Information Technology Security in Healthcare

November 2013

Information Technology Security

in

Healthcare

Edited by

Nurhizam Safie, Ph.D

Health IT Security Forum

www.healthitsecurity.org

SYNOPSIS

Information technology (IT) which being used in our daily work today. In addition, the information technologies (IT) are actually expanding from time to time and it's included in the health world. In the healthcare system, services and structure are basically using IT. Information technology (IT) helps to improve the health sector to make it more efficient and quality. Using the IT Security in healthcare also give another advantage where all the patient information being stored in secure with the help of IT. This book will introduce the readers about the IT Security that helps to secure all the information in the healthcare area.

In chapter one, the reader will be exposed to pseudonymization techniques. In this chapter, readers will understand better about what is pseudonymization and what is the techniques being used. This chapter also tells the readers the purposes of pseudonymization in the health care and its literature review. Besides that, the readers also can find out about privacy-enhancing techniques or in the acronym named PETs. In the second chapter, the writer explains about hospital information system (HIS) which is designed to run and manage the information within the hospital. By using the HIS, the hospitals can operate smoothly and the data can be retrieved in no time. It also goes green systems which it helps to save the paper means help to save trees from extinction. In nowadays, the technologies become more challenging day by day and it cause the confidential data being hacked by irresponsible party. Therefore, HIS helps to secure and prevent it from happening.

In the third chapter, it also touches on the information technology (IT) but in another sector in health society. Health IT (HIT) is an area which it involved IT in designing, developing, creating, usage and maintaining the information specifically in the health care world. The readers will know about what HIT provides to the health world when finishing reading this chapter. This

chapter also will discuss on the studies that are correlated to the HIT worldwide. It also exposes the threaten that Health IT Security being treated. This chapter also highlights recommendation on how to overcome all those threats.

In chapter four, the readers will know about the Security Review Framework which it was proposed to implement in the Hospital Information System. The framework will stress on the purposes of the security review of the systems in the hospitals. Besides that, it also stress on how to identify the security early design flaws on the Software Development Life Cycle (SDLC) and to provide a security or risk profile to make decisions regarding the hospital information systems implementation. The last chapter is about Health IT Security: GNU Health. In the chapter, the readers will know more about the health IT and what the mechanisms being used in the hospitals. Besides that, the readers also will know what is GNU and GNU Health. The readers will be expose to the GNU Health software which is now owned by United Nations.

TABLE OF CONTENTS

LIST OF TABLE

LIST OF FIGURES

INTRODUCTION

The world today is powerfully attached to the information technology (IT) where most of the people on earth are craving to use it. Fundamentally, IT is strongly believed can lighten and assist the humankind in operating their daily activities. The vast adoption of the IT in numerous industries worldwide is enough to show that the importance of IT at the present time. The health industry is one of the many industries which adapt the IT in their practice to improve its quality and efficiency.

The experts acknowledged that by implementing the IT in the health industry does bring the abundant benefits that can help the physicians, patients and hospital staff in doing their work. Widespread use of the IT in the health industry contributes to the improvement of the health care quality, reducing the medical errors, increasing the efficiency of the administrative management, paperless and easing the patients and healthcare professionals' communication. For instance, Shekelle, Morton & Keeler (2006) stated that 'The studies demonstrated improvements in provider performance when clinical information management and decision support tools were made available within an EHR system, particularly when the EHRs had the capacity to store data with high fidelity, to make those data readily accessible, and to help translate them into context-specific information that can empower providers in their work.' In a meantime, Meingast, Roosta & Sastry (2006) indicated that 'electronic patient records and sensor networks for in-home patient monitoring are at the current forefront of new technologies. Paper-based patient records are being put in electronic format enabling patients to access their records via the Internet. Remote patient monitoring is becoming more feasible as specialized sensors can be placed inside homes.

Knowing that health IT plays an important role in the health industry of the studies conducted, however, does not distinguish the fact which it is also has its own risks especially in terms of the security. Dealing with the IT especially with the involvement with the Internet, the security and privacy of the health data are always being questioned. According to A. Buckovich (1999), 'the awareness of privacy issues has grown, too, with the increased use of technology in health care (e.g., electronic medical records), advancements in genetic testing, and news reports on the misuse of information, such as the sale by CVS and Giant of consumers' prescription information to a marketing company.' Applying IT in the health industry has caused the privacy of the health and patient data are endangered due to the various threats which come from the cyber. For example, the health and data patient are being exposed because of the hack threats, fraud, malicious code and data breach. These threats are not only causing the lost of the health and patient data, but also cost the government millions of dollars a year to overcome the lost. Definitely, it is not the good side of the health IT that should be put aside and left out. Various actions have been taken in order to protect the privacy of the health and patient data which are being used throughout the world through the information sharing and exchanging.

The GNU Health and Pseudonymization are the example of the software or application which is invented to protect the health and patient data. It seems that the software can aid the health practitioners to use the health IT securely without worrying about the privacy of the data that is being handled.

Briefly, this book is representing the health information technology and narrowing to its security. There are five chapters in this book and will be focusing on the health IT security and also discussing about implementation of the hospital information system (HIS).

CHAPTER 1

PSEUDONYMIZATION TECHNIQUES FOR PRIVACY STUDY WITH CLINICAL DATA

Yahaya Abd Rahim

ABSTRACT

Privacy is the right of individuals or organizations to determine how their data or information being shared with others people. Privacy is also a very complex topic that touches legal, social and technical issues. Day by day, the need in managing and handling large amount of data and information of the patients have risen in legal and ethical challenges. First of all, this chapter will begin by giving the meaning of the scientific terms and follow up with types of protection for the healthcare data. Next, the paper will introduce about the purpose of pseudonymization and its literature review. This chapter also introduces and shows on the privacy-enhancing techniques (PETs) and implementation of the privacy-protection problems. Practical approaches on the pseudonymization model for batch data collection are presented. The actual application which has been described the techniques today have proved that there are possible benefits of searching the medicine that innovative privacy-enhancing techniques can provide. Technically, the PETs solutions can unlock lots of valuable data sources, otherwise it will not avail.

1.0 INTRODUCTION

In this vast world, we can find many types of organizations by just looking at their name and each of the organizations have data or information to keep from specifics group or

individuals. This kind of data or information can be in privacy and public type. For example, there are organizations about the law firms, schools, universities and even the communities itself have their own organizations. This included the hospital organizations which have the largest operation in managing and handling the data or the information of the patients. Proper techniques are needed in managing the data to avoid inaccuracy and misplaced of information.

Besides that, organizations like the hospitals, clinics or pharmacies have vast amounts of personal data which it had been collected, stored and processed. They have interests in releasing the information and data which they have found from the sources they have collected. They intend to share these data because it can be benefits for other researchers or other public purposes. However, most of the data have sensitive natures for example the medical data, the disease and the patients' name. Although the data generally used for the benefit of the community, but still it can be easily abused by malicious people.

Incidents that occur are frequently reported in the public media, but what concern the patients is how proper treatments of the sensitive data. People tend to become more apprehensive when their personal healthcare-related data are at stake, mainly because they can easily imagine the motives for abusing and assessing and even more about its impact. In the recent incidents, where an outsourced transcriber threatened to disclose all medical records she had processed form one of United State (US) hospital clearly illustrate that the threat to privacy is genuine. Public authorities are also aware of these repercussions, and they are putting extensive effort into controlling the privacy of protection legislation. Nowadays, we can't deny that privacy protection directly gives impacts to the personal well-being as well as society as a whole. Indeed, some go as far as to believe that failure to protect privacy might lead to our ruin**.** Privacy is in fact recognized as a fundamental human right.

Until now, in Malaysia not a single organization pays careful attention to the requirement of obtaining the informed consent from subjects. Because of that, most of the hospital or clinic very cautions in assessing their information because they knew the impact of the information enclosed are very complex. Thus, a real danger that informed consent is rather an ill-informed consent. Research ethics and security guidelines demand research units to divert more resources, time for privacy and identity protection. However, the burdensome requirements governing the transmission of medical information could unnecessarily discourage the research. Well-intentioned privacy laws should not clash with the legitimate use of information when clearly to the public's benefit.

Protecting human rights for example like privacy while maximizing research productivity is one of the coming challenges. A first step towards this goal is the research and implementation of technical solutions to the privacy problem. Privacy-enhancing techniques or technologies (PETs) should be provided with to unlock invaluable data sources for the benefit of society without endangering individual privacy.

This paper will introduce the readers the purpose of pseudonymization techniques to the hospitals, clinics and pharmacies. Furthermore, this paper will touch about the pseudonymization techniques which can help to secure the data from anonymous. Lastly, this paper also focuses on the possible use of privacy enhancing techniques in the context of research and statistics for health care.

1.1 SCIENTIFIC TERMS

Pseudonymous

Cambridge Dictionaries Online stated that “Pseudonymous is a name that person, such as a writer uses, instead of their real name, especially in their work.” Based on Oxford Dictionaries Online, the meaning of pseudonymous is writing or written under a false name. In other means, pseudonymous referred to a nickname or a symbol or coding that symbolize to that person or thing.

Pseudonymization Techniques

Based on Wikipedia, the meaning of pseudonymization is a procedure by which the most identifying fields within a data record are replaced by one or more artificial. It is a method or procedure to obtain and identify the data when the data actually have been replaced by another name or by symbol or by code.

Electronic health records (EHRs)

Based on CMS.Gov, an electronic health record is an electronic version of a patient medical history, that is maintained by the provider over time and may include all of the key administrative clinical data relevant to the person care under a particular provider, including demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports.

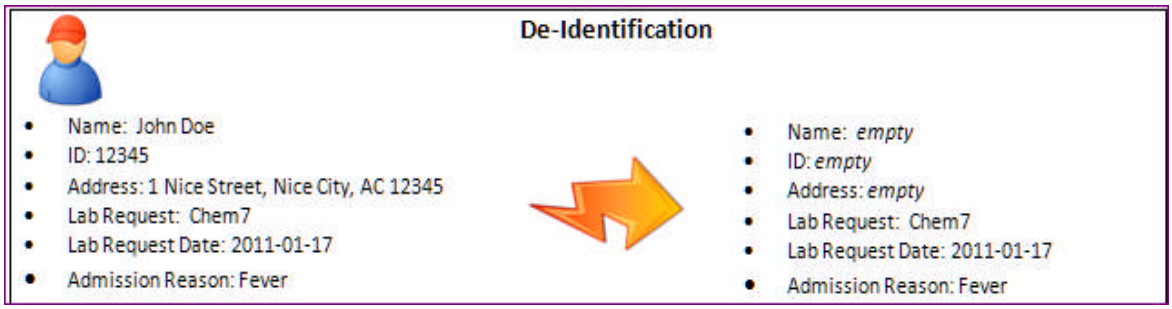
National Health Service (NHS)

Based on Wikipedia, National Health Service may refer to one or more of the four publicly funded healthcare system within the United Kingdom. The systems are primarily funded through general taxation rather than requiring private insurance payment. This service provide a comprehensive range of health services, the vast majority of which are free at point of use for the residents in the United Kingdom.

1.2 TYPES OF PROTECTION FOR HEALTHCARE DATA

- De-Identification or Anonymization

Figure 1.1 : The de-Identification graphic



It is a term for removing or covering the protected information. In another meaning, the de-identification route remove the identifiers of the patients from the data set and it make the information cannot be retrieved to the owner. In healthcare information context, de-identification occurs when all identifiers such as the name, IDs, address, phone numbers and etc. were removed from the information set. In this way, patients' information or identity was protected while most of the data remain and available for sharing with other people, organizations, statical analysis or related uses. The aim of de-identification is to obscure the identifiable data items within the persons records sufficiently that the risk of potential identification of the subject or a person's record is minimized to acceptable levels, this will provide effective anonymization. Although the risk of identification cannot be fully removed

this can be minimized with the use of multiple pseudonym. De-identified data should still be used within a secure environment with staff access on a need to know basis.

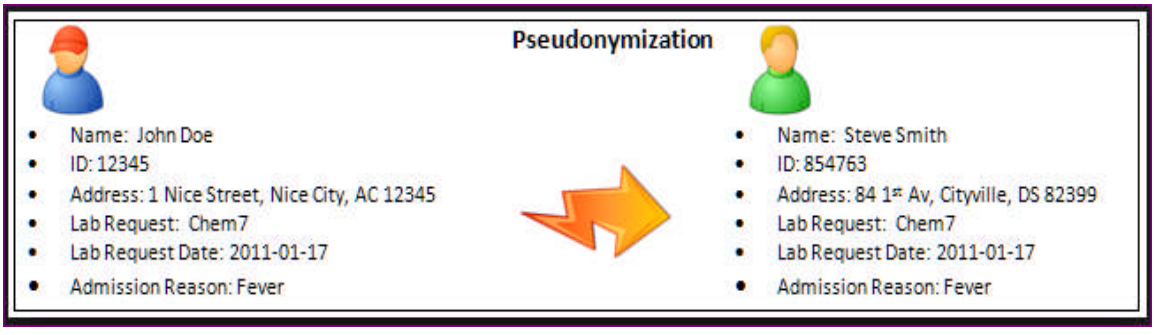
De-identification can be achieved by:

- Removing patient identifiers;
- The use of identifier ranges, for example; value ranges instead of age;
- By using a pseudonym.

If patient data is required the National Health Service (NHS) number is the most secure form of identifiable data. The NHS number should be included within all patient records and documentation in line with the current Connecting for Health NHS number campaign. However, in Malaysia, there is no existence of NHS so the data will be kept in the organization itself.

- Pseudonymization

Figure 1.2 : The pseudonymization graphic

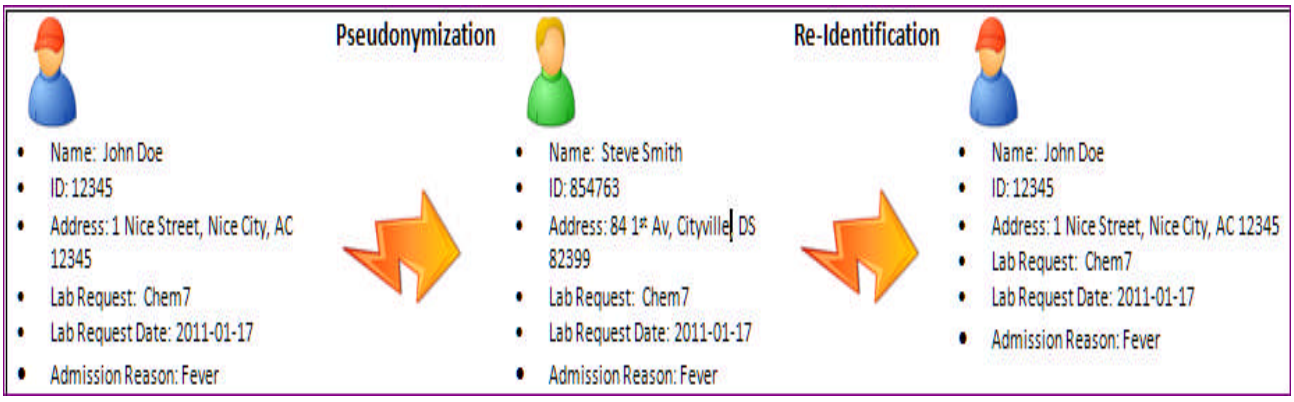


Pseudonymization is a division of the anonymization. Also known as de-identification, is the process involved to enable the National Health Service (NHS)

organisations to undertake secondary use of patient data in a legal, safe and secure manner. Pseudonymisation involves the removing of identifiers from patient data so that a patient/service user may not be identified. However where multiple sets of data are used, links should be enabled so that it is possible to analyse data sets and trends over time. The process of pseudonymization is replacing the data-element identifiers with a new identifiers so the subject will completely be replaced with a new subject. After the substitution, it is no longer possible to link the subject with the data set. When pseudonymization techniques are consistently applied, the same pseudonym is provided for individual patients across different data sets and over time. This allows the linking of data sets and other information. In healthcare context, we can 'pseudonymize' the patient information by replacing patient-identifying data with unrelated data and the result is a new profile for the same patient. The data continuing look complete and the personal data of the patient remain protected.

