the implementation of patient registration user interface

5.3 Evaluation of the Prototype

This sub-chapter presents the security and usability evaluation of the proposed prototype. The evaluation of the prototype was conducted by subjects who provided their response using interview survey.

The system user test was run with 10 participants. Participants for the evaluation are potential or actual end users chosen from two different hospitals, namely Black lion hospital and Korean hospital. Participants were drawn from various departments of the hospitals such as OPD (Out Patient Department), card room, General Medicine and IT staff. We have selected 5 participant from each hospital.

The first part of the evaluation was intended to assess the usability of the system in Black lion hospital. Afterwards, we continue the evaluation with the security and privacy perspective. The summary of the response from the participants is as follows.

In evaluating the proposed prototype, participants were confident in supporting the idea of introducing free and open source based health information system due to the fact that the system easy to use. The participants said that the open source based electronic information system is not common in the hospital. One participant said "electronic patient information system is not common enough but it is a major concern for the future". The participants were confident at answering yes on the usability and applicability of the proposed prototype in their hospital. Health information systems experts from Korean hospital who were involved in this study reported existence of electronic patient information system in place but are not efficient as most of them lack information security and privacy supports. One health data expert said "I have tested the developed system. As I have seen the system has high potential of improving the existing health information system in Black lion hospital ".

Majority of interviewees from Black lion hospital believed that hospital has sensitive information so there should be high security in order to prevent sensitive information from access of unauthorized users.

Interviewee personnel of Korean healthcare providers said that it is significant to provide good privacy and safety to patient sensitive information as well as Electronic Health Records of Healthcare providers. A small breach of sensitive information of healthcare causes the disclosing of sensitive information to unauthorized users, fraud risk is increased, and violation is arising to patient privacy.

Interestingly, participants were suggesting features which are already included in the prototype such as security and privacy is very important. This assured us about the demand and political feasibility of the prototype in real scenario.

In general, all participants supported the idea behind the proposed prototype and show their hopes that the prototype is applicable in their hospital. The doctor who was contacted in this study quoted saying "I believe this application could be very useful in developing countries and also could save time, resources and workload in addition to that the interfaces are easy to use ".

5.4 Discussion

The document analysis and the interviews indicated current practice of electronic and non electronic patient information system and how it lacks information security and privacy architecture. Disclosing of sensitive information to unauthorized users, fraud risk is increased, and violation is arising to patient privacy. But security and privacy are major concern of both the patient and the hospital. Black lion hospital currently has a serious challenge and problems in handling patient information system.

The proposed prototype has implemented electronic patient information system that is easy to manage and use. In addition, the proposed prototype has implemented security and privacy of sensitive patient information. Compared with paper based methods, which require extra efforts, the proposed prototype reduces errors, save time, and save money in the health information system. The proposed prototype is based on open source technologies, which allow future development with less effort, which can be affordable and manageable by the economy of the developing regions like Ethiopia. So, the proposed prototype seems to have capability of enhancing the information security and privacy in health information system.

5.4.1 Answering the Research Questions

RQ1: What are the available open sources that can be used in health information system? And which of those open source systems are appropriate for building secure HIS?

There are several types of open source health information systems that are available for use by physicians and hospitals. While answering this research question, we have critically analyzed several literature review by considering different factors such as both modular and complete EMRs, security features, specific requirements of the systems adopted by our hospital, the database they support whether it is proprietary or free open source, platform support and storage capability.

By considering those factors we have found that OpenMRS has the most potential and is the fast growing open source system available today. Because it has common framework and is almost completely comprised of free, open source components. Its modular software architecture allows separate components of software to “plug in” to the main system and allows additional functionalities to be added (and removed) without changing the core system.

RQ2: What security architecture and implementation is suitable to safeguard patient information in HIS?

To answer this research question, information security and privacy architecture has been proposed. The prototype has been developed from the open source selected after evaluating several available open sources. Security and privacy architecture for sensitive information system maintained through the implementation of appropriate security and privacy aspects formally proved and discussed according to the description of Chapter 4. which include encrypt and decrypt electronic health information in database, auditing/audit logs (record actions) related to electronic health information, verify that electronic health information has not been accessed by unauthorized user and detect the modification and deletion of electronic health information and audit logs and insure that patient information is not disclosed to third parties.

Generally, the goal of this thesis work is to enhance information security, privacy and safety of patient using free and open source HIS to benefit patients and the healthcare system overall. Moreover, it has already been observed that the use of open source based health information system is feasible both in general healthcare domain and in Black Lion healthcare system.

