CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

The paper-based health records currently in use may generate an extensive paper trail. There is consequently a great interest in moving from paper-based health records to Electronic Health Records (EHRs). These efforts are principally being made by independent organization. Many governments rely on integrated EHRs because of the benefits expected from them. One example of this interest is that of the US government. In 2004, the US President decided that the majority of Americans would be connected to EHRs by 2014 (Hesse et al., 2010).

However, the advances in Information and Communications Technologies (ICT) have led to a situation in which patients' health data are confronting new security and privacy threats. The three fundamental security goals are Confidentiality, Integrity and Availability (CIA) (Rabi et al., 2011). The protection and security of personal information is critical in the health sector, and it is thus necessary to ensure the CIA of personal health information (ISO, 2012).

Therefore, today, the big challenge is how to maintain integrity, security and availability of this information while dealing with medical commercials, patients, and the social pressures for information sharing versus privacy. The challenge begins with restricted rules, enforceable policies, procedures and guidelines, and is followed by technical system solutions that have data security issues (Murtaza, 2012).

Security defects in some of these systems could cause the disclosure of information to unauthorized persons or companies, and health data therefore need protection against

manipulations, unauthorized accesses and abuses, which includes taking into account privacy, trustworthiness, authentication, responsibility and availability issues (Fernandez-Aleman et al., 2013).

Therefore, there is a real concern about both people's and entities' access levels to patients' EHRs or also known as Electronic Medical Records (EMRs). A patient's EMR might be fragmented and accessible from several sites (by visiting different doctors' offices, hospitals, providers and others). The aim of this research is to design and implement a prototype of Hospital Management System (HMS) that maintain privacy and security of patients' data. The system includes some of the industry best practices to increase security of the system such as encryption of the patient database file, Role-Based Access and Logging. The integrity of health information must therefore be protected to ensure patients' safety in order to preserve their privacy during the use of EMRs.

1.2 BACKGROUND OF THE RESEARCH

Patient privacy is a major issue for today's healthcare providers. Safeguarding the confidentiality, integrity, and availability of patient information is no longer a goal, it is a legal requirement. This research have developed certain safeguards in the Hospital Management System (HMS) prototype as follows:

- Introduced a log-on process to identify each user of the system where the administrator can grant privilege access for each user.
- Allows the supervisor and the physician to create and update the patient's medical record.
- View a record by the supervisor of the patient and the doctor.

- The use of medical records for each patient for doctor follow-up.
- Allows the doctor to prescribe drugs for a patient.
- Allows the administrator to create and modify new employees to the list of system operators.
- Allows the patient to make an appointment online.
- Showcase the history of the patient through medical reports.

Researcher also implemented some of the industry best practices to increase security of the HMS:

- Encryption of the patient database file.
- Role-Based Access.
- User logging and activity monitoring.

1.3 PROBLEM STATEMENT

Patients lack trust in Electronic Medical Records (EMRs) or Electronic Health Records (EHRs) feeling that the confidentiality and accuracy of their electronic health information is at risk.

According to Fernadez-Aleman et al. (2013), security and privacy in EHRs can be seriously threatened by hackers, viruses, and worms. Many reports of accidental loss or the theft of sensitive clinical data have appeared in recent years. Knowing the security and privacy features that EHR systems have could be critical if these risks are to be confronted and measures to increase the data protection of EHRs are to be adopted. According to studies carried out in several countries, concerns regarding data security and privacy have appeared.

Certain proposals and solutions were developed to improve security and privacy of EHRs, among them are using the symmetric encryption standard of AES algorithm and pseudonym generation systems dual-pass and proposed a hybrid security model that is the basis of a combination of local and distributed models because each health institution has a security system, an access right management and privacy protection policies according to user role (Elger et al., 2010).

EHRs data and metadata are encrypted using Attribute-Based Encryption (ABE) scheme that uses public and private keys. These keys are managed by Trusted Authority (TA), which can access all encrypted EHRs. The safe keyword search is permitted by an encrypted scheme, PEKS. The data is encrypted using efficient symmetric key cryptography, and the attribute-based encryption is used to make the symmetric keys accessible to authorized users. The private key is communicated to the users via a secure link such as SSL thereby preventing eavesdropper from learning anything about the key (Narayan et al., 2010).

All communications are encrypted with asymmetric encryption algorithm. To ensure transmission security, confidential medical information such as the hashed patient identity H(PI) and the patient's medical record are asymmetrically encrypted with the medical practitioner public key. Patient's anonymity is maintained throughout all communications. Each EHR in a hospital is associated with a patient's ID hash, H(ID), to maintain his/her anonymity. Each health care institution must sign its EHRs to verify their authenticity and integrity (Quantin et al., 2011).