- Re-identification

Figure 1.3 : The re-identification graphic



Re-identification is to identify the identity of the data. Re-identification is a process to restore the initial information and data to the pseudonymiztion data set. To re-identify the data, the users would need to use a series of reversing the map structure and construct it as the data has been pseudonymized. There are few cases that need to re-identification. For example, the pseudonymized data has send to external system for processing and once the process completed, the information would be re-identified and pushed into the correct patient file.

1.3 PURPOSE OF PSEUDONYMIZATION TECHNIQUES

E-health enables the sharing of patient-related data whenever and wherever it necessary. Electronic health records (EHRs) promise to improve communication between the health care providers so it leads to better quality of patients' treatment and reduce the costs. However, patient information is highly sensitive has made a promising goal for the attackers and have been demanded by the insurance companies and their employers is increasing social and political pressure regarding the prevention of health data misuse. This work addresses the problem and introduced us a new methodology that will protect the health records from unauthorized access and lets the patients as the data owner to decide who the authorized persons. For an example, the patient chooses a person who he or she close to share their health information. Therefore, the methodology prevents data disclosure that negatively influences the patient's life by being denied health insurance or employment. It is also a requirement for the organization to respect people’s private lives unless there is a lawful exemption to the Human Rights requirements and that information obtained in confidence should not normally be used in an identifiable form without the permission of the service user concerned.

1.4 PRIVACY ENCHANCING TECHNIQUES

Privacy enhancing techniques (PETs) are a very hot topic that involving the privacy protection of data. PETs are the huge volumes of data containing sensitive information and privacy are being collected and stored by various of sensors and monitoring systems, auditing systems and etc. Need practical approaches based on two different pseudonymization models, both are from the batch and the interactive data collection and exchange, are described and analyzed.

There are many situations in which privacy can be an issue. Until now many research covers many different areas such as the following:

- Anonymous communication (anonymous remailers, anonymous surfing, etc.)
- Anonymous transactions
- Anonymous publication and storage
- Anonymous credentials
- Anonymity in files and databases

In PETs, it uses pseudonyms. The reason is to hide the real identity of a user by using a bogus identity. Pseudonyms prevent providers from linking isolated transaction to a certain user. The benefits using pseudonyms is that the information such as the patient profile cannot be used

by the third party to link pseudonyms. By focusing on medical applications, in which privacy issues were raised by the information content of the stored data so the paper was discussed in it. Privacy-enhancing techniques for privacy protection within databases help us to protect the privacy of a subject of a database record like person records or organization records that listed in the database. Simply put, these privacy-enhancing techniques allow storing relevant and useful information in a way that no one can ever find out, who the information is actually about. Lists are some of the examples of these techniques are (non exhaustive list):

- ‘‘Hard” de-identification of the owner of the data;
- Various types of anonymization and/or pseudonymization;
- Privacy risk assessment techniques;
- Controlled database alteration (modification, swapping or deletion of data);
- Data flow segmentation;

Today, privacy-enhancing technique technology has already proven its usefulness for privacy protection in marketing and research data collected in United State **[5]** and even in Malaysia or other Asian countries like Singapore, Japan and etc, the (PETs) is growing up parallel with the country's urbanization. However in this paper, our focus with the lies on implementation of pseudonymization techniques, and complementary PETs enhancing with the clinical environment in Malaysia country; and our experiment is one of the public hospitals, in south city.

1.5 PSEUDONYMIZATION TECHNIQUES

Pseudonymization is referring to privacy-enhancing techniques (PETs) and the methods that being used to replace the true (nominative) identities of individuals or organizations in the databases by pseudo-identities (pseudo-IDs) or in other meaning another name or nickname which it cannot be linked directly to their corresponding nominative identities. With this technique, the data that contain patients' information which are identifiers and ''payload data" (non-identifying data) are being separated. The pseudonymization process will translate the given identifiers into a pseudo-ID by using a secure, dynamic and preferably irreversible cryptographic techniques (the identifier transformation process should not be performed with translation tables). For an observer, the resulting pseudo-IDs are thus represented by complete random selections of characters. This transformation can be implemented differently according to the project requirements.

Pseudonymization can:

- always map a given identifier with the same pseudo-ID;
- map a given identifier with a different pseudo-ID;
- time-dependant (e.g. always varying or changing over specified time intervals);
- location-dependant (e.g. when changing the data comes from different places);
- content-dependant (e.g. changing according to the content);

Pseudonymization is the use of data collection where large amounts of data from different sources were gathered for statistical processing and data mining for example the research studies. In contrast, horizontal types of data exchange (for direct care), vertical communication in the context of disease management studies and other research does not require identities. This is because the pseudonymization will help to find the solutions. It is a powerful and flexible tool

for privacy protection in the databases, which it able to reconcile the two following conflict requirements which are the adequate protection of individuals and he organizations with respect to their identity and privacy, and the second is the possibility of linking data associated with the same data subject (through the pseudo-IDs) irrespective of the collection time and place.

However, the uses of pseudonymization technology was not as straight forward as suggested because of the flexibility. When using the pseudonymization technology with careless it could lead to misconduct of privacy protection. The danger mainly lies within the division of identifiers and the payload. The important things that the users should alert us before they precede this process, they have to make sure the payload data does not contain any fields that could lead to indirect re-identification on content, not on identifiers. Careful privacy assessment is the key to having a good privacy protection through pseudonymization. Privacy gauging or privacy risk assessment will measure the risk of a subject which in a ‘‘privacy protected” database if they can be re-identified the subject without cooperation or against the subject will. It consists in measuring all the possibilities of a data subject could be re-identified using the information that is available (hidden) in the database. If the re-identification have small risk , the better and strong the privacy of the subject listed in that database would be protected. Conducting a privacy analysis was a difficult task but at this point, not a single measure for database privacy was fully satisfied with it and this matter is still a hot topic in scientific communities. However, extensive research, mainly conducted by statisticians (area of statistical databases, etc.) and computer scientists such as the data miners or security experts are making significant progress.

From our literature view, by using the privacy risk assessment techniques, pseudonymization performance can be guaranteed. The data collection models were used to estimate the risk level for re-identification by attackers (a priori risk assessment). It also approximates on how the data should be separated (identifiers versus payload), filtered (removal of information) and transformed (transforming payload information in order to make it less identifying) which it subsequently determined on the basis of these results. This means, the fact in that one of the uses of privacy risk assessment techniques is to determine correct configuration of PETs.

Many more aspects of the pseudonymization process are closely linked and key to ensuring optimum privacy protection, as for example, the location of the identifier and payload processing, the number of steps in which the pseudonymization is performed.

1.6 PSEUDONYMIZATION IMPLEMENTATIONS

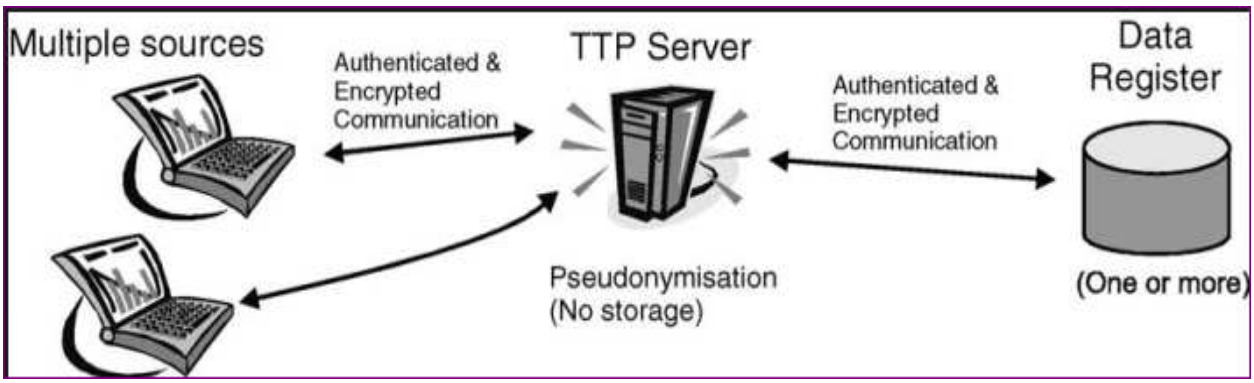
The pseudonymization as described above provides privacy protection for data collection for research and market studies. It also can be used in organizations especially in clinical, pharmacies and hospitals.

Two logical entities involved in handling the data are as follows

1. The data suppliers or ‘sources’.
2. The data collectors, one or several ‘data registers’ where the pseudonymized data are stored.

Data suppliers typically have access to nominative data (e.g. treating doctors), the data collectors should only have access to anonymous data.

Figure 1.4 : Pseudonymization techniques for privacy enhancing technologies.



In batch data collection, a possible scenario is the use of pseudonymization of the batch data collection. The three interacting entities are shown in the figure above. The difference towards the traditional data collection is the sources such as electronic medical record systems does not necessarily interact directly with the database and vice versa. The communication needed to route through a pseudonymization server (TTP server), where the pseudonymization and the processing of relevant data take place, as required.

Data is gathered and packed at the sources, typically in local databases. An example could be a local patient database which is managed at a clinic. The data is transmitted on a regular basis to the register through the TTP server where it is pseudonymized. The data that can be extracted from the local databases is split into two variables; identities and (screened) payload data according to rules determined during the privacy risk assessment stage. Identifiers are pre-pseudonymized at the source, like a first transformation into pre-pseudo-IDs is performed. The payload data (assessment data) is filtered for indirect identifying data and transformed it to avoid re-identification of the anonymous data. Finally, the pre-pseudo-IDs are encrypted using a public-key scheme for decryption by the TTP server exclusively. The payload data are public-

key encrypted to the register, so that only the register can read the data. Both are then transmitted to the TTP over secure links (authenticated and encrypted).

Full trustworthiness and integrity of the service is thus guaranteed not only by means of policy but also on a technical level. First, because the TTP never actually processes real identities (there is a pre-pseudonymization stage). Second, because although the payload information passes through the TTP server, the latter can neither interpret nor modify the assessment data and to fully trust this data is encrypted for decryption by the final destination (data register) only. As a researcher, we believe and understood that although the pre-pseudonymized information leaving the source no longer contains any real identities, but this does not always guarantee absolute privacy because, as the pre-pseudonymization software is available from many sources, a smart intruder might find a way to map identities with their corresponding pseudo-identities for a 'dictionary attack' by entering known identities and creating a translation table. This technique may be like such an attack can be prevented by use of tamper-proof pseudonymization devices. These are however not yet deployed in real data collection scenarios.

From the previous research, we believe by performing a second transformation in a centrally controlled location for example in the TTP server, optimum security can be offered against such malicious attacks and etc. But as already mentioned there are more advantages to the use of an intermediary party. As the TTP server dynamically con-trols the pseudonymization process, additional privacy protecting functionality can be added like monitoring of incoming identities against such attacks, re-mappings of identifies, data flow segmentation, data source anonymization, etc.

After this second stage, we propose at the TTP in which the pre-pseudonymized identifiers are transformed into the final pseudo-Ids may be by using cryptographic algorithms, both the payload data and the pseudo-Ids are transferred to the register via secure communication. At the register, the data can then be stored and pro-cessed without raising any privacy concerns.

1.7 CONCLUSION

Privacy includes the right of individuals and organizations to determine for themselves on when, how and to what extent information about themselves can be communicated to others. Several types of privacy-enhancing technologies exist that can be used for the correct treatment of sensitive data in medicine, but in this paper we focus that advanced pseudonymization techniques can provide optimal privacy protection of individuals. The research also shows that the privacy-enhancing techniques currently deployed in medical research, which proves that the use of pseudonymization and other innovative privacy enhancing techniques can un-lock valuable data sources, otherwise legally not available.

CHAPTER 2

HOSPITAL INFORMATION SYSTEM (HIS) :

THE IMPLEMENTATION, CHALLENGES AND SECURITY PLANNING

Riza Kurniawan

ABSTRACT

Hospital Information System (HIS) is a system which is designed to run and manage the information within the hospital so that the healthcare personnel can do their work effectively. By installing the Hospital Information System (HIS), the hospital can operate smoothly as the related data are no longer managed manually and surely it will be a great help for them. In this day and age; this computer system has become one of the vital parts in the hospitals and must be given a solemn concern. The unsuccessful of implementing this system in particular hospitals will lead to the insecurity of their administrative and medical information. The more challenging and advanced the technologies these days causing the information that should be confidential could easily be hacked by an irresponsible party. Therefore, this paper will discuss the implementation, challenges and security planning of the HIS in the hospital in order to improve the health and nursing care of patients optimally.

2.0 INTRODUCTION

Hospitals are institutions that always have been busy with the patients, the staff and the health care providers. Therefore, it is very crucial for the hospitals have a system that can organize all the important data so as to ease the health care personnel's works. Hospital Information System (HIS) is a system that can aid the hospital personnel to manage all those data

effectively. This system was introduced in the 1960s and developed as the health care facilities changed. During those days, only the staff used the HIS as for the billing and hospital inventory purposes. Today in modern hospitals, it can be said that hospital information system is used in all clinical, financial and administrative applications.

Basically, HIS is functioned as to manage the data related to the clinic, finance departments, laboratory, nursing, pharmacy and radiotherapy and pathology department. The hospitals that use the HIS have the quick access to the information about the patients' record (demographic, diet plan, medical history), the important data of the hospital finance systems and also the distribution of medications. According to Landolt (2012), patient data need to be better protected because of the data protection laws and because sensitive, personal data should be guaranteed confidentiality, integrity, and availability. The implementation of the HIS can protect this data from being hacked easily and avoid the careless of the healthcare personnel from happening. An effective HIS should be user-friendly and well-informed by the vendors to the health care personals regarding the user-manual. Having an effective HIS in the hospital gives out these advantages; enhances information integrity, reduces transcription errors, reduces duplication of information entries and optimizes report turnaround times.