Chapter Six

Conclusion and Future Work

6.1 Conclusion

To establish greater public trust in HIS and patients and thereby facilitate adoption of these new technologies, a comprehensive privacy and security architecture must be in place. We adopted and enhanced free and open source software in hoping to strengthen the information security and privacy of health information system. We did this by enhancing the security and privacy architecture of the system. To achieve this we have implemented various changes. We implemented TT-RBAC to protect against loss and unauthorized access to information. An audit feature, which records who accessed patient information, what changes were made and when. We address the security and privacy concerns of PHR system by integrating advanced cryptographic techniques, such as RSA and AES, into PHR system.

The main theme of this thesis is that such major paradigm shifts demand a rethinking of the security and privacy aspects and solutions. The desire is to engage all parties, including the clinicians and patients, and understand what is acceptable and desirable before the coming generation of healthcare systems is deployed. There will certainly be tension between security and usability, between patient privacy and the clinician convenience. The point here is therefore to hit the balance between the two and come up with a system that satisfies both.

Accordingly, we have developed a prototype based on an open source called OpenMRS that overcomes the above limitations and ensure adequate privacy and security protections for HIS. This is done through the implementation of appropriate technical capabilities such as encrypt and decrypt electronic health information, audit and control procedures, anonymization mechanism which is called k-anonymity. In addition to that we implement TT-RBAC to prevent unauthorized or inappropriate access, patient consent to disclose medical record and secure back up.

The prototype is tested based on the demo data of OpenMRS and evaluated by health professionals in Black lion and Korean hospitals. According to the evaluation the proposed

prototype meets all of our objectives and shows that it strikes a balance between usability, security and privacy of patient information.

6.2 Contributions

The contribution of this thesis is a novel information security and privacy architecture that provides strong authentication and authorization mechanisms to conduct dynamic membership of groups and individuals to share or access sensitive information. It also prevents legal users accessing unauthorized sensitive information against internal security threats. The architecture achieves strong protection for sensitive information storage in order to overcome security threats that compromise credentials of information systems. Finally, the proposed architecture achieves privacy protection and includes a feature to detect and prevent intrusion.

6.3 Future Work

Since the advancement of EMR increases vulnerability of the privacy and security of health data, especially sensitive health data which might have great impact to the health service, future works to the continuation of this work are:

- Securing health data by means of biometric technologies such as finger print.
- Online access to such record by patient is another important aspect of the service that can be add-on to the proposed system.

References

[1] Fostering a Security and Privacy Culture, www.wikipeda.org (2002), From: http://en.wikipedia.org/wiki/E-Services, Retrieved On Oct 15,2013

[2] Naikuo Y., Howard, B. and Ning, Z, A Purpose-Based Access Control Model, 2007. Proceedings of the 3rd International Conference on Data Engineering Workshop, Istanbul

[3] Information Technology Development Creativity, www.cms.gov (2005), From: http://www.cms.gov/EHR Incentive Programs/ Downloads/EP-MU-TOC.pdf, Retrieved On Oct 15, 2013

[4] Model Based Design of Trustworthy Health Information Systems, From: http://www.dagstuhl.de/de/programm/kalender/semhp/?semnr=09073, Retrieved on Oct 15,2013

[5] NRC National Research Council (1997), Protecting Electronic Health Information.

[6] Healthcare data privacy and security , www.cms.gov (2010), From ,http://www.cms.gov/EHR Incentive Programs /Downloads/EP-MU-TOC.pdf, Retrieved On Oct 8,2013

[7] Mercuri, R., The HIPAA-potamus in healthcare data security, 2004, International Journal of u- and e-Service.

[8] Security and Privacy System Architecture for an e-Hospital Environment , www.hhs.gov (2002), From: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html, Retrieved Oct 8,2013

[9] Use and disclosure of personal information, www.metahealthcare.com (1999), From: http://www.metahealthcare.com/solutions/openmrs/, Retrieved On Nov 02,2013

[10] AApplebaum, P.S. (2002), Privacy in psychiatric treatment, threats and response, American Journal of Psychiatry, Vol. 159,

[11] Tikur Anbessa (BlackLion) Hospital, www.inctr.org (2013), From, http://www.inctr.org/network-magazine/current-edition/partner-profile/tikur-anbessa-black-lionhospital/, Retrieved On Nov 3,2013

[12] Data Protection Acts 1988, www.dataprotection.ie (2003), From, http:// www.foi .gov.ie/regulations/regulation, Retrieved On Feb 1,2015

[13] www.dataprotection.ie (2003), Data Protection Guidelines on research in the Health Sector, From, http://www.dataprotection.ie/documents/guidance/Health research, Retrieved On Feb 1,2015

[14] Guidelines of the Irish College of General Practitioners National General practice Information Technology Group (www.gpit.ie) Data Protection Acts 1988.