Fernadez-Aleman et al. (2013) stated that EHRs allow structured medical data to be shared between authorized health stakeholders in order to improve the quality of healthcare delivery and to achieve massive savings. In these systems, privacy and

security concerns are tremendously important, since the patient may encounter serious problems if sensitive information is disclosed. Certain healthcare online portals lack some security features to protect patient's data. Table 1.1 showed existing hospital management systems available on the internet, including its advantages and disadvantages from security and privacy aspects.

Table 1.1 Hospital Management Systems Security Features Comparison

Hospital management systems	Security Features	Advantages	Disadvantages
EHS	•Personal smartcard coupled. •Personal identification number.	Allows clinicians to access the electronic health records of their patients by entering the national ID number of the patient.	Verify the identity of e-card holder requires a long time to verify the holder contacted server outside the hospital.
CSMCW	Password policy is enabled.	It can help patients answer questions like - What are my lab results? - What doctor treated me during my stay?	If Universal Password or Advanced Password Rules are not enabled, password policies are not enforced, and passwords on connected systems cannot be reset.
St Mary	Secure Socket Layer (SSL) encryption technology to ensure the integrity and privacy of patient information.	• Fully integrated clinical and financial systems. • Single and multiple (intercompany) facility functionality.	SSL encrypt the information that you send using the server, it takes more server resources than if the information weren't encrypted. The performance difference is only noticeable for web sites with very large numbers of visitors and can be minimized with special hardware.
Carolinas	SSL on its Web site for transmitting information.	• Turns data into meaningful and actionable information. • Simplified user experience/User defined and adoptable/Modular (pay for what you need).	The patient can edit their own the medical file, including medical data because the medical data file is encrypted as only uses encryption to exchange data outside of the organization and not inside.
VorroHealth	• Cookies to log IP addresses and browser information for the purposes of system administration and user functionality. • The system has a tracking feature to log user activity.	•Willing and able to integrate with any System. •Providers own and have immediate access to their data.	Cookies really irritating when personal data is linked to the user's surfing activities – all of this available because the user once entered his name & address, etc., via an input form on a website. This creates a reusable profile of that user, which can be exploited by others without permission.
iCure	SSL encryption technology to ensure the integrity and privacy of patient information.	Contains a registration form, normal pages access speed and all the features are accessible from the main page.	There is no staff list which is a big handicap for a health management website. The interface design is not attractive; there is no treatments list and no patient's file.
Osoft	SSL encryption technology to ensure the integrity and privacy of patient information.	This web portal contains appointment form with attractive design and good pages access speed, all features are accessible.	Lacks of staff list implementation, registration form, treatments list and patient's file.
CMA	SSL encryption technology to ensure the integrity and privacy of patient information.	This web portal contains appointment form, it is well designed and the speed to access pages is acceptable, all features are accessible and maintains a staff list.	This web portal lacks on providing registration form and it does not maintain a patient's file.

It can be seen from Table 1.1 that it is very important to ensure the privacy and security of health information. In addition, when breaches of health information occur, they can have serious consequences for the organization, including reputation and financial harm or harm to patients. Poor privacy and security practices heighten the vulnerability of patient information in health information system, increasing the risk of successful cyber-attack. To help cultivate patients' trust, a Health Management System should:

- Maintain accurate information in patients' records,
- Ensure patients have a way to request electronic access to their medical record.
- Carefully handle patients' health information to protect their privacy.
- Ensure patients' health information is accessible to authorized representatives only.

As the EMR are exchanged over many departments in the same health care organization, the probability of losing the privacy of the patient is very high. So, researcher proposed using the Triple DES algorithm to encrypt the whole patient record to maintain security and privacy of the patient record.

1.4 RESEARCH OBJECTIVES

The Research Objectives (RO) for this research are as below:

RO1: To determine the features and design requirements to develop Hospital Management System (HMS).

RO2: To design and develop HMS with security requirements against unauthorized access to Electronic Medical Records (EMRs).

RO3: To evaluate the effectiveness HMS implementation.

1.5 RESEARCH QUESTIONS

The Research Questions (RQ) for this research are as below:

RQ1: How to determine the features and design requirements to develop Hospital Management System (HMS)?

RQ2: How to design and develop HMS with security requirements against unauthorized access to Electronic Medical Records (EMRs) for a hospital?

RQ3: How to evaluate the effectiveness of HMS implementation?

1.6 RESEARCH SCOPE

This research scope is to develop a secured prototype of Hospital Management System (HMS) which includes safeguards to protect patient's records.

The following functions in the system for patients, doctors and system administrator:

- Logon process can identify each user including administrator and grant access to the system.
- To help the supervisor and the physician to create and update the patient's medical record. Record can be viewed by the supervisor of the patient and the doctor.
- Allow the patient to make appointment.
- The administrator can create and modify employee's record in the employee's database.
- The use of a patient's medical record for follow-up treatment by a doctor.
- Allow for a doctor to prescribe the medicine for a patient.
- Showcase the medical report of a patient.