In this chapter, it will elaborate about the objectives of the implementation of HIS in the hospital. Knowing the objective of implementing the HIS enables the top management of the hospital to realize that how important HIS to be implemented in their hospital. Then, by listing the challenges that might become a threat to the implementation of HIS gives the understanding about weaknesses in the hospital management and the improvement can be made. This paper also explores on the HIS security specification. Briefly, this paper consists of three sections

which are HIS implementation objective, challenges to the implementation of HIS and the HIS security specifications.

2.1 THE OBJECTIVES OF THE HIS IMPLEMENTATION

Before implementing the HIS, it is very important to identify the objectives of the HIS implementation. By doing this, everyone could have a clear understanding about the requirement of HIS implementation in the hospitals. Thus, it will help the hospital management to boost up their services and upgrade their staffs' skills. In short, the general purpose of implementing the HIS is to improve the health and the nursing care to patients optimally. From this general purpose, it can be divided into several specific objectives to ensure that the HIS implementation is guided with the concrete reasons.

2.1.1 Upgrading the Technologies

It is noted that in this modern age, everything has changed rapidly including the healthcare facilities. The evolving of the health care facilities forcing the hospitals to implement the HIS in order to increase their efficiency when dealing with the patients and manage all classified data. Landolt (2012) stated that the growing integration of complex hospital information systems, the widespread use of mobile devices and the increasing amount of communication between health care providers require special attention regarding information security. Hence, the top management of the hospitals should change the conventional way of administrating the hospital into the modern way to be able to compete in globalization.

2.1.2 Increasing Workers Performance

Encouraging the workers to increase their productivity is very important because having the excellent workers would give a positive impact to the hospital performance. This is because they will boost the hospital performance; making the hospital to be the main option among other hospitals by the patients. Implementing HIS in the hospitals can motivate the workers to work practically and improve their performances as they have the tools that can aid them in doing the works. Furthermore, the HIS implementation can also reduce the errors in all aspects of health care. HIS will help the healthcare personnel to minimize the errors as they sometimes tend to be careless when dealing with the data. With the implementation of the HIS in the hospital, the healthcare personnel can rely on the system and they will be more cautious when doing their job as they are trained on using the HIS.

2.1.3 Enhancing the Human Resource Requirement

The human resource department plays a significant role especially in managing the staff and the health care personnel. This department responsible for keeping all the records regarding the employees and establish the employment policies. Their field of works is also covered in maintaining individual employee files and personnel administrative records of the hospital. To facilitate these tasks efficiently, the implementation of the HIS could handle them electronically. For instance, the human resource department in the St Michael's Hospital uses Wiztec HR Management Information System to organize all the files and records. In addition the implementation of the HIS is necessary to keep the records and also protect them.

2.1.4 Reducing Hospital Cost

K. Lee & H. Kwon (2011) concluded that HIS measuring by the information system applications had a relationship with the reduced total cost. This means that implementing the HIS in the hospital can reduce the cost expense. This is because the study shows the application of HIS in particular hospital uses less resource for patient care meaning that they can save the labour cost. Apart from that, the study also implied that adoption of automated notes and records, computerized physician order entry (CPOE), and clinical decision support (CDS) system could lower the hospital admission cost. Here, it is proved that HIS can reduce the hospital cost and for sure it will benefit the hospital in terms of the budget.

2.2 CHALLENGES IN IMPLEMENTING HIS

It is undeniable that the implementation of HIS could bring numerous benefits to the hospital. However, to implement this system in the particular hospital, there must be challenges that could appear due to several reasons. All the challenges that are identified should be given serious attention before the implementation of HIS can be made. This is because if these challenges could not be overcome, then, the implementation of HIS would never happen.

The understanding about computer is still less even in this modern age. This is might due to the inequalities of information exposure in a certain area. When the staff and healthcare personnel do not acquire the knowledge about the computer, then it is hard for them to handle the HIS. That is why the implementation of the HIS in the certain hospitals could not be done as they are not well-inform in computer knowledge.

The implementation of HIS also cannot be completed is because the understanding of the specialized fields of information about business and management roles are still minimal. The less understanding of the specialists in IT field about business and management roles resulting to the difficulties for both parties to cooperate.

It is aware that some of the computer equipment price is high. Therefore, the hospital management feels that it does not bring so many benefits to the hospital when buying the computer equipment. In some hospitals, the budget is spent for developing the health care facilities and they always overlook to upgrade the computer equipment. For instance, they proud to have more advanced tools; CT-scan, Ultrasound 4 dimensions and other equipment that is expensive. As a result, the technology-based archiving and administrative receive less attention from the hospital. This lack of the computer equipment will be a barrier to implementing the HIS in a particular hospital.

Another thing that becomes a challenge to the implementation of the HIS in the hospitals is the developers have less live vision, mission and strategy to convince the hospital to implement the HIS in the hospitals. Moreover, the factor that can be an obstacle is they cannot implement the HIS because of the hospital policies made by the management or the owner of the hospital. Sometimes, the top management of the hospital could not fully understand the requirements of the hospital themselves. That is why a good communication between the high management and lower employee is very vital in order to improve the hospital management and customer services. Apart from that, the hospitals also have less anticipation of changes in the subsystem (clinical and non-clinical services). They still stuck with the traditional way and do not want to change it to the systematic way.

2.2.1. Habits that Threaten the Security of HIS

The implementation of HIS is not just has its own challenges, but HIS security also is threatened by the habits that usually take place in the hospitals. It cannot be denied that those habits are usually made by the hospital staff themselves and also the lack of understanding in using the HIS among them. This is may be because of the developers do not inform the staff properly and the ignorance of the staff and healthcare personnel about the HIS. Besides that, those habits also could cause the failure to the HIS implementation in the hospital as they do not properly using the system as instructed.

2.2.2 Username and Password Storage

This phenomenon doesn't only happen within the hospitals, but also in many companies. It can be seen that in the hospitals, the username and password storage does not handle carefully by them. This is because the username and password storage are affixed on the monitor screen, written in the workbench and clearly written on the bulletin board at the nursing station. These actions are totally insecure as everyone can snitch the username and password easily without anyone notices it. By viewing those two classified information, it will allow the irresponsible party to take the advantage on the careless actions made by the staff and healthcare personnel. For example, they could use the username and password to steal the patients and hospital information for the bad intention.

2.2.3 Provide Username and Password to Others

Providing the username and password to others including the outsiders always happen in the hospital. This irresponsible action of the staff and healthcare personnel mainly because they ask their friends to mark the attendance even they do not come to work (illegal absent), requesting their friends to key in the patient data because they are busy and reluctant to learn the system. Obviously, they do not think about the consequences of doing that or do not know it is wrong actions. Besides that, they trust their colleagues too much and this might cause the information that should not be exposed to others will leak out.

2.2.4 Leaving the Computer Screen Open

Leaving the computer screen open is another habit that often done by the staff and the health care personnel. Sometimes they just left the computer screen open when they have to attend to the patient treatment. They thought that it is okay if they just left it for a while treat the patient but they are wrong. Moreover, they also use the computer for the personal use and they talk to friends and the computer screen is opened. It is very dangerous for them to expose the computer screen open as it will risk all the important data in the computer. Thus, they must aware that the patient data must be protected and kept confidential.

2.2.5 Write down the IP Address of the Server in a Place that is Easy to Read

Normally, in the particular hospital, they have their own server and controlled it by themselves. Every server has its own unique address that used to route information to them. One of the habits that do not clever to do is writing down the IP address of the server in a place that is easy to be read by anyone. This will lead to the exposure of the server hacking by the outsiders.

2.3 KEY SUCCESS IMPLEMENTATION HIS

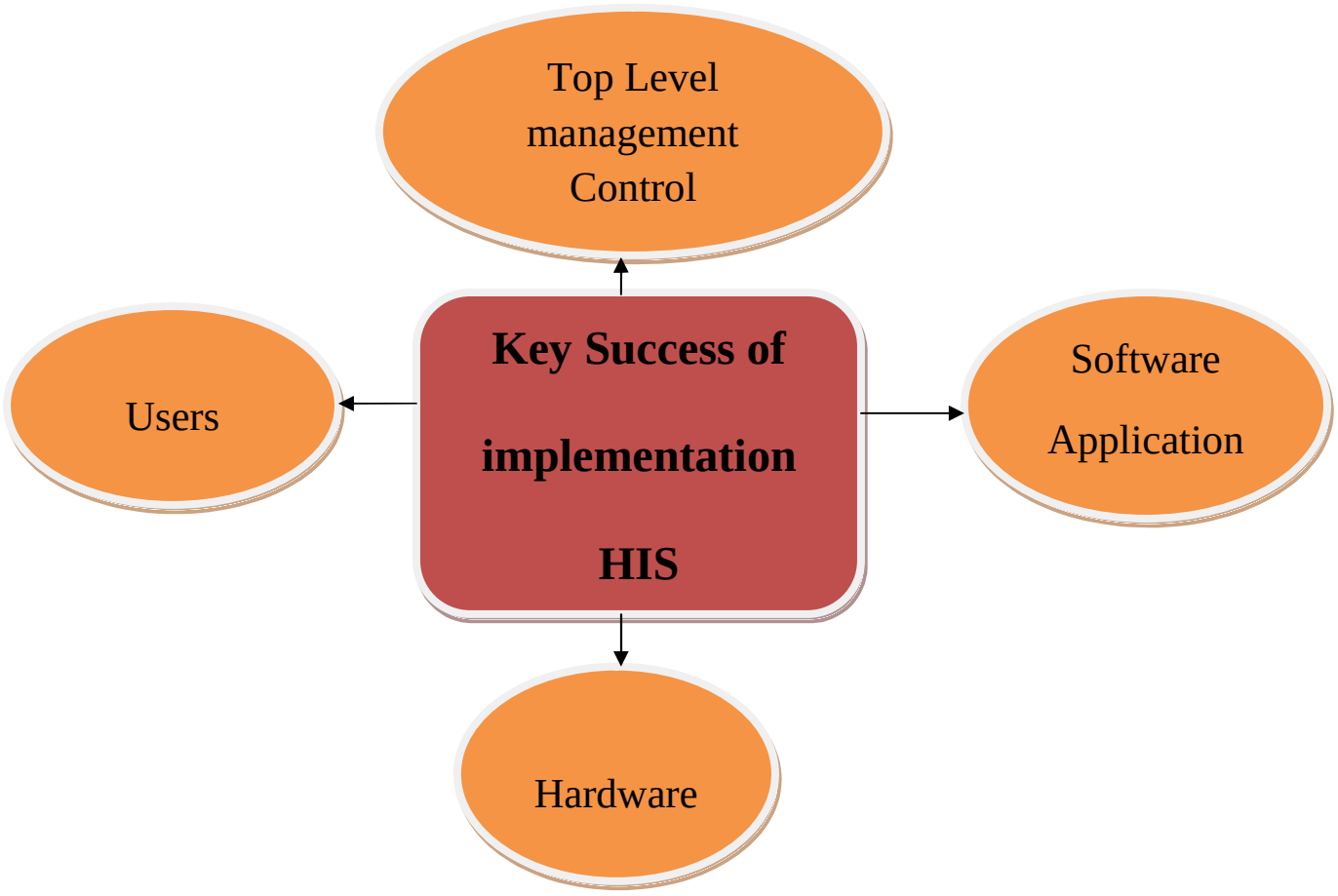


Figure 2.1 : Key to successful implementations HIS

The HIS implementation surely benefit the hospital in many aspects. However, the successful of HIS implementation will not happen if the HIS does not being used effectively. To ensure that the HIS implementation is successful; there are several factors that should be taken by all the parties who will use this system.

2.3.1 Software Application

There are many software applications that provide the Hospital Information System in the market. They offer numerous of services together with the HIS installation that might seem interesting to attract the customer and as a marketing strategy. However, one should bear in a mind that it is very crucial to choose the most suitable software application which suits the needs of the hospital rather than considering the brand and the popularity. The expert who works in the hospital should figure out the needs of the hospital and try to find the best software applications that can fulfill the needs of the hospital.

On top of that, the expert also must ensure that the software application is user-friendly software and not too sophisticated for the users to use it. For example, the Netripples Hospital Management System (HMS) offers a system that can automate all the activities of the hospital mainly in managing the information. This software is specifically designed to be user friendly software. Thus, the system is designed modularly. Integrating modules and adding users allows the flexibility of the user to plan implementation in phases. Besides that, Pflege Portal is also software that easy to be used. It is being used in German for quality assurance (bedsore, decubitus ulcer). It is easy to personalize and it is the web based Hospital Information System that is written in

Perl and tested on MySQL. Advanced Hospital Management System is free software which will help the healthcare personnel to handle almost everything. The program can look after Inpatients, Opd patients, billing, maintain hospital info (ward id, the doctor in charge) and handle the payment.