[15] Freedom of Information Act 1997 section 28(6) Regulations 1999

[16] Davidson, P.L., A Complex Multi-location Enterprise: Issues and possible Solutions. Healthcare Information Systems. Auerbach Publications, New York, NY 199. Available: http://www.cedarcreek.org / HCvsIT.htm, 2004.

[17] Doolin B., Power and resistance in the implementation of a medical management information system Information Systems Journal. 14(4) , (2004)

[18] www.Market Research.com (2007), Wireless Opportunities in Healthcare, Kalorama Information, From: http://www.Market Research.com, Retrieved Oct 27,2013

[19] Ramsaroop, P. and Ball, M.J. (2000) 'A model for more useful patient health records', MD Computing, Vol. 17, No. 4, pp.45–48.

[20] Landry, J. P., Pardue, J. H., Johnsten, T., Campbell, M., & Patidar, P.(2011). A threat tree for health information security and privacy. InV. Sambamurthy & M. Tanniru (Eds.), Proceedings of the 17th Americas Conference on Information Systems. Detroit: AIS.

[21] Shahri, A. B., & Ismail, Z. (2012). A tree model for identification of threats as the first stage of risk assessment in HIS. Journal of Information Security, 3(2), 169–176.

[22] Rindfleisch, T.C., (1997). Privacy information technology and healthcare. Communications of the ACM, 40(8),

[23] Rohm, A. J.,& Milne, G. R. (2004). Just what the doctor ordered: the role of information sensitivity and trust in reducing medical information privacy concern. Managing the Future of HealthCare Delivery, 57(9), 1000–1011. doi:10.1016/S0148-2963(02).

[24] Johnson, M. E. (2009). Data hemorrhages in the health-care sector. In R. Dingledine & P. Golle (Eds.), Financial cryptography and data security, LNCS 5628 (pp. 71–89). Berlin: Springer-Verlag.

[25] Appari, A., & Johnson,M. E. (2010). Information security and privacy in healthcare: current state of research. International Journal of Internet and Enterprise Management, 6(4), 279–314. doi:10.1504/IJIEM.2010.035624.

[26] Appelbaum, P. S. (2002). Privacy in psychiatric treatment: threats and responses. The American Journal of Psychiatry, 159(11), 1809– 1818.

[27] Kotz, D. (2011). A threat taxonomy for mHealth privacy. Proceedings of the Third International Conference on Communication Systems and Networks (pp. 1–6). Bangalore: IEEE.

[28] Gritzalis, D. A. (1998). Enhancing security and improving interoperability in healthcare information systems. Informatics for Health and Social Care, 23(4), 309–323. doi:10.3109/14639239809025367.

[29] Dong, C. and Dulay, N. (2006) 'Privacy preserving trust negotiation for pervasive healthcare', Proceedings of Pervasive health Conferences and Workshops, Innsbruck, Austria, pp.1–9.

[30] Hung, P.C.K. (2005) 'Towards a privacy access control model for e-healthcare services', Proceedings of 3rd Annual Conference on Privacy, Security and Trust, New Brunswick, Canada, http://www.lib.unb.ca/Texts/PST/2005/

[31] Peyton, L., Hu, J., Doshi, C. and Seguin, P. (2007) 'Addressing privacy in a federated identity management network for e-health', Proceedings of the 8th World Congress on the Management of eBusiness, Toronto, Canada, pp.12–12.

[32] Raman, A. (2007) 'Enforcing privacy through security in remote patient monitoring ecosystems', 6th International Special Topic Conference on Information Technology Applications in Biomedicine, Tokyo, Japan, pp.298–301.

[33] Zheng, Y., Chen, Y. and Hung, P.C.K. (2007) 'Privacy access control model with location constraints for XML services', Proceedings of the 23rd International Conference on Data Engineering Workshop, Istanbul, Turkey, pp.371–378.

[34] Sankar, P., Moran, S., Merz, J.F. and Jones, N.L. (2003) 'Patient perspectives on medical confidentiality: a review of the literature', Journal of General Internal Medicine, Vol. 18, pp.659–669.

[35] Bansal, G., Zaheid, F.M. and Gefen, D. (2007) 'The impact of personal dispositions on privacy and trust in disclosing health information online', Americas Conference on Information Systems, Keystone, CO, http://aisel.aisnet.org/amcis2007/57

[36] Campbell, B., Thomson, H., Slater, J., Coward, C., Wyatt, K. and Sweeney, K. (2007) 'Extracting information from hospital records: What patients think about consent', Quality and Safety in Healthcare, Vol. 16, No. 6, pp.404–408.