The security and privacy measures in the system:

- Cyphering the clear text data on patient's record.
- Providing audit logging for user's access to the system.
- Maintain a secure login technique to disable user accounts if misused.

1.7 RESEARCH SIGNIFICANCE

There are various steps that healthcare providers must take to guard patients' information in the form of electronic records. It involves privacy and confidentiality of patient's record, and securing patient data from being lost or corrupted. Researcher have reviewed and assessed some of the existing HMS portals and discovered some missing functionalities that were being overcome in researcher's system. A risk analysis framework was also created based on NIST and HIPAA standards to increase security and privacy of EMRs. The system developed in this research is a prototype of secured Hospital Management System (HMS).

1.8 DEFINITION OF TERMS

Terms that are related to researcher's research are explained below:

Electronic Health Records (EHRs) or Electronic Medical Records (EMRs): Is a digital collection of patient health information compiled at one or more meetings in any care delivery setting. A patient's record typically includes patient demographics, progress notes, problems, medication, vital signs, past medical history, immunizations, laboratory data and radiology reports.

Electronic Health Information Exchange (HIE): Is to allow doctors, nurses, pharmacists, other health care providers and patients to appropriately access and securely share a patient's vital medical information electronically-improving the speed, quality, safety and cost of patient care.

Computer Security: Is the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information data, and telecommunications). This definition introduces three key objectives that are at the heart of computer security as shown in Figure 1.1:

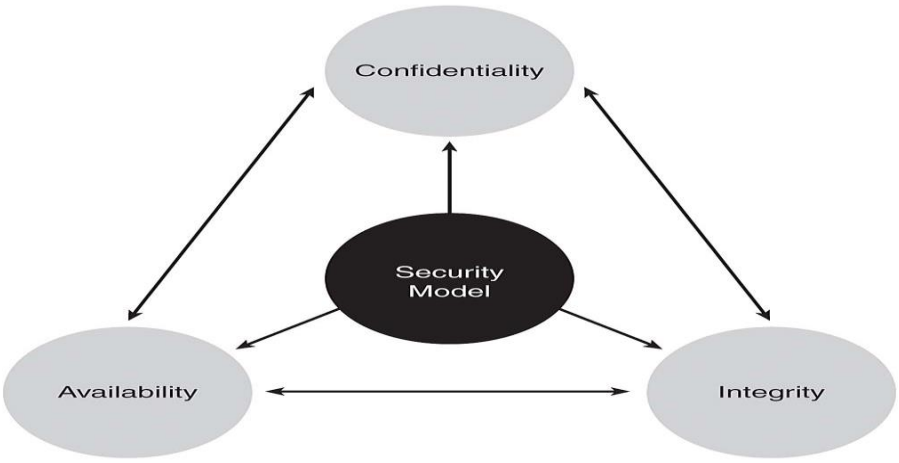

Figure 1.1: CIA Model (Source: ISO, 2012)

- ✓ ***Confidentiality:*** This term covers two related concepts:-

  Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

  Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

- ✓ ***Integrity:*** This term covers two related concepts:-

  Data integrity: Assures that information and programs are changed only in a specified and authorized manner.

  System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

- ✓ ***Availability:*** Assures that systems work promptly and service is not denied to authorize users.

Patient privacy: Patient privacy refers to the right of patients to determine when, how and to what extent their health information is shared with others. It involves maintaining confidentiality and sharing identifying data, known as protected health information only with healthcare providers and related professionals who need it in order to care for the patient.

Encryption: Encryption is a method of converting an original message of regular text into encoded text. The text is encrypted by means of an algorithm (a type of formula). If information is encrypted, there is a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (translate) the text and convert it into plain, comprehensible text.

Triple DES: Triple DES is EDE (encrypt, decrypt, encrypt). The way that it works is that you take three 56-bit keys, and encrypt with K1, decrypt with K2 and encrypt with K3. There are two-key and three-key versions.

1.9 LIMITATION OF THE RESEARCH

In this study, some of the limits were encountered, including the lack of time, the circumstances of war in Libya and the lack of human resources that have enough knowledge about the application of electronic medical records system.

Limitations can be described as follows:

- Administrative obstacles such as routine procedures were delaying the process of transition towards e-health management, a lack of human resources personnel training courses in the field of e-health management, and weak stimulation of physical or mental use of electronic technologies.
- Technical obstacles such as lack of guides describing the mechanisms of EMRs system, lack of accurate and integrated databases, and weak of technology infrastructure required for the change to a computerized form of electronic medical records.
- Human obstacles such as lack of confidence in hospital management staff for electronic transactions, the shortage of specialized personnel in computer operation and maintenance, and weakness of the English language skills for some of the health institutions staff.