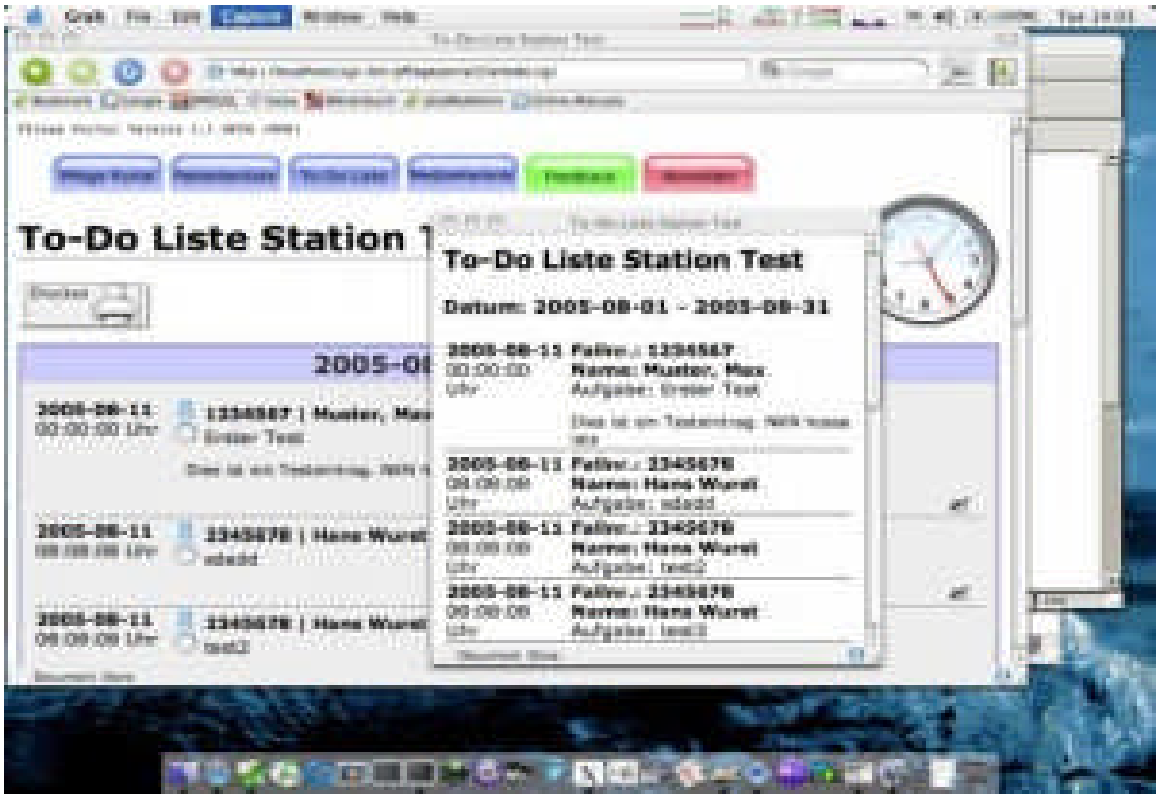
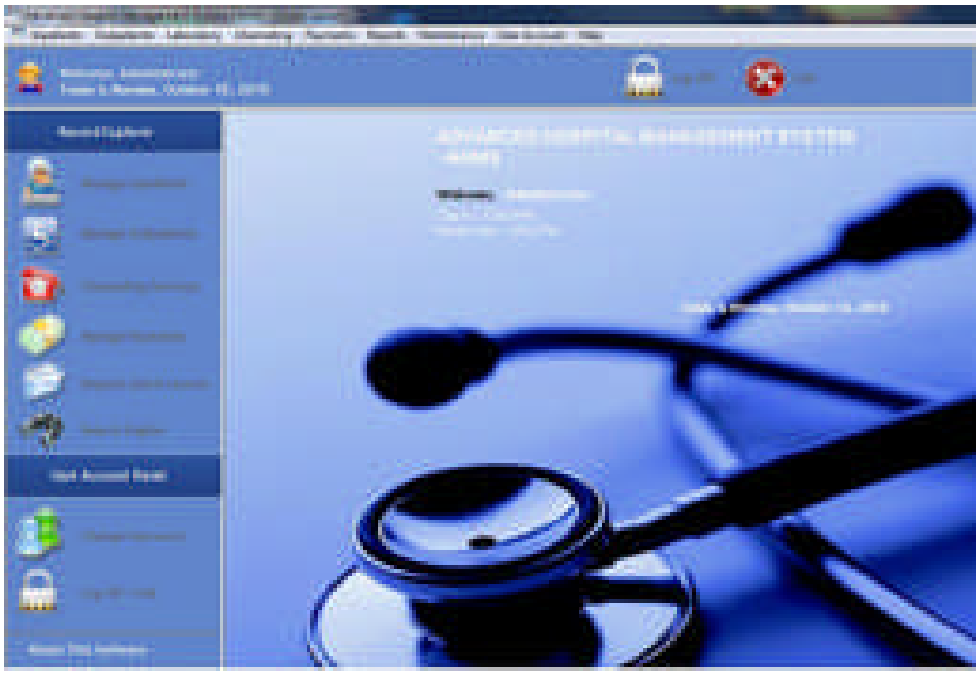


Figure 2.2 : The to do list

Figure 2.3 : Advanced Hospital Management System



2.3.2 Hardware

Before implementing the HIS, it is important to have the sufficient facilities especially the hardware. Upgrading the hardware from the old one to the new one is very vital because the hardware acts as a delivery system for the software solutions. For example, the Random Access Memory (RAM), the storage capability must be upgraded, to have a vivid effect on system performance. Not just that, the storage capacity of the hard disk also needs to be updated as all the software titles and most of the files are stored in it. Besides that, the processor that's been installed in the computer should operate with a high performance. For instance, the latest processors that have a tremendous effect to

computer performance and being talked a lot in a market which are the AMD FX-6300, Intel Core i7-3770K and Intel Core i5.

2.3.3 Users

Another key of success of the HIS implementation is the users. It is noted that the users are the one who will determine whether the HIS implementation is succeeding or not as they use the system. It has no use if the hospital implements the most reliable HIS on the market, but it is not being used optimally. To ensure the users really benefit the HIS implementation, they should be well-trained by the developers on how to use the system. The training should be continually held, to update the users with the changes that happen in the system, so there will be no misunderstanding occurs in the future as they already informed about the changes. By holding this training, the users would be reminded of how to use the system optimally, the do's and don'ts when using the system and their responsibilities in using the system.

2.3.4 Top Level Management Control

The top level management should remind their employees regularly about the responsibilities of using the HIS. Moreover, they also have to control and supervise their employees' activities particularly in anything that interconnected with the data management and the HIS. Supervising and controlling the employees' activities will

facilitate the top management to take an instance action if they found something suspicious on the system.

2.4 HIS SECURITY SPECIFICATIONS

- The Installation of Firewalls and Routers Manageable

  The purpose of the installation of the firewalls and routers manageable is to enable the HIS implementation to be done on the computer's IP routing. A computer with the IP number that gets access to the server can be managed or specified. The firewall and routers work when a firewall detects a DOS attack cut off the DOS attack, and outputs a log indicating an attack, and designates a source IP address of the DOS attack. A filtering command for cutting off an attack is generated in a router, and transmits it to the router. The router discards a packet transmitted from the specified IP address through the filtering operation.

- Authentication Aspect

  The authentication aspect means each user has their own identity (user id) and password with particular different authority in stages accordance with the duties and responsibilities. The authentication works by allowing only the users who have the id and password to get access to the application and the outsiders could not use the application at all. Not just that, these users will only get access to the information and application that are related to their work field and responsibilities. Apart from that, each user must use their own user Id and

password every time they want to get access to the application. By doing this, it can protect the information from circulating around the hospital without any supervision which may lead to the leaking of the information to the public.

- Access Control Aspects

  Every authorized user accesses to the applications, data and information should accordance to their authority. In simpler words, each user can only get access to the certain information that relates to their duties and responsibilities. For example, the nurses are not allowed to access the information from the Human Resources Department as they do not have the authority there and it is out of their field of expertise. Furthermore, to ensure the confidentiality aspect of the system, the process of exchanging data between the server and client is done encrypted (encrypt / decrypt) using the Secure Socket Layer (SSL). Therefore, if there is data in the traffic intercepted by unauthorized persons will not be able to understand the contents. SSL is a protocol that uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer.

- Non Repudiation Aspect

  According to Rouse (2008), non-repudiation is the assurance that someone cannot deny anything. Typically, non-repudiation is when the users cannot deny the

authenticity of their signature on a document or the sending of a message that they originated. For example, if there are any changes in the particular data, the user id, date and the time will be recorded automatically by the application. The data that have been recorded can only be seen by the management department to allow them to track down the one who did it and the time if they found irregularities in the existing data.

- To conform to the Data Integrity

  In order to conform to the data integrity, if there is any change in the data, it should be seen immediately by the other departments that are involved in order to overcome the changes. Thus, to ensure the availability of systems and data (Availability), allows doing the mirroring servers, so if one server crash or malfunction, then there is a backup of the other servers as the mirroring works by copying the server to the other computer.

- Installing the SmartKey or Biometric Authentication

  It is an optional for the hospital whether they want to install the biometric authentication in their computer or not. This is because by installing this system, only the authorize the person who can use the system. R. Mark (2000) stated that Biometrics is the science of identifying a person through the electronic examination of his or her physical characteristics (e.g. fingerprints, voice, or retina patterns). These methods are extraordinarily useful as protections against fraud as well as an impediment to unauthorized electronic access to data

networks. Biometric systems allow only those persons possessing a unique biological characteristic to present themselves as the authentic person in a non-face to face transaction over the telephone or a computer network. One of the biometric developers is Smart Tone, Inc. that authenticates a user of its system without the drawbacks normally associated with biometric characteristics.

2.5 CONCLUSION

In short, it is clear that the HIS implementation is beneficial for the hospital holistically. However, to make the Hospital Management Information System (HIS) implementation accomplish, there are several solutions which must be carried out by the Hospital to solve the problems and the obstacles that hinder the development of Hospital Management Information System (HIS):

- ✓ Provide insight to every member of the organization on the importance of hospital management information system,
- ✓ Provide intensive training to the users of Hospital Information System
- ✓ Provide incentives to all employees who can take advantage if the Hospital Information System works with optimal.
- ✓ Provide education about how important to keep the security system in Hospital Information System.

CHAPTER 3

HEALTH IT SECURITY

Assoc. Prof. Dr. Zuraini Ismail

ABSTRACT

The Information Technology (IT) has become ubiquitous in this present day where everything in this globe attaches to this tremendous creation in a man history. When discussing the implementation of IT in many fields (business, education and administrative), it always emphasizes on how this magic tool helps the man to simplify their work. The wide usage of IT worldwide and its attachment in almost fields, the health industry is not excepted from adopting the IT in its practices. In brief, Health IT (HIT) is an area in which the IT is involved in designing, developing, creating, usage and maintaining the information systems specifically for the healthcare industry. The HIT is purposed in providing a better healthcare to the patients, easing the patients and healthcare provider communication and also reducing the errors and deficiency in the health care practices. This paper will discuss on the studies that are correlated to the HIT worldwide. It emphasizes on the threats that threaten the Health IT Security due to the evolving of IT day by day and it also talks about the IT issues in the HIS. This paper also highlights the recommendation on how to overcome all those threats in order to protect the health IT from any harmful from the outsider.

3.0 INTRODUCTION

Health Information Technology has brought a new environment to the health industry. This new environment change the application of paper-based system to the electronic or digital system which is believed gives a great effect. Health IT consists of several components which are the infrastructure and application. As for the Health IT infrastructure, its vital components are EHR, EMR and PHR. EHR stands for electronic health record which is an official individual digital health records and is shared by some agencies. Electronic medical record or EMR is an individual's health record within the healthcare institution and PHR means a personal health record which is a self-maintained health records. On the other hand, the electronic billing, decision support system and clinical data analyses are the examples of the Health IT application.

The implementation of HIT in the hospitals gives several advantages to the healthcare provider. HIT can improve the information sharing among the health care providers about the therapies, the treatment and the knowledge. Some clinics and hospitals install the software and application that will guide the practitioners in the treatment and diagnosis for the patient. Moreover, the HIT is able to reduce the medical errors and increasing the quality of the health care. This is because some HIT vendors offer patients the ability to keep and manage their personal medical record online whereby those records can be seen by the patient and their doctors. This system will enable the doctors to access the medical history of the patient and help to facilitate coordination of care among different doctors. (M. Herrick, Gorman, & C. Goodman, 2010).

Looking at the vast IT alignment with the health industry, it is signalling that IT plays an important role in helping the healthcare personnel in operating the hospital all day long. It is undeniable that the involvement of the IT in the health industry has been a great aid, however, all

the IT systems are still threatened by the numerous kind of threats from the internet. A. Buckovich (1999) stated that the 'awareness of privacy issues has grown, too, with the increased use of technology in health care (e.g., electronic medical records), advancements in genetic testing, and news reports on the misuse of information, such as the sale by CVS and Giant of consumers' prescription information to a marketing company.'

According to the Internet World Stats Website, until 30th June, 2012, there are 2,405,518,376 internet users worldwide. The Asia represents the highest number of internet users with 44.8% or 7016.7 million users and the least number of internet users is at the Oceania/Australia with 1.0% or 24.3 million internet users. The picture below shows the internet users in the world distribution by world region for the year 2012.

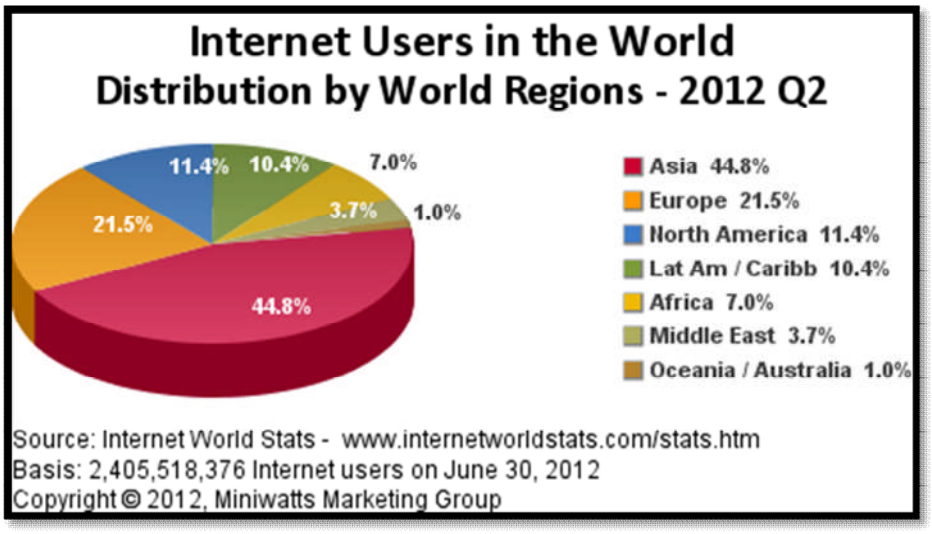


Figure 3.1 : Internet Users in the World Distribution by World Regions.

From to the picture above, it can be concluded that with the growing of internet users' resulting the health IT is exposure to the threats which will endanger the confidentiality of the hospital and patient information. Paper-based systems are not completely private or secure, but

digital systems create new challenges. Blumenthal (2011) emphasized that the media report almost daily breaches in public and private electronic information systems, both health- and non–health-related.

3.1 CYBER THREATS

The cyber threats are the threats that come from the cyber as well as from the technology. For the technology related threats, the threats occur in the computer system and the networks. These threats could cause serious damage to the computer system, network and affecting the privacy of the patient and hospital information.

- Hack Threat

  The health IT is always endangered by the hack threat whether from the hospitals as well as from the outside. The hacker is the one who has the ability to enter the system without being tracked by anyone. The purposes of hacking the system is to steal the information from the system, use the PC as a spam machine and to do a denial of service (DOS) attack on the other computer. Hacking threat is very dangerous because it can cause the important data of the hospitals to be stole especially the data that is correlated with the patients.

- The Fraud

  The fraud is an act of deceiving a person or organization by doing something despicable and claiming a false statement. The fraud in the health IT can happen if the person has the user identity and the password of the computer or application in the hospitals. The person can get access to the hospital and do disgraceful things and the owner of the id and password would be blamed. The image of the hospitals also can be

affected because fraud can use the hospitals' application and ask for money from other organizations or do something that is humiliating the hospitals.

- Malicious Code

The health IT can be threatened by the malicious code. Malicious code is a program that is designed to destroy, to steal information, use up resources on a computer and allows unauthorized access to the computer. The virus, spyware, worm, and Trojan horse are some of the malicious code type. All those malicious codes can be spread via email, infected floppy disks, instant messages, file-sharing services and pop-up ads.

- Denial Service Attack

A denial of service attack is another technology related threats to the health IT. Denial of service attack or DOS is an attempt of making one or more computer to malfunction. Typically, DOS is involved many computers and the attack is done simultaneously. This is due to the modus operation of DOS is by sending the stream of requests to a specific server at the same time. If the server cannot cope with the simultaneous requests, incoming request will be queued and causing the slow response or no response at all. This threat can be very problematic, especially when it causes a large website to be unavailable during the high-traffic time.