[37] Angst, C.M., Agrawal, R. and Downing, J. (2006) An Empirical Examination of the Importance of Defining the PHR for Research and for Practice, http: //ssrn .com/ abstract = 9 04611

[38] Sloane E.B., "Using Standards to Automate Electronic Health Records (EHRs) and to Create Integrated Healthcare Enterprises", Proceedings of the 29th Annual International Conference of the IEEE EMBS, Aug. 2007.

[39] National E-Health Transition Authority. Draft Concept of Operations: Relating to the introduction of a personally controlled electronic health record (PCEHR) system. 2011.

[40] Sandhu, R. S. and Samarati, P. Access control: principle and practice. Communications Magazine, IEEE, 32, 9 1994), 40-48.

[41] Kadhem, H. Amagasa, T. Kitagawa, H. A Novel Framework for Database Security based on Mixed Cryptography Internet and Web Applications and Services, 2009. ICIW '09. Fourth International

[42] Sparrow, M. K., "License to Steal. How Fraud Bleeds America's HealthCare System", West view Press; 2000. ISBN: 0-8133-6810-3.

[43] J. West, "How open is open enough? Melding proprietary and open source platform strategies," Research Policy, vol. 32, no. 7, pp. 1259-1285, Jul. 2003.

[44] Reynolds CJ, Wyatt JC. Open source, open standards, and healthcare information systems. J Med Internet Res 2011;13:e24.

[45] Open Source initiatives. Available from: http://www.Opensource. org/docs/osd. Accessed on 2012 Dec 6.

[46] Gallivan MJ. Striking a balance between trust and control in a virtual organization: A content analysis of open source software case studies. Inf Syst J 2001;11:277-304.

[47] Webster PC. The rise of open-source electronic health records. Lancet 2011;377:1641-2.

[48] National Consumer Health Privacy Survey 2005, California HealthCare Foundation (November 2005)(2005 National Consumer Survey).

[49] Mu, Y., Susilo, W., Lin, W.-X., Ruan, C.: Identity-based authenticated broadcast encryption and distributed authenticated encryption. In: ASIAN, in: LNCS, vol. 3321, pp. 169–181 (2004)

[50] Byun, J.-W., Bertino, E. and Li, N. Purpose based access control of complex data for privacy protection. In Proceedings of the Proceedings of the tenth ACM symposium on Access control models and technologies (Stockholm, Sweden, 2005).

[51] Naikuo, Y., Howard, B. and Ning, Z,A Purpose-Based Access Control Model, 2007.

[52] Al-Fedaghi, S. S. Beyond purpose-based privacy access control. In Proceedings of the Proceedings of the eighteenth conference on Australasian database - Volume 63 (Ballarat, Victoria, Australia, 2007). Australian Computer Society, Inc.

[53] J.A. Akinyele, C.U. Lehmann, M.D. Green, M.W. Pagano, Z.N.J. Peterson, and A.D. Rubin. Self-protecting electronic medical records using attribute-based encryption. Technical report, Cryptology ePrint Archive, Report 2010/565, 2010. http://eprint. iacr. org/2010/565.

[54] Myong H. Kang, Joon S. Park, Judith N. Froscher, "Access Control Mechanisms for Inter-Organizational Workflow", SACMAT'01, May 3-4, 2001, Chantilly, Virginia, USA pp 66-74. ACM 1-58113-350-2/01/0005.

[55] John A. Miller, Mei Fan, Shengli Wu, Ismailcem B. Arpinar, Amit P.Sheth, Krys J. Kochut, "Security for the METEOR Workflow Management System", Large Scale Distributed Information Systems Lab (LSDIS), Department of Computer Science, the University of http://LSDIS.cs.uga.edu

[56] Reid, J., Cheong, I., Henricksen, M., Smith, J.: A Novel Use of RBAC to Protect Privacy in Distributed HealthCare Information Systems. In: Eighth Australasian Conference on Information Security and Privacy (ACISP 2003), (2003)

[57] Zhang, L., Ahn, G., Chu, B, A role-based delegation framework for healthcare information systems. In: The Seventh ACM Symposium on Access Control Models and Technologies (SACMAT'02), (2002)

[58] Mavridis, I., Pangalos, G., Khair, M.: eMEDAC: role-based access control supporting discretionary and mandatory features, in: Proceedings of 13th IFIP WG 11.3 Working Conference on Database Security, Seattle, WA, USA, 25-28, pp. 55-63 (1999)