- The Harassment

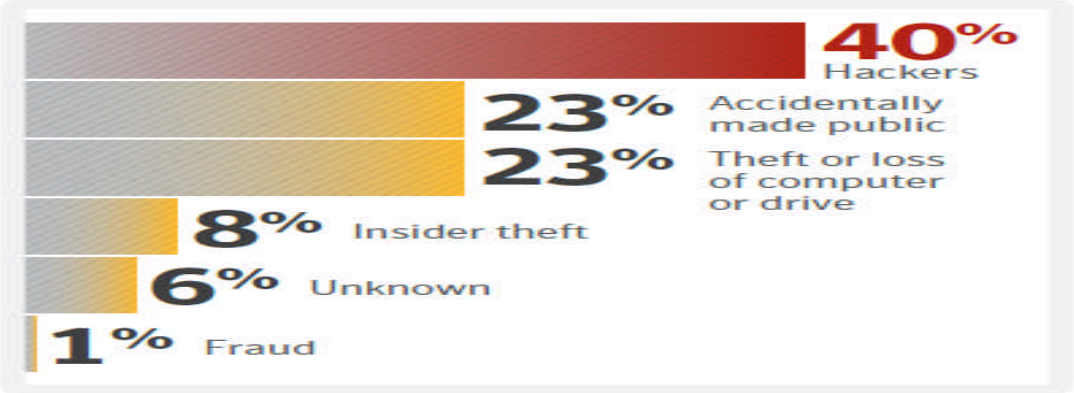
The harassment of the computing also is one of the technology related threat to the health IT. It can be called as harassment when a person uses the computer or the

computer network to act obscene, rude and profane, or make a suggestion on the illegal activity or immoral nature.

- Data Breach

A data breach is a threat that always happens in any organizations and companies. This threat means a confidential and protected data of particular organization are potentially being stolen and viewed by the unauthorized individual to do so. In the hospitals, the data breaches typically happen because the criminals want to steal the personal health information (PHI), personal identifiable information, trade secret or intellectual property. The data breach does not only happen secretly, but if the authorized individual shows the classified data to the unauthorized individual, it is also categorized as a data breach.

Figure 3.2 : The top causes of the data breach in 2012.



Based on the internet threats report in 2012, the healthcare industry has the largest disclosed data breach by the industries with 36%. From this report, it can be concluded that the

data breach is the biggest threat to the health industry. In the same report, the health website placed in the ninth rank on the website exploitation with 1.7%. The results from this report emphasized that the health IT security is always being targeted by the hackers to hack the computer system and the network.

3.2 STUDIES ON HEALTH IT SECURITY

3.2.1 2012 Hospital Security Survey

Perception Solutions for Health Facilities Management (HFM) and the American Society for Healthcare Engineering (ASHE) have conducted a survey at the hospital on June 2012. The objective of the survey was to learn about the trends in the hospital security. The survey showed the result as follows:

- U.S. hospitals have increased security to protect their electronic records.
- More that 90% of hospital respondents and 65% of physician practice respondents conducted a risk analysis.
- Approximately 80 of the respondents reported that their organization shares information with at least one other type of organizations.
- Firewalls and user access controls continue to be most frequently used types of security technology used by healthcare organizations.

In the same survey, Beth Burmahl indicated that to adopt the technologies which will help to upgrade the security system in the hospitals, the hospital security and the information technology (IT) must cooperate closely.

"But adopting technology such as radio-frequency identification (RFID) and digital Internet protocol (IP)-video surveillance systems means hospital security and information technology (IT) departments must work together closely to design, install and maintain the sophisticated security systems that require resources from both."

3.2.2 3rd Annual Benchmark Study on Patient Privacy & Data Security 2012

The Ponemon Institute held a 3rd Annual Benchmark Study on Patient Privacy & Data Security 2012. This study is to identify about patient privacy and the data security of the hospitals in America. This study revealed that the lack of technologies, resources and trained personnel consequence many healthcare organizations having difficulty to deal with privacy and data security risks. According to this study, it was found that 94% hospitals in America were experiencing data breaches and 45% of them were suffering from more than 5 breaches. Furthermore, it was noted from the study that 54% of the organizations have suffered from the medical identity theft. Generally, about 21, 210, 439 individuals have been affected by the data breaches at the healthcare organizations and 1.85 million American were affected by the medical identity theft in that particular year.

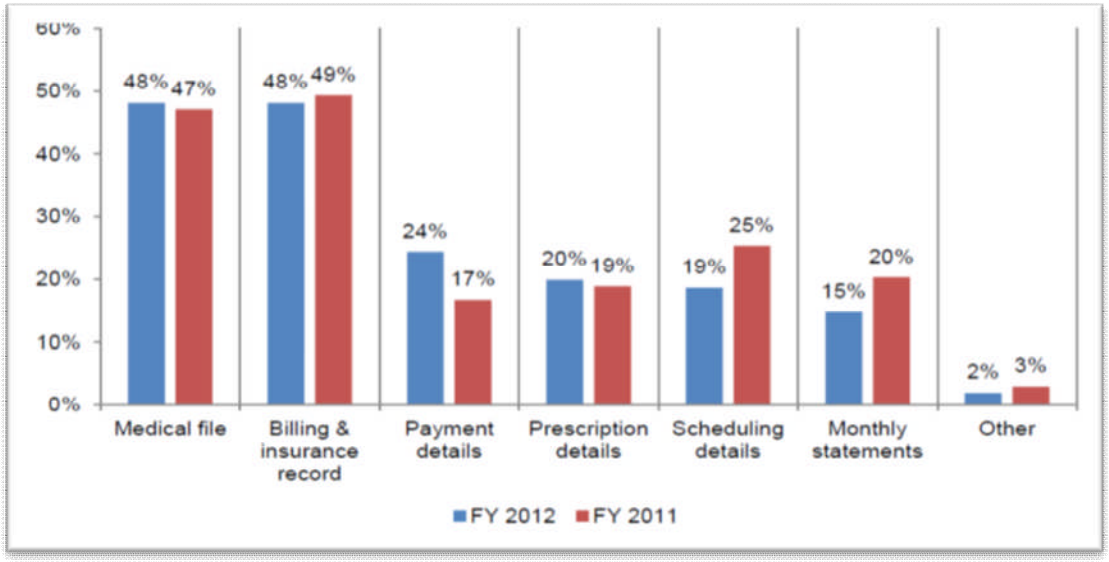


Figure 3.3 : Types of stolen and lost data in the year 2011 and 2012

Based on the figure above, it is clearly shown that the medical files, billing and the health insurance record are the data that always been stolen or lost. These files are the important files and records which should be kept confidential to avoid any bad consequences in future. For instance, the cyber criminals could exploit the stolen medical record and use it for fraud. As for the billing and insurance record, they would steal the card and account number, so that they can use it to transfer the money from the account. Data breaches have cost the United States healthcare industry as high as $7 billion in the year 2012 and the annual cost for the medical identity thief is $41.3 billion in the year 2012. This data indicated that the data breaches can affect the economy in a particular country severely.

It is reported in this study that data breaches and medical identity thief occur because of several reasons. The causes are divided into three categories. The first category is the common mistakes that happened in the hospitals, the second is the lack

defence by the organizations and the third is the threats that come from the current technologies.

- The Common Mistakes and Errors Occur in the Hospitals

The data breaches and the medical identity thief are happening because of the common errors and mistakes occur in the hospitals. Firstly, the technical glitch can also cause the data breaches and medical identity thief. The technical glitch might cause from the malfunction of the health IT security software, the power glitch where the power is temporarily not function and the bug that encountered with the web browsers. These glitches are unavoidable which allow someone to take advantage of the situation and steal the important data from the organizations.

The criminal attack or also being called as a cybercriminals is chosen by the employees as a reason to the data breaches and medical identity occurrence. The Malicious Code, hack threat and fraud are the examples of the cyber criminals. Normally, the cyber criminals purposely enter the organizational systems to steal the classified data and use them to get money. The cybercriminals are always out of control and well-trained personnel are needed in each organization in order to prevent or stop them.

Next, one of the major causes of the data breaches is the employee mistakes. The employees themselves agree that the data breaches and the medical identity thief happen because of their carelessness in handling the data that are related to the patient and the organizations. Their actions which are leaving the computer screen open, giving the username and password to others and the username and password clearly written in the place that is easy to be read endangered the important data of the patients and

organizations. To prevent this from happening too frequently, the higher level management should hold a short seminar or training that will teach and guide the employees in handling the data.

From the survey of this study, the majority of the employees agrees that data breaches happen for the stolen or lost computing devices. For instance, tablet, thumb drive and memory cards are the common stolen or lost computing devices and typically contain numerous important classified data. If these computing devices are stolen or lost, the classified data on the devices would be exposed to the irresponsible individual and use them for the wrong purposes. Therefore, it is very important for the individual who is responsible for handling the data to be extra careful especially in keeping the computing devices.

- Organizations Lack Defence

Result from the study showed that 67% of the health organizations are lack of defense which means they do not have the sources or the ability to prevent the medical identity thief. They do not confident that they can prevent and detect the medical identity thief which might be because of the lack of the technologies, resources and well-trained IT personnel in their organization. There are lots of works need to be done in order to upgrade the technologies and injecting the budget to the health organizations, so that the health IT security is secure enough from the cyber threats.

- The new technology trend threatens patient data

Bring Your Own Devices (BYOD) is a current IT trend which the organizations allow their employees to bring their own devices to connect to their networks or enterprise system. This is part of parallel system also known as a shadow IT; any hardware or software within an enterprise that is not supported by the organization's IT central department. BYOD however, does not secure enough to be used if it is connected to the corporate or patient data. The employees themselves do not sure if it is secure to use their own devices to connect to the networks or the organization system.

According to the study, most of the hospitals are using the cloud-based services. They probably use the cloud services as it is can be delivered to them as a service whenever and wherever they need. The cloud service covered all the things on the Internet; the delivery of software, infrastructure and storage. Looking at the embracing of the cloud service in the health organizations, it is quite worrying when some of them do not confident if they can keep the data secure in the cloud service. In this case, the cloud providers must provide a guaranteed service level and security to their consumers.

3.3 IT SECURITY ISSUES IN HIS

The security issues in a Healthcare Information System basically come from research domains that the health care system frequent goes through. These include the healthcare consumers and providers, the inter-organizational of healthcare and also the other public policy that frequently which have become the most frequently used research domains for healthcare information system. Having research using these domains eventually at the same time will bring along the threats to the Information Privacy and Security presents in the healthcare.

Healthcare consumers as a research domain in Healthcare Information Security have used the IT for health care in many fields of work which have also included in the section on Personal Health Record Management, Clinical Trial Participation and the Personal Disposition to Data Disclosure. Due to this on-going process, the healthcare privacy and security system might be exposed to the threats that might be resulted from these activities. Therefore, the flowing and continuous activities between the IT of the healthcare and their consumers have lead many possible threats to affect the system. As they were dealing with the personal health record management and private data of their patients, the information might get leaked out as the security system of the Information Privacy and Security are not secure and effective enough.

In addition, threats to the Information Privacy and Security also might be caused from the providers. Providers as one of the research domains basically help a lot in providing data flows to the healthcare. It includes the data flows of the impact of IT on medical errors, RIFD deployment in medication admin, risk analysis and assessment, telemedicine or eHealth and helps in pervasive the Computing in healthcare as well as in the operations management. On the other hand, the providers are actually bringing the threats to the healthcare information security as well especially in the aspect of the access control, information integrity, network security, privacy policy management and the healthcare risk management. This security issue has become a big problem as it has given bad effects on the healthcare information security' performance.

Inter-organizational systems (IOS) are ICT-based systems that enable organizations to share information and to electronically conduct business across organizational boundaries. Inter-organizational systems may promote much major interest of organizations, e.g. by enhancing cost effectiveness, speed and flexibility (Boonstra A. Vries, J. D., 2004). Same goes to the healthcare organization, IOS also share lots of data and information with the information system

in healthcare especially in the terms of the Health Services Subcontracting, Integrated Healthcare Systems and Billing and Payment Efficacy. However, an IOS can also be a threat to some organization, especially to the healthcare information system as they share a lot of information with each other. For instance, while sharing all the data, threats may be easily attack the access control of the healthcare information system, giving a risk to the data interoperability, causing fraud control and also giving a risk to have a multi-institutional network security.

Another all-time favourite research domain in healthcare information security is the public policy. Public policy has become one most important source for information in the area of study for Medical Research, Law Enforcement, Nationwide Health Information Network (NHIN) and the Regional Health Information Organizations (RHIOs). Social welfare programs, disaster response/disease control and also the pricing of Health Services. However, leaving the public policy to become one of the domains has giving side effects to the Information Security in healthcare as well. The information security might be risked of having some serious data issues like healthcare data interoperability, regulatory implications to the healthcare practice or technology adoption as well as to disclosure of secured data.

Healthcare data interoperability is a cornerstone issue as the domains for making the research have become more heavily involved in health IT issues, which have included the electronic health records, accountable care organizations and the mobile health innovations. It was believed that interoperability can be a litigious issue among the vendors that don't want to share proprietary system information and providers that don't trust sending patient information databases for anyone to see. On the other hand, the problems in the healthcare practice or technology usually are happening within the organizations in which nurses' work; (1) organizational governing boards that focus on safety; (2) the practice of evidence-based

management and leadership; (3) effective nursing leadership; (4) adequate staffing; (5) provision of ongoing learning and clinical decision making support to nursing staff; (6) mechanism that promote interdisciplinary collaboration; (7) work design practices that defend fatigue and unsafe work; and (8) a fair and just error reporting, analysis, and feedback system with training and rewards for patient safety (Ann E.K, 2006). In short, having the problems in the healthcare practice especially within the nurses will lead to the regulatory implications towards the organization as they play a big role in emphasizing patients' safety and the management practices. Moreover, it is also very crucial for healthcare providers like the public policy organization to report health issues, such as influenza outbreaks to public health authorities. However, the reluctance to share patient data for public health purposes has become a major issue due to their concerns for both patient privacy and provider confidentiality. This letter has led to other issues and threats to the healthcare information system.

3.4 PRIVACY

Privacy is normally referred to the right control access to oneself, and it includes the physical privacy such as ensuring curtains are closed during physical examinations. Moreover, privacy also may relate to the information or data about oneself and an information privacy law regulates the handling of personal information through enforceable privacy principles. In addition, privacy also is viewed as a key governing principle of the patient-physician relationship (Appari A. 2010; Johnson. M. E, 2010). Therefore, it has become a legal duty for the healthcare practitioners to protect and maintain their patients' data against the inappropriate disclosure of personal health information.

3.4.1 Information Privacy Protection

An excellent Health Information Privacy should stress more on the Information Privacy Protection as that is where the privacy of every patient's health information is confidential held on. Therefore, to make sure the confidentiality of the Information Privacy Protection, a study on that subject has eventually been made. The study has shown that the information privacy protection have been studied in the five different contexts which are about the; awareness, consent, access, integrity or security and the enforcement.

As a result, in the aspect of awareness within the healthcare practitioners is at a low practice. This is because the awareness in the healthcare is currently being practiced due to the cost factor and the lack of patient awareness. Upgrading and assisting the security system in healthcare especially in the privacy sector does require a high cost, thus inflating the awareness to be practiced within every healthcare. Same goes to the lack of awareness among the patients. A patient generally does not really care about their health data confidentially as they believe that the practitioners will take care of everything.