[59] William T, Gail-Joon A, Tanusree P, Seng-Phil H, "Access Control in Collaborative Systems", ACM Computing Surveys, Vol. 37, No. 1, March 2005, pp.29-41

[60] Randike G., NEHTA B., Tony S: Privacy Oriented Access Control for Electronic Health Records

[61] Dimitris G, Costas L., A security architecture for interconnecting health information systems, Department of Information and Communication Systems Engineering, University of the Aegean, Samos GR-83200, Greece

[62] Etsegenet G, Privacy Aware Pervasive Healthcare System (PAPHS), Addis Ababa university ,2014

[63] Frank B, Ajex H, John H, Rob W, Peter Z, Improving healthcare in Central Africa via OpenMRS,

[64] Webster PC. The rise of open-source electronic health records. Lancet 2011;377:1641-2.

[65] Guy, C., Houghton, MI, SeadM., Providing an Additional Factor for Patient Identification Based on Digital Fingerprint

[66] Mamlin, BW; Biondich, PG; Wolfe, BA; Fraser, H; Jazayeri, D; Allen, C; Miranda, J; Tierney, WM (2006), "Cooking up an open source EMR for developing countries: OpenMRS a recipe for successful collaboration", AMIA Annual Symposium proceedings:

[67] Anderson R, A Security Policy Model for Clinical Information System, IEEE Symposium on Security and Privacy, 1996.

[68] Blobel B. Authorisation and access control for electronic health record systems. Int J Med Inform. 2004 Mar 31.

[69] Gaithersburg I, Electronic medical records and patient privacy. The Healthcare Manager, 2000

[70] AHIMA. "Privacy and Security Audits of Electronic Health Information." Journal of AHIMA 88, no.3 (March 2014).

[71] G. Ghinita, P. Karras, P. Kalnis, and N. Mamoulis. Fast Data Anonymization with Low Information Loss. In vldb, 2007.

[72] William S, Cryptography and Network Security-Principles and Practices,3rd Edition, Pearson Education Asia, 2003.

Appendices

Appendix A: Questionnaire

Dear Participants

I am currently pursuing Msc. research at Addis Ababa University. A key aim of my research is to explore, investigate and analyze information security and privacy in health information systems, with a particular focus on Black Lion health services. Key research objectives include investigation of the current situation regarding information systems security and privacy in health services, analysis of information security policy and methods to verify their consistency, identification of the main problems and barriers for the information system security and privacy.

I would like your kind contribution in the research process by completing the questionnaire. The data derived from the questionnaires will be used in analyzing patient records used at your workplace. I would also like to stress that all responses will be treated confidentially.

Selemawit Hadush
Addis Ababa University
Email: solhadush.27@gmail.com

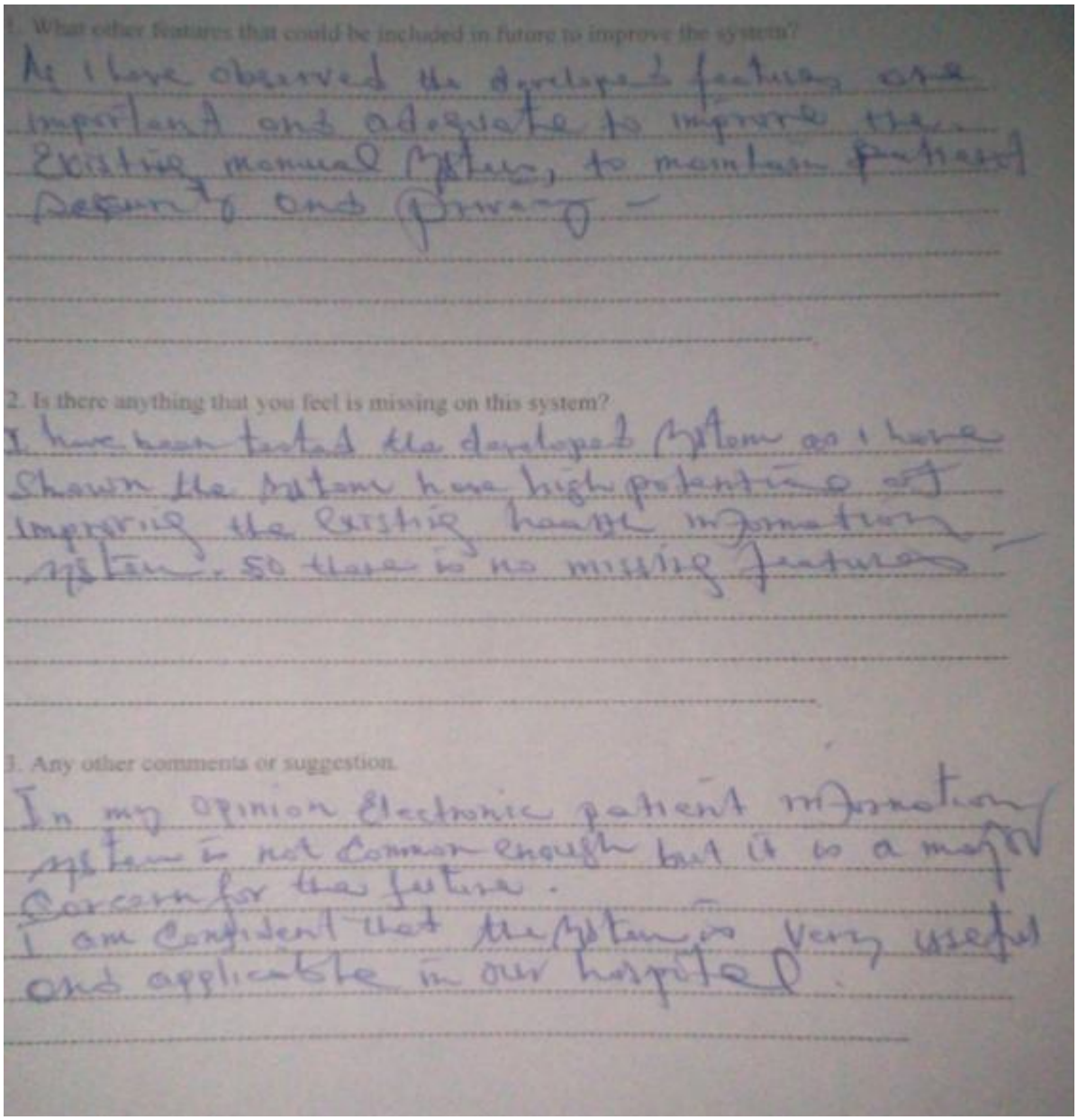
Questions

1. For how long have you held your position in the organization and what does it imply?
2. What are the basic principles for patient identification in your organization?
3. Have the users received any education in information security? What kind of information have they received?
4. How are user registrations managed? How do you manage user accounts? How are the users verified?
5. Are there any other specific tools for authorization, such as Smart cards, biometrical methods etc.? How is unauthorized access to computerized records prevented and how can the protection be improved?
6. What kind of access policy do you use?
7. How do you transfer patient information to other healthcare units? If you use any technical equipment, is the information encrypted in any way? What kind of encryption is being used? If no encryption, how is the information kept confidential?

8. How do you get knowledge about constitutions and other rules and how they can be used in your daily work? From your opinion, are they complete and sufficient?
9. Do you have any problem regarding information security of Electronic Health Record?
10. How is unauthorized access to computerized records prevented?
11. How the data is stored, is there any centralized or decentralized data base system?
12. Does your organization store and process patient records electronically?
13. What kind of policies do you have describing how the security work should be managed? Do you follow any standards or other guidelines?
14. How are policies followed-up and further developed in your organization?
15. In your opinion, what are the positive aspects of information security (in contrast to problems)?
16. In your opinion, would the possibility of availability of needed patient information generate new security problems in the future?
17. What security demands and requirements will then be needed?
18. What needs to be considered for the future, concerning information security and privacy?
19. Do you have access to these electronic records?
20. Do you have any problem regarding information security of Electronic Health Record?
21 . Do you use different access levels such as read, write and delete and can the user change it? In what way can you change recorded information? What access do you have?
22. Are there any parts of the record that you have access to that you feel are not necessary for you to carry out your job?
23. Can you pass your access rights to someone else (if yes, are there any restrictions) Which items of patient medical record you perceive as being confidential and which not?
24. How is unauthorized access to patient records prevented and how can protection against unauthorized access improve?
25. How do you transfer patient information to other healthcare units? Is the information encrypted in any way?
26. How often are you provided back-ups of records?

27. What improvements need to be done with information security and privacy as well as technical improvements?

Appendix B: Sample System Usability Evaluation questions



1. What other features that could be included in future to improve the system?

As I have observed the developed features are important and adequate to improve the existing manual system, to maintain patient confidentiality and privacy.