Therefore, due to the lack of awareness among the healthcare practitioners and the patients, the consent has not strictly been done. According to the National Health Service, consent to treatment is the principle that a person must give their permission before they receive any type of medical treatment. Consent is most needed from a patient regardless of the treatment and the principle of consent is an important part medical ethics and it also has become a part of the international human rights law. The consent has only been valid when it has been made voluntary and well-informed. Thus, the patients himself or

herself have to give the permission or volunteer themselves before they can undergo any treatment. Moreover, they also must have understood the information given to them before they made their informed decision. However, due to the lack of awareness about consent among the patient, this principle cannot strictly be done in the healthcare.

Access control is a key feature of healthcare information systems. It is about enforcing rules to ensure that only authorized users can get access to resources in a system. In healthcare systems, it brings means that protecting the patient privacy (Rostad.L, 2009). Its top priority is to provide the best possible care towards their patients. However, in healthcare, access control is hardly can be accessed by some users. It was said to be accessible but not with easy procedures and sometimes it incur some costs as well to access the information system of the healthcare. On the other hand, the integrity and the security within the healthcare are strictly under practiced as it is highly crucial to protect the privacy of the healthcare information system.

In addition, the enforcement purpose for healthcare information system also has no any specific act that is being enacted in order to protect the PMI Healthcare Community of Practice privacy especially in government hospitals, except for the standard ethical code of professional contacts.

3.4.2 Privacy Mechanism in Security PMI

The privacy Mechanism in Security PMI can be divided into four different sections which are; Legislation, Ethical Code of Conduct, Privacy Protection Technology and also the Privacy Awareness. Legislation in privacy mechanism for PMI is eventually based on any information privacy or data protection act that enforced in that specific

country while the Ethical Code of Conduct is based on the hospital or the ministry's policies and medical act. The privacy protection technology in securing PMI is importantly needed in order to enhance the PMI database and management system in accordance to the latest privacy mechanism technologies. Finally, the privacy awareness should be continuously be trained among the health care practitioners and education need to be provided for all personnel in HIS hospital so that they would become even aware about the privacy mechanism in securing the healthcare and PMI.

3.5 RECOMMENDATIONS

In order to maintain the secure security and privacy of healthcare information system and technology, a few steps should be considered to be taken. The first suggestion to esteem the security within the healthcare information system is by putting the defence in depth. This can be done by emphasizing by multiple, overlapping, and mutually the supportive defensive systems into the highest level. Keeping upgrading the systems also may help in being up-to-date with the latest technology that can be used to keep a secure and effective system in the healthcare information system.

Moreover, educating the employees also can be a big help to keep the system in healthcare secured and confidential. The employees shall especially be the nurses as they usually get involved the most with the patients and outsiders. The education then shall be emphasize on how to raise their awareness about the risks of social engineering and how to counter it by having some staff training for them.

To prevent the same data loss problem to be happening again, the data loss prevention training should be getting underway as this can help in preventing the data loss and exfiltration

with data loss protection software on the network to occur someday. Besides, the system also should be assisted with a full range of protection technology. A full range of protection technology can help to overcome issues like insufficient Antivirus within the system that often happens in the health care system. In addition, a network-based protection and reputation technology also must be deployed on endpoints to help prevent any threats or attacks that come upon the system. Subsequently, it is also vital to consider the Always On SSL to encrypt visitors' interactions in protecting the public-facing websites. This is because the Always On SSL is an end-to-end security that can help protect every webpage user visit which therefore can help to protect the entire user experience from start to finish, making it safer to search and share.

Protecting the code when a user is signing the certificates also can help in improving the security system in every HIS. A certificate is a must in order to apply a rigorous protection and security policies to the safeguard keys. This certificate should be done by the certificate owner himself so that it would be customized according to his needed privacy policy. Lastly is by having the software updating and review patching processes. It is truly essential to update and patch all software into the system prompt in order to maintain the secure security system in every health care.

3.6 CONCLUSION

The implementation of HIT security in hospitals and healthcare can give plenty advantages to these organizations. Both of the healthcare organizations can share their data and information even easier and appropriate than before. However, implementing the Information Technology into hospitals and healthcare also can give some security issues which include the threats and viruses that may harass the system functions. The vulnerabilities that usually

occurred within the security mechanism while sharing the information with other research domains will lead to the occurrences of any possible threats. In addition, physical security solutions for healthcare require a balancing act between safety and service, quality of care and regulatory compliance. Therefore, it is essential to keep the physical security in a good performance so that the healthcare security system can maintain its secure and effective system performance. Besides, the Information Security Culture that includes all socio-cultural measures which support technical security methods also must be maintained into a good shape as it has become a natural aspect in the daily activity of every employee. The last aspect that should be emphasized on this security issue is about the PMI Privacy. As PMI provides privacy statement that covers five main areas; Awareness, Choice, Access and Correction, Security, and Additional Website Issues, it would be easy to use the PMI to protect the HIT security and privacy policy.

In addition, it also has become heavily important to identify the current problems that are happening within the health care system. This should be done by using different view of users so that the issues can easily be spotted. Only after we had done by detecting the problems, we can move to the next step which is to find the appropriate solutions for the problems occurred. All these steps must be taken in order to protect the privacy and confidentiality of PMI.

Lastly, the security awareness must be raised especially among the health care practitioners and patients. Staff training that focus on the security awareness should be held frequently just to make sure that the practitioners and other staff understood about their responsibility in maintaining the excellent and secure IT system and security system in HIT and health care. Moreover, the information security cultural factors in the healthcare informatics environment also should be identified especially in the sector of security behaviour, security knowledge and security awareness.

CHAPTER 4
SECURITY REVIEW FRAMEWORK FOR HOSPITAL INFORMATION SYSTEM

Hadi Syahrial

ABSTRACT

This paper presents the Security Review Framework which is proposed to be implemented in Hospital Information System. The framework will lay emphasis on the purposes of the security review of the system in hospitals, how to identify the security early design flaws on in the Software Development Life Cycle (SDLC) and to provide a security or risk profile to make decisions regarding the hospital information system implementation. In addition, this paper also will focus on how to identify the threats which are happened to be exposed to the hospital information system and at the same time will determine any inherent security weaknesses within the proposed design of the hospital information system under review.

4.0 INTRODUCTION

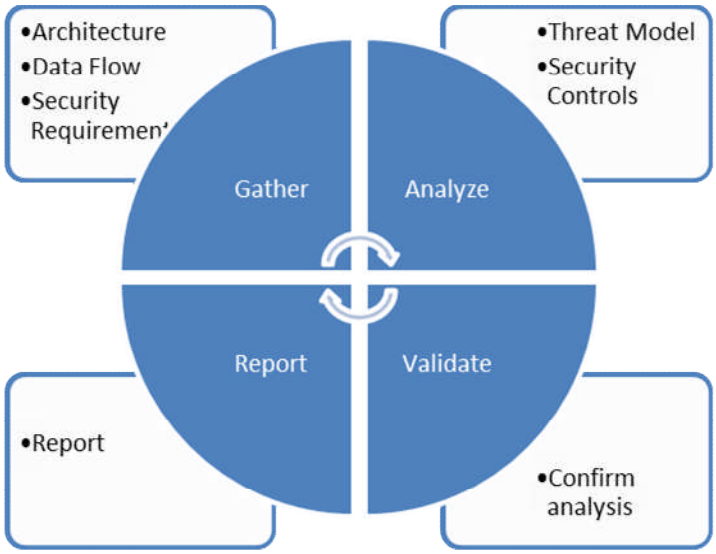
A Security Review is a collaborative process used to identify security-related issues, determine the level of risk associated with the security-related issues, and make informed decisions about risk mitigation or acceptance. This process should be completed for all services and service changes that may affect security prior to go-live. A security review is most essential in response to security concerns or new security-related requirements.

The purposes for coming out with the security review framework for Hospital Information System are mainly to provide a secure security advisor in developing the SLDC which will be controlling the security in place, for a better understands about the threats a hospital information system is exposed to and lastly is to determine any inherent security weaknesses within the proposed design of the hospital information system under reviews. In this modern computing era, health care system is a crucial aspect of society since it involves the security of the citizens' confidential personal data and the health care system management and information system as well. Therefore, these days, many countries tried to reform their health care system due to the rapid growth of their citizens' populations. Moreover, the increasing cost of health care providers, insurance companies, hospitals and on patients also are being the factors to shift forward security of the Hospital Information System into a more proactive which will be focusing on the early detection or protection over any threats.

The purpose of this paper is to review the security framework for the Hospital Information System and also to highlight the importance of implementing it in every hospital and healthcare worldwide. The first part of this paper emphasises about the Hospital Information System (HIS), which will give a deeper information about the HIS. Then, the second part will discuss on the purposes of providing a secure security system into the Hospital Information System and also a deeper understanding about how to identify the security design flaws on in the Software Development Life Cycle (SDLC). In addition, the second part also will expose the possible threats which might be exposed to the Hospital Information System. The second part then concludes the topic with the determination of any security weaknesses especially within the proposed design of the Hospital Information System under review.

The last part of the paper presents the proposed framework for the security which should be implemented into the Hospital Information System. This most crucial part will talk about the stages that are present in the Security Review Framework. Figure 4.1 shows the stages present in the Security Review Framework.

Figure 4.1 : The stages present in the Security Review Framework for Hospital Information System



4.1 HOSPITAL INFORMATION SYSTEM

Hospital Information System (HIS) is a designated system which works in running and managing the information within the hospital in order to ease the health care personals works. A hospital can operate smoothly when HIS is applied in the system. This is because the related data within the hospital system is no longer managed manually but will be managed fully by HIS. A Hospital Information System which has become one of the aspects of the present invention is configured by; a mobile terminal for inputting or outputting data of medical activities at an execution site of medical activities in a hospital; a hospital information management system for

managing the information within the hospital; and a server for controlling the communication of data of the medical activities within the hospital information management system (Suzuki H., 2003; Omori S. 2003).

On the whole, Hospital Information System (HIS) is a system that can aid the hospital management system or hospital personals to control all the data by using a more effective way. HIS was introduced in the 1960s and then was developed as the health care facilities changed. Back to the past, HIS was only used by the staff in billing and for the hospital purposes but nowadays, HIS are used in all clinical, financial and administrative applications. The effector functions of HIS are mostly used in managing the data which related to the clinic, finance departments, laboratory, nursing, pharmacy and radiotherapy and pathology departments. The uses of HIS in hospital have made a quick access to the information about the patients' record (demographic, diet plan, medical history), the important data if the hospital finance system and also the distribution of medications. The implementation of HIS has fit the patient needs in protecting their personal data into a more guaranteed confidential, integrate and availability data flows. In addition, having an effective HIS in hospital management system gives out these advantages; enhances information integrity, reduces transcription errors, reduces duplication of information entries and optimizes report turnaround times.

4.2 PURPOSE OF SECURITY REVIEW

Security system in the hospital is a must because the hospital is one of the most people intensive places. Hospital is the place which provides services to people who needs treatment and advice beyond their illness (Das N.C, 2000). The hospital uses very costly equipments,

fixtures and machines in treating their patient thus the equipments and machine safety is really essential. On top of that, not only the hospital system is important but safety of patients, attendants and their property has also become the moral duty of the hospital.

The security review framework's objective is to fix and make the hospital management system become more secure in the aspect of the hospital property, patient's belongings, hospital buildings and fixtures, hospital staff and also patient visits. All of these aspects need to have a secure security services. Thus, in order to fix the security system for hospital, a security review framework has been set up. The first purpose in coming out with the security review framework is to provide a security advisor who can help in the developing the understanding of the Software Development Life Cycle (SDLC) process. It is because in order to quickly understand the security controls for a hospital system, it has become a must to understand the Software Development Life Cycle (SDLC) process first. A Software Development Life Cycle is essentially a series of steps, or phases, that provide a model for the development and lifecycle management of an application or piece of software. The methodology within the SDLC process can vary across industries and organizations, but standards such as ISO/IEC 12207 represent processes that establish a Lifecycle for software, and provide a model for the development, acquisition, and configuration of software systems (Glynn, F. 2008). In short, SDLC is a framework that describes the activities performed at each stage of a software development project.

The second purpose is to make a better understanding about the threats the hospital information system is exposed to. There are many categories of threat that may affect the hospital information security system. All these threats will lower the quality service of the

hospital information system. The list of possible affecting threats to hospital security system is shown in Table 4.1 below.

No.	Categories of Threat
1	Power failure/loss
2	Network Infrastructure failure or errors
3	Technological obsolescence
4	Hardware failure or errors
5	Software failures or errors
6	Deviations in quality of service
7	Operational issues
8	Malware attacks (Malicious virus, Worm, Trojan horses, Spyware and Adware)
9	Communications interception
10	Masquerading
11	Unauthorized use of a health information application
12	Repudiation
13	Communications infiltration
14	Social Engineering attacks
15	Technical failure
16	Deliberate Acts of Theft (including theft of equipment or data)
17	Misuse of system resources
18	Acts of Human Error or Failure

19	Staff shortage
20	Wilful damage
21	Environmental Support Failure/Natural disasters
22	Terrorist Attacks

Table 4.1 : List of possible affecting threats to hospital security system

Lastly is to determine if there is any inherent security weakness within the proposed design of the Hospital Information System under review. The proposed of the security review framework will be presented and evaluated so that the idea of security framework is secure enough to protect the hospital management system and hospital information system.

4.3 SECURITY REVIEW FRAMEWORK

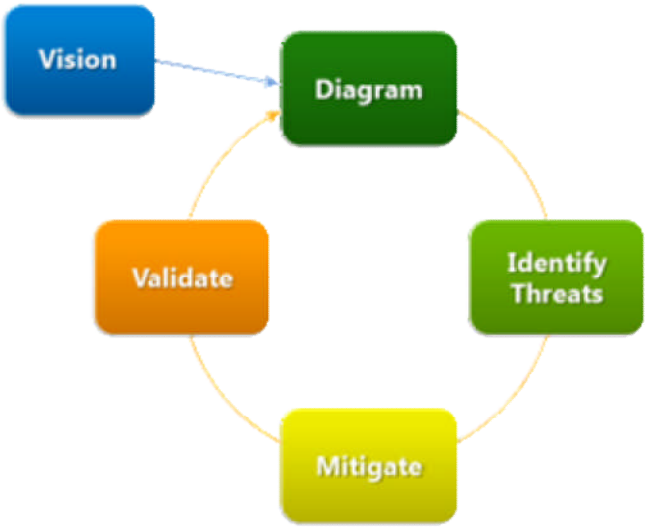
The proposed Security Review Framework for Hospital Information System consisted of four vital stages which are; gather, analyse, validate and report the suggested framework.

4.3.1 Gathering the data for Security Framework

The first requirement in gathering the data for security framework is to review the technical architecture and then build a comprehensive security architecture framework. A comprehensive security architecture framework is the planned framework which has successfully been designed to be included in the hospital information system itself. Building an ample framework helps in giving out the efficient and well-organized security services for the hospital management system.