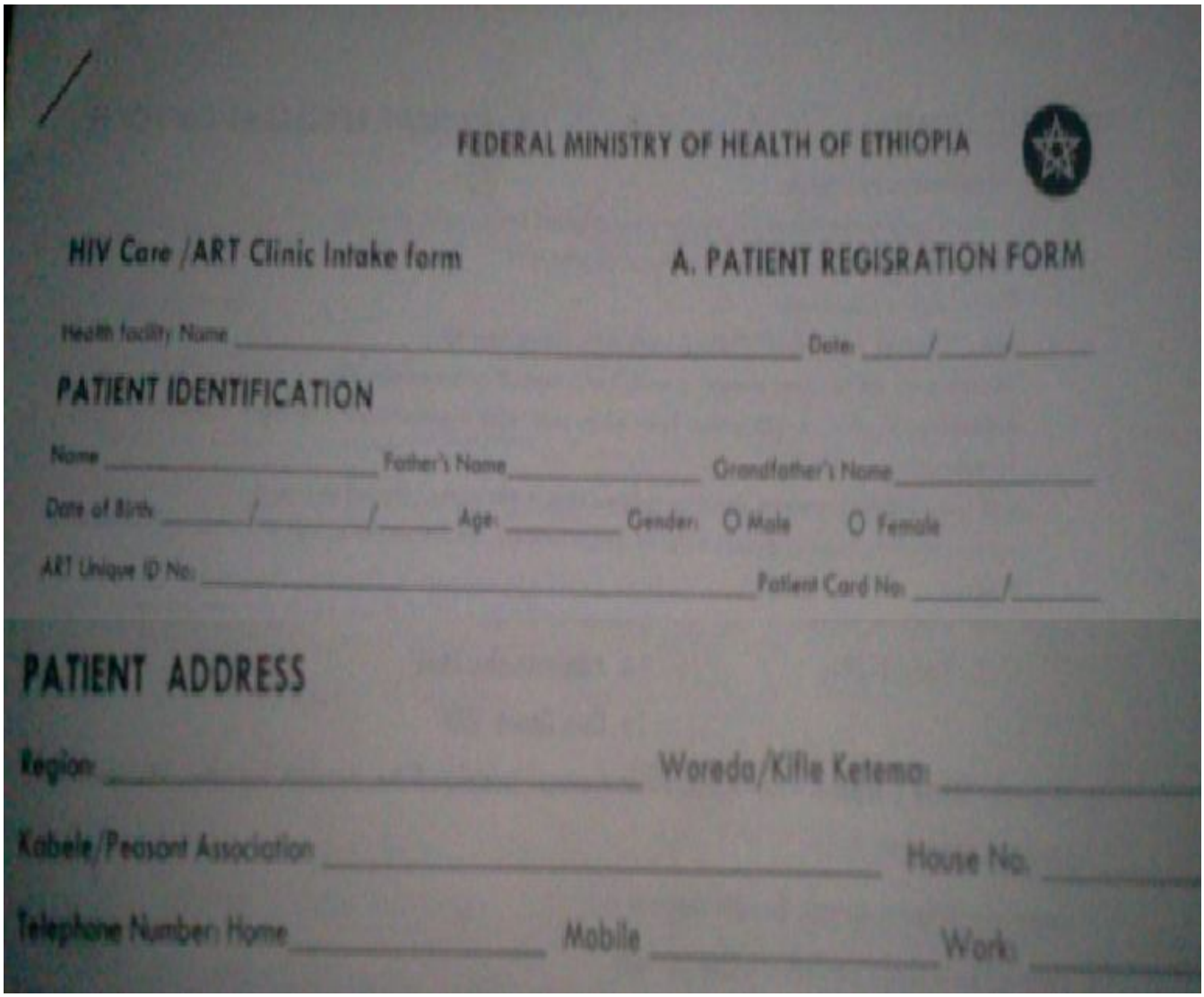
2. Is there anything that you feel is missing on this system?

I have been tested the developed system as I have shown the system have high potential of improving the existing health information system. So there is no missing features.

3. Any other comments or suggestion

In my opinion Electronic patient information system is not common enough but it is a major concern for the future.
I am confident that the system is very useful and applicable in our hospital.