Hospital Information System consist a lot of valuable and important data aspects which includes the aspect of the hospital property, patient's belongings, hospital buildings and fixtures, hospital staff and also patient visits. Unlike physical assets that can be locked up in a vault, data is a fluid asset that is changing and moving every second. Thus, it is extremely crucial to assure that those important data is protected and are put in a secure security system. The second thing needed to be gathered is the review data flow for the suggested framework. This can be done using the Microsoft SDL Threat Modeling. Threat modeling is a core element of the Microsoft Security Development Lifecycle (SDL) and as a part of the design phase of the SDL, threat modeling allows software architects to identify and mitigate potential security issues early, when they are relatively easy and cost-effective to resolve. Consequently, Microsoft Security Development Lifecycle (SDL) can help to reduce the total cost of development. The SDL threat Modeling Tool is the first threat modeling tool which is not designed for security experts. It makes threat Modeling easier for all developers by providing guidance on creating and analysing threat models. It can enable any developer or software architect to communicate about the security design of their systems, analyse those designs for potential security issues using a proven methodology and also to suggest and manage mitigations for security issues. Therefore, by using the Microsoft SDL Threat Modeling, it would be easier to design a secure and efficient security system for Hospital Information System. Figure 4.4.1 shows the Microsoft SDL Threat Modeling's design for security system.

Figure 4.2 : Microsoft SDL Threat Modeling's design for security system.



The last thing to be gathered is the security requirements of the Hospital Information System itself. A security requirement will include the misuse case, Health Insurance Portability and Accountability Act (HIPAA) Security Rules and the vendor evaluation. Misuse case is a technique that is used to support the early determination of security requirements by improving communication and understanding about security issues within the project group and evaluated this through example models and interviews with experts (Andreas L. Opdahl, 2009; Sindre G., 2009). Misuse case would be effective in collecting and fulfilling the security requirements because it is easy to be understood and used, fills a perceived need and is useful for facilitating communication and creativity early throughout the process of security requirements. Next is by adding the Health Insurance Portability and Accountability Act (HIPAA) into the hospital or healthcare system as it have the ability to transfer and continue health insurance coverage for millions workers and their families when they change or lose their jobs, reduce health

care fraud and abuse, mandates industry-wide standards for health care information on electronic billing processes and finally it can requires the protection and confidential handling of protected health information for the hospital. Lastly is to collect the vendor evaluation and insert it into the proposed framework. Vendor evaluation is extremely important in supporting the procuring both materials and external services, by making use of data from MM, from the Logistics Information System (LIS info structure S013), and from quality management.

4.3.2 Analysing the Security Review Framework

The second imperative step in building the Security Review Framework for Hospital Information System is to analyse the proposed framework itself. This will include in analysing the threat model for the security review system, ways to control the security system and the penetration test for the future implanted security system.

The first and foremost thing to be analysed is the threat model used in the Security Review Framework. In this proposed security system, the Microsoft SDL Threat Modeling has been used to handle the prototype of the proposed security system. The most suitable threat model that should be used is the Microsoft Security Development Lifecycle (SDL) Threat Modeling Tool 3.0 which can allow for early and structured analysis and proactive mitigation and tracking of potential security and privacy issues in new and existing applications especially in the Hospital Information System. In addition, the tool integrates with bug-tracking systems, thereby integrating the threat modeling process into the standard development process. Indeed, this can help the Hospital

Information System becomes more secure and effective in their security vulnerabilities as bugs and mitigations as features.

Next is to analyse the security controls that should be in charge of handling the security management system. In order to achieve the most secure and effective security techniques, the most suitable code of practice for information security management should be brought into play. Therefore, ISO 27002:2005 is strongly recommended to be used in the Hospital Information Security Management. ISO 27002:2005 comprises ISO 17799:2005 and ISO 17799:2005/Cor.1:2007. Its content is technically identical to ISO 17799:2005. ISO 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. ISO 27002:2005 contains the best practices of control objectives and controls in the areas of; security policy; organization of information security; asset management; human resources security; physical and environmental security; communications and operations management; access control; information system acquisition, development and maintenance; information security incident management; and compliance. The control objectives and controls in ISO 27002: 2005 are meant to be implemented to fulfil the requirements needed by a risk management. For that reason, it is the best to use ISO 27002:2005 in developing the organizational security standards and effective security management practices, and also to help build confidence in inter-organizational activities.

The final thing to be analyse is the penetration test. This method of evaluating the computer and the network security can be done by simulating and attack upon the computer system or network from external and internal threats. The process will involve

and active analysis of the system for any potential vulnerabilities that could result from the poor or improper system configuration, both known and unknown hardware or software flaws, and operational weaknesses in process or technical countermeasures. The effective penetration tests will result into the accurate assessment of the potential impacts of the Hospital Information System and it also will outline a range of technical and procedural countermeasures to reduce risks.

4.3.3 Validating the Security Review Framework

The third stage of the Security Review Framework is to authorize and confirm the following analysed subjects for Security Review Framework which are; the threat model and the security controls. Therefore, it has been confirmed that the selected threat model is the Microsoft Security Development Lifecycle (SDL) Threat Modeling Tool 3.0 which can provide a better and more secure security management system. Due to its excellent features and good performance which can allow for early structured analysis and proactive mitigation and tracking of potential security and privacy issues in new and existing applications especially in the Hospital Information System, it is strongly recommended to apply this into the hospital management system. Moreover, this tool is integrated with bug-tracking systems; thereby integrating the threat modeling process into the standard development process which can help the Hospital Information System becomes more secure and effective in their security vulnerabilities as bugs and mitigations as features. Regarding the Security Controls, ISO 27002:2005 indeed has become the excellent choice as it contains the best practices of control objectives and controls in the areas of; security policy; organization of information security; asset

management; human resources security; physical and environmental security; communications and operations management; access control; information system acquisition, development and maintenance; information security incident management; and compliance. Therefore, the control of the security will be easier to handle as ISO 27002:2005 are fully meant to be implemented to meet the terms needed by a risk management.

4.3.4 Reporting the Security Review Framework

The last and final stage in framing the Security Review for Hospital Information System is to report the proposal. The report must be made in two versions which are the draft report and the final report. Draft report should consist about the rough ideas about the proposed framework. Draft report then will be submitted and will be analysed and if there are any mistake needs to be improved, then they must go through the paper again and look up the inaccuracy in the improvisation process. Finally, the final report will be submitted after several processes of improvisation. The final report should be updated and have complete features that show the exact proposed Security Review Framework which include the objectives and purposes of the Security Review Framework for Hospital Information System, a little bit introduction or summary of Hospital Information System (HIS), and also the four stages which featured the Security Review Framework; gathering, analysing, validating and reporting the framework for HIS.

4.4 CONCLUSION

In essence, this Security Review Framework should be implemented in Hospital Information System (HIS) in order to provide a security advisor who can help in the developing the understanding of the Software Development Life Cycle (SDLC) process. Due to its complexes in performance, SDLC must be conducted by a professional security advisor who can understand the security controls and management for a hospital. A SDLC is basically a series of steps, or phases, that provide a model for the development and lifecycle management of an application or piece of software. In the other words, SDLC is a framework that describes the activities performed at each stage of a software development project. Therefore, by understanding the goals of implementing the SDLC in Hospital Information System (HIS), it will become much easier to identify the security design flaws earlier.

In addition, it is also has become really essential to provide a security or risk profile like ISO 27002:2005 to make decisions regarding the security implementation of Hospital Information System (HIS). This is because ISO 27002:2005 contains the best practices of control over the objectives and controls in the areas of; security policy; organization of information security; asset management; human resources security; physical and environmental security; communications and operations management; access control; information system acquisition, development and maintenance; information security incident management; and compliance. Moreover, the control objectives and controls in ISO 27002: 2005 are principally implemented to serve the requirements needed by a risk management. For that reason, it is the best to use ISO 27002:2005 in developing the organizational security standards and effective security management practices, and also to help build confidence in inter-organizational activities.

CHAPTER 5

Health IT Security: GNU Health

Seyed Mohammad Motahar

ABSTRACT

In organizations such as the hospitals, clinics and pharmacies manage lots of data and information about the patients' health. Some of this data may contain sensitive issues and must be stored securely. This is why we need information technology in the organization because it stores the data in order. We also need the presence of software which it will secure all the data that's being stored and only certain people can view it. This chapter will help the reader to get to know the basic technology that being used in the organizations. Next, it will introduce the reader about the health care information systems and lastly, it will explain about the GNU software.

5.0 INTRODUCTION

Every human needs a house to keep them from danger and to keep secure. The house will prevent them from getting sick, danger and most important is to keep privacy from others. This is why the house is one of the four need in life. We as a human being need protection and want a secure place to live. In organizations such as the hospitals, clinic and pharmacies they need to keep the patients' information safe. To manage the data safe and secure without having leaks, they need a software which can ensure their data are being stored with security.

What is Health IT Security? First, let's look at the meaning of Health IT which it is a management of health information across the computerized systems in the organizations. For the

Health IT Security, it stressed out on the security aspects of the management of the health information across the computerized systems in the organizations. As Chaudhry (2006) state that health information technology (HIT) was viewed as the most promising tool for improving the overall in quality, safety and the efficiency of the health delivery system. HIT helps the hospitals, clinics and pharmacies manage the data of health information across the computerized system in the organizations.

A software that could help to keep the data from unauthorized person or group is the GNU Health software. This software was adopted by the United Nations because United Nations want to help in improving the privacy and the security of the data, especially in the health world. This will help the management to collect, process, store and transmit the data as it being requested by a certain group or person. On this paper it will tell more about the GNU software and how the organizations use it.

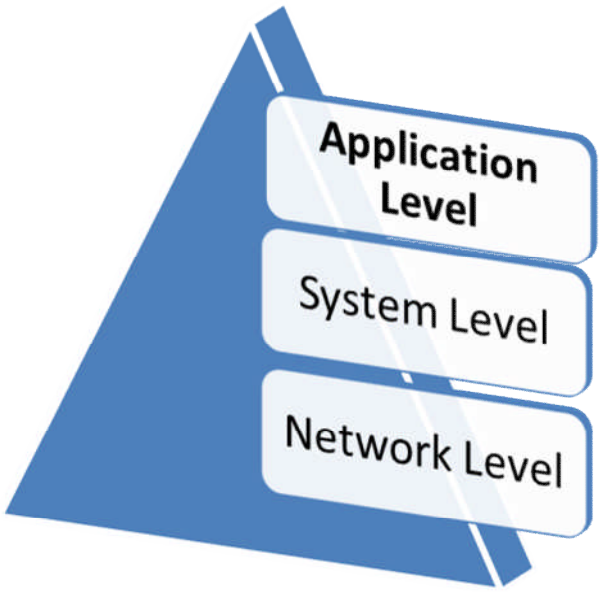
5.1 ENHANCE THE SECURITY IN HEALTH IT

At the Social Security Administration the Official Website of United State Social Security, the Health IT is a revolutionary new program that brings the speed and the power of the electronic in medical records to the disability determination process. For example, when a person applied for disability benefits, the Social Security must obtain a complete health record. This requirement is needed to make an accurate determination. Usually, it takes a month for the health care organizations to provide the patient's case but with the electronic records transmission it could just take a whole day or just a minute. Thus, the patient can get the help that they need faster than they thought.

Privacy and security are dominant concerns for any health IT system and it must be addressed at the outset. With a comprehensive thoughtful and flexible approach, it can ensure the enhanced privacy and security which built into health IT systems will strengthen the consumer trust and confidence. Health Information Technology (HIT) is a management of health information that using computerized systems. Health IT Security touches on the security aspects of the management of the health information in computerized systems. HIT involves the exchange of health information in an electronic environment. The abilities of Health IT are to advance clinical care, improve population health and reduce the cost.

Besides that, it also poses new challenges and opportunities for protecting individually identifiable health information. HIT is the most capable tool for improving the quality, the safety and the efficiency of the health delivery system in health organizations. Health IT promises a number of potential benefits for individuals, health care providers and the nation's health care systems. It helps to protect the patient privacy and guide the nation's adoption of health information technology. It is imperative that the privacy and security of electronic health information be insured as this information is maintained and transmitted electronically. As a part of the health organization, we need to learn more about the technologies that will enhance the security in Health IT.

Figure 5.1 : Review of Security Mechanism in EHR modules.



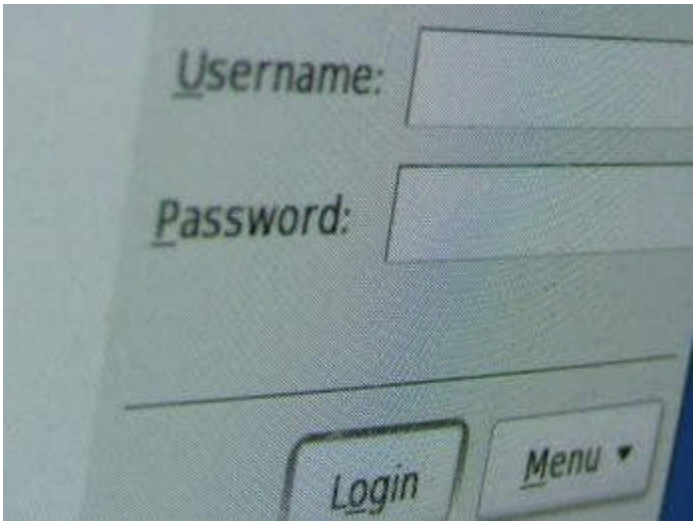
The figure above is a pyramid shown the level of security mechanisms in EHR modules. On this section, it will be focusing on the application level. Based on the security mechanisms in EHR modules, there were separated into two sections. The first section is about User/Pass Mechanisms. In this section, it is about the firewalls/VPNs and biometric mechanisms. The second section is about role based security mechanisms. In this section, there are four sub-topics which are PKI and Kerberos, cryptographic algorithms, electronic tags and RFID chip for authentication.

5.1.1 User/Pass Mechanisms.

Security is an important aspect of any application design. When the web services are deployed and being accessed, you might like to restrict its

accesses to a particular set of users/ groups or any users of a particular role. The most common authentication mechanisms seen in current EHRs are an 'identifier' together with a 'password' (Allaert et al. 2004). Most users of EHRs believe that password checking included in the system will ensure system security of EHRs. However, the password checking alone to ensure access restriction does not secure adequate security for EHRs (Khin Than Win 2005).