Appendix C: Some Forms of the Black Lion Hospital



FEDERAL MINISTRY OF HEALTH OF ETHIOPIA

HIV Care /ART Clinic Intake form

A. PATIENT REGISRATION FORM

Health facility Name _____ Date: ____/____/____

PATIENT IDENTIFICATION

Name _____ Father's Name _____ Grandfather's Name _____

Date of Birth ____/____/____ Age: _____ Gender: O Male O Female

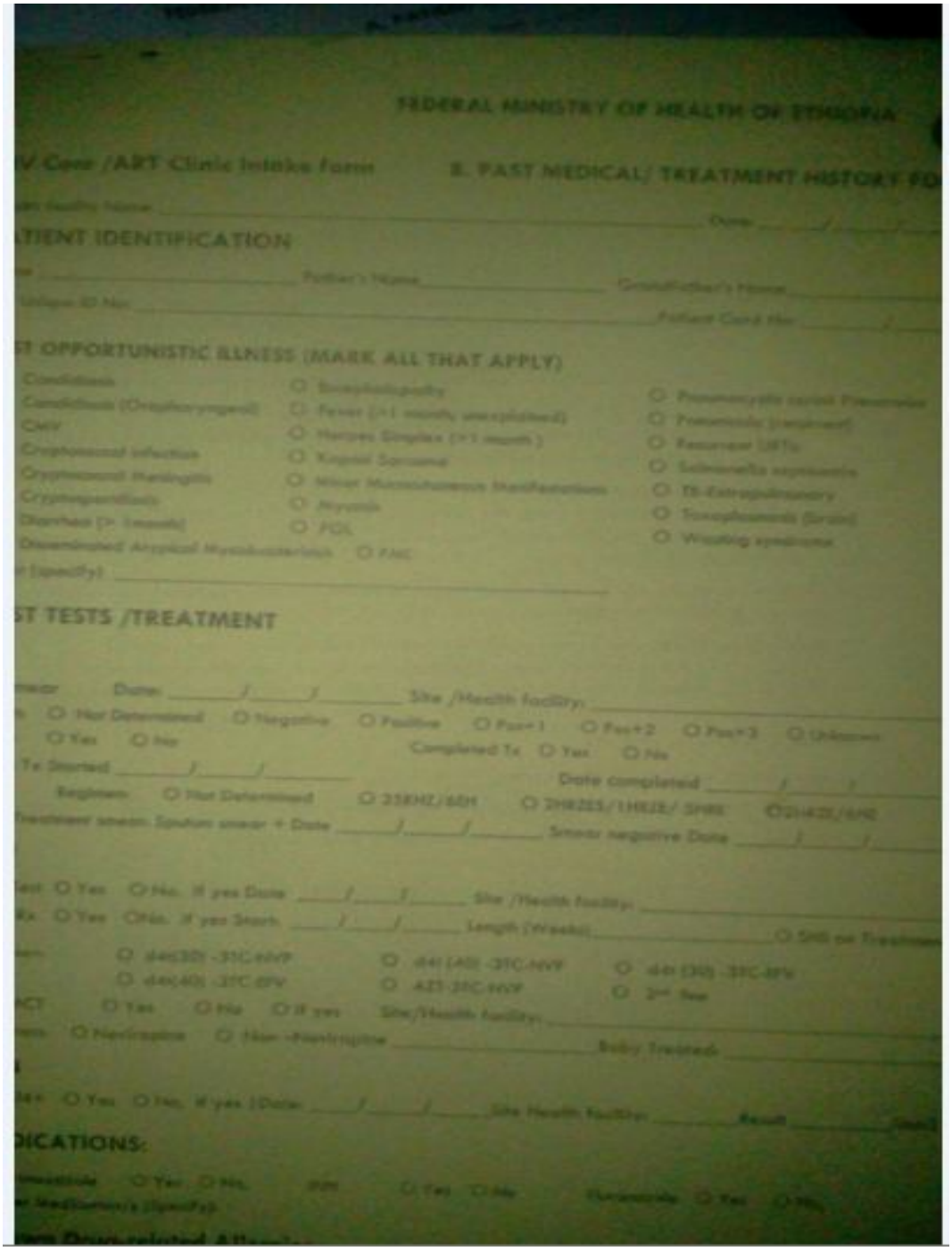
ART Unique ID No: _____ Patient Card No: ____/____

PATIENT ADDRESS

Region: _____ Woreda/Kifle Ketema: _____

Kebele/Peasant Association _____ House No. _____

Telephone Number: Home _____ Mobile _____ Work: _____


FEDERAL MINISTRY OF HEALTH OF ETHIOPIA
V Care /ART Clinic Intake form
II. PAST MEDICAL/ TREATMENT HISTORY FO
TIENT IDENTIFICATION
T OPPORTUNISTIC ILLNESS (MARK ALL THAT APPLY)
ST TESTS /TREATMENT
DICATIONS:

Declaration

I declare that this thesis is my original work and has not been presented for degree in any other university, and that all sources of material used for the thesis have been acknowledged.

Declared by:

Name: Selemawit Hadush

Signature: _____

Date _____

Confirmed by advisor:

Name: Dr.Dejene Ejigu (PhD)

Signature: _____

Date _____

Name: Berhanu Borena

Signature: _____

Date _____

Place and date of submission: Addis Ababa University, April, 2015