Figure 5.2 : User/Pass Mechanisms



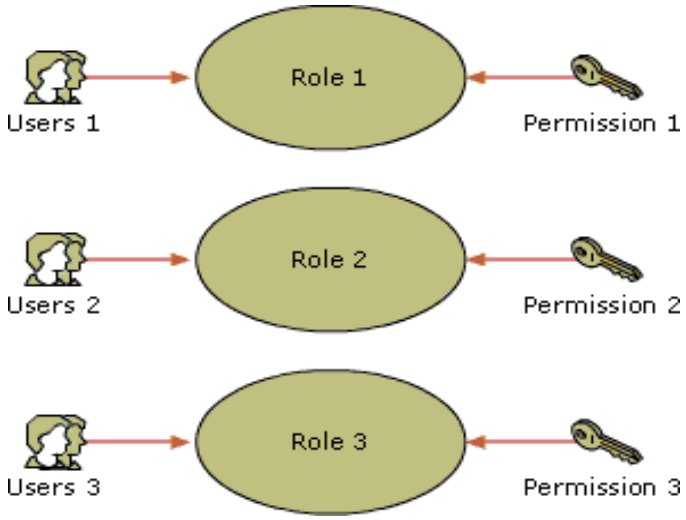
Virtual private networks (VPNs) increasingly getting attention in medical practices across the country to link multiple sites , eliminate unnecessary in record- keeping and at the same time keep the patients' information secure. A virtual private network broadens of a private network across a public network, for example the internet. It allows a computer to send and receive data, across shared or public networks as if it were directly connected to the private network. A VPN

connection is similar to a wide area network (WAN) link between the sites. The hospitals, clinics and insurance provider highly demand towards VPNs because they need to link multiple geographically diverse business locations. Nowadays, virtual private network is a necessary for organizations to keep their data especially hospitals, clinics and pharmacies which they have lots of sensitive data to protect. VPNs were needed to make sure the data being transferred as soon as possible and what's most important is the data is accurate.

The biometric is a method to identify the human by their characteristics or traits. To identify the person we can use these methods such as fingerprints, finger scans, iris scans, face scans, voice recognition and signature scans. Vein scans and DNA are being used in research for authentication. Biometric or in another name biometric authentication is being used in computer science as a form of identification and access control. Biometric also being used to monitor the patients who under surveillance. Biometric identifiers are often classified as a physiological versus behaviour in characteristics. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. This biometric mechanism has helped the hospitals and clinics by lessening the process, save waiting time and give accurate data.

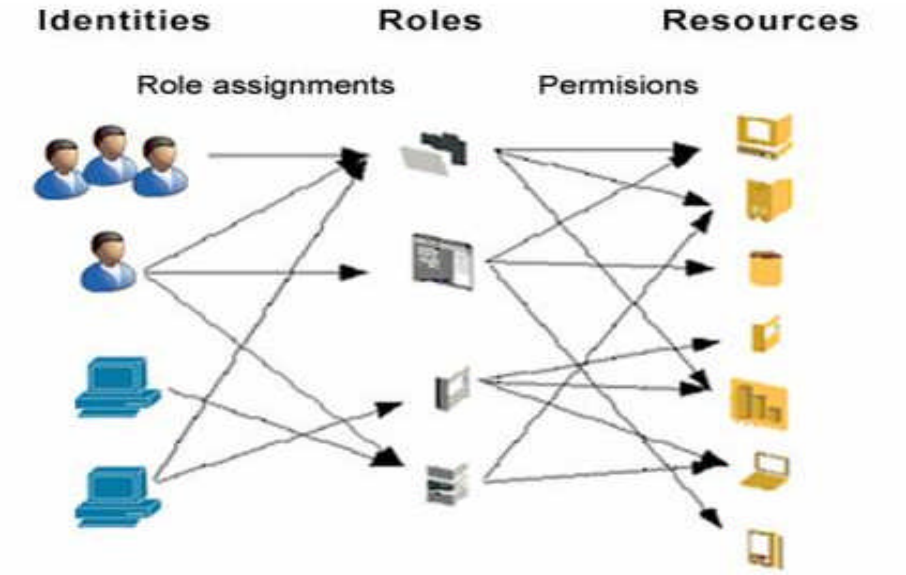
5.1.2 Role-based Security Mechanisms

Figure 5.3 : Role based security model



As being stated in IBM, " A role based security model provides a way for administrators to control user and group access to objects that are under a defined security point within the object hierarchy according to the role the user or group is expected to perform within the organizations." For example, within a hospital system the role of doctor can include operations to perform diagnosis, prescribe medication, and order laboratory tests; and the role of researcher can be limited to gathering anonymous clinical information for studies. (NIST/ITL Bulletin)

Figure 5.4 : Role based access model



Role-Based Access Control (RBAC) is a non-discretionary access control mechanism which allows and promotes the central administration of an organization's specific security policy. Once the transactions of a Role are established within a system, these transactions tend to remain relatively constant or change slowly over time. The administrative task consists of granting and revoking membership to the set of specified named roles within the system. When a new person enters the organization, the administrator simply grants membership to an existing role. When a person's function change within the organization, the user membership to his existing roles can be easily deleted and new ones granted. Finally, when a person leaves the organization, all memberships to all Roles are deleted. For an organization that experiences a large turnover of personnel, a role-based security policy is the only logical choice (Ferraiolo 1992). Enterprise

Systems including Microsoft Active Directory, Microsoft SQL Server, SELinux, grsecurity, FreeBSD, Solaris, Oracle DBMS, PostgreSQL 8.1, SAP R/3, accepted the model to manage user privilege.

As R. Margaret said about the public key infrastructure "A PKI (public key infrastructure) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. Although the components of a PKI are generally understood, a number of different vendor approaches and services are emerging. Meanwhile, an Internet standard for PKI is being worked on. The public key infrastructure assumes the use of public key cryptography, which is the most common method on the Internet for authenticating a message sender or encrypting a message."

Cryptographic algorithms are series of procedure which used to receive and deliver messages in a cryptographic system. Cryptographic algorithms is a procedure that protects the data by from unauthorized people. These algorithms have a wide variety of uses, such as ensuring the security and authenticated financial transactions. Most cryptography algorithms involve in the use of encryption, which it allows two parties to communicate but in the same time, it's preventing unauthorized third parties from understanding those communications. Encryption converts human readable plain text into something

unreadable, also known as *ciphertext*. The encrypted data is then decrypted to restore it, making it understandable to the intended party. Both encryption and decryption operate based on algorithms.

5.2 HEALTHCARE INFORMATION SYSTEM

Based on Wikipedia, Healthcare Information Systems (HCIS) is a discipline at the intersection of information science, computer science and health care. Healthcare Information Systems is a system that integrates the data collection, processing, reporting and the use of information. This system is necessary to improve the health service effectiveness and the efficiency through better management at all levels of health services. The HCIS provides a comprehensive purchasing program for long period care facilities. It also offers a claims management, nurse consulting and consultant dietician services. Healthcare Information System meant for meticulously maintaining the patients' health care records and ensuring the information or the patients' data are confidential and secure being kept. The person who is in charge of maintaining, updating and securing all of the patients' health care information must have tremendous attention to detail.

HCIS is being used by hospitals, nursing and residential care facilities, physicians and surgeons, other ambulatory health care services, medical and diagnostic laboratories, dentist and dental clinics, home health care services, other health practitioners and outpatient care center. HCIS is highly personal as a conclusion, any kind of data or information being transferred between parties via the technology could fall into wrong hand and it involves lots of risk. Thus, patients' perceived probability of compromised privacy is often higher than the actual probability. The electronic information can be

made as secure as paper records and the electronic storage may be perceived as having a higher likelihood of leakage. This would attract the media attention.

5.3 GNU HEALTH

What is GNU? Who created the GNU software? Richard Stallman is the person who responsible in the making of GNU software which it has been launched in 1983 and until now he remains as the Chief GNUisance. The word GNU is pronounced as g'noo, which we were saying 'grew' but the *r* being replaced with *n*. GNU is a recursive acronym that means GNU's Not Unix—a way for giving tribute to the technical ideas of Unix but at the same time they state that GNU and Unix is a different thing. Technically, the GNU is like a Unix but unlike the Unix, the GNU gives the users' freedom. The name "GNU" was chosen because of these three reasons; first, it was a recursive acronym for "GNU's Not Unix", second, because it was a real word, and third, it was fun to say. GNU is an operating system which would combine all together with the people in the organizations for the free will of all software and the users can control their computing.

Figure 5.5 : GNU software logo

The aim of GNU is to present a Unix-compatible system that would be 100% a free software. The word “free” in ‘free software’ pertains the freedom of the users not the price. Once the users have the software, they have four specific freedoms. The first freedom is freedom the to run the program as they wish. Next is the freedom to make copies of this programme and give it to your friend or co-workers. Besides that, the users also get the freedom to change the programme as they wanted because they have the full access to the source code. Lastly, the users have the freedom to distribute an improved version to help build the community but if you redistribute the GNU software, you may charge a fee for the physical act of transferring or gives away copies.

Figure 5.6 : GNU Health logo

Figure 5.7 : United Nation University logo

Luis Falcon has started the GNU Health as a project for the health promotion and the disease prevention in the rural areas. It has an initial name which is Medical. Today, GNU Health has evolved into a health and hospital information system (HIS), with a multi-disciplinary international teams of contributors. It is being used by the United Nations, publics hospitals and Ministries of Health and private institutions around the globe. GNU Health is a project under GNU Solidario which is one of the non-profit non-government organizations (NGO) that's worked in the area of health and education with a free software. The purposes of the GNU Health are to run in the health centres, to take care of the daily clinical practice and to manage the health centre resources. GNU Health/Solidario and United Nations University International Institute for Global Health (UNU-IIGH) has signed an agreement in 2011 with a mission to train health professionals around the world on the systems, as a way of promoting free software in the public health especially in emerging economies. Since then, both of the organizations have been cooperating and expanding their network of partners to deliver health in a universal way which also works towards the UN's Millenium Development goals.

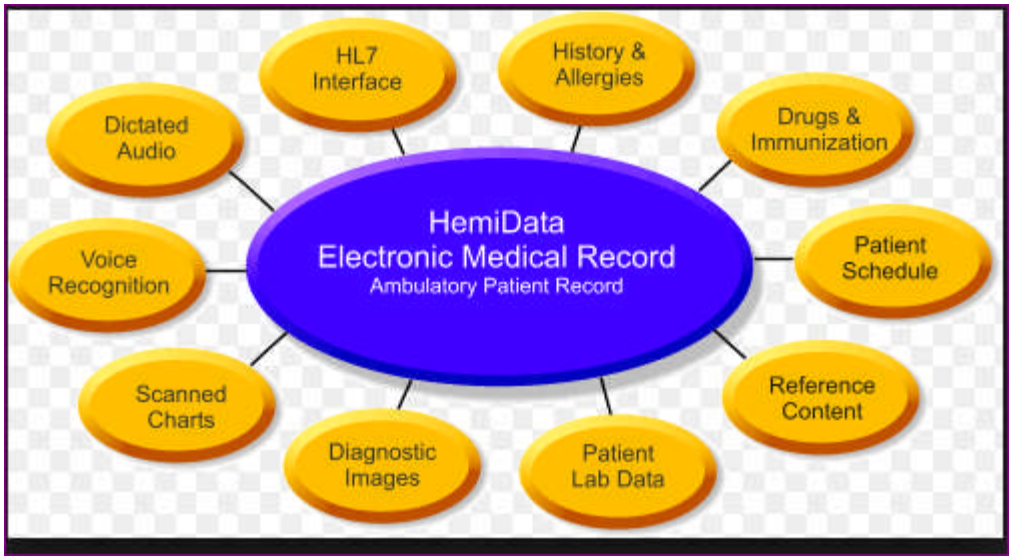
GNU Health's goal is to contribute with the health professionals around the world. Together, they think and researches to improve the lives of the underprivileged and provide a free system that optimizes about the health promotion and disease prevention. The GNU Health software is an official GNU Package, and the Hospital Information System (HIS) was adopted by the United Nations University International Institute for Global Health (UNU-IIGH), for the implementations and trainings.

GNU Health is a free Health and Hospital Information System with the following functionality:

- Electronic Medical Record (EMR)

EMR is a digital version of a paper chart that contains all of patients' medical data that originally would be found in the paper based on the record. It contains all the information ranging from pathology, radiology and clinical information that has been combined and structured in a digital form. An EMR is mostly used by providers for diagnosis and treatment. EMR was designed to capture and re-present data that accurately capture the state of the patient all the times. It also allows the user to view the entire patient history without the need to track down the previous medical record volume. Everything being viewed is accurate, appropriate and legible. EMR also reduces the chances of the data replication because there is only one modifiable file which means the file is regularly up to date when it viewed. Due to the information that compiled in one file, it makes the works much more effectively when it needed to extract the medical data of the possible trends and long term changes in the patient.

Figure 5.8 : Patient record in electronic medical record (EMR)

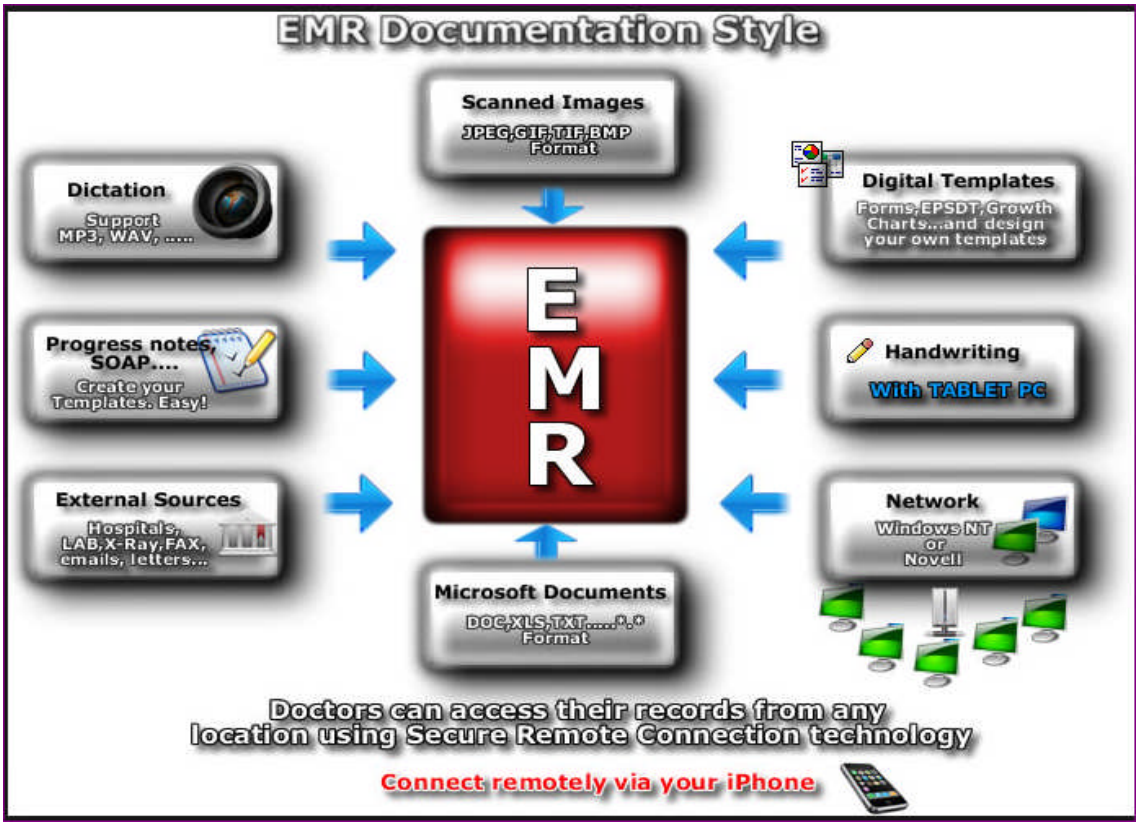


The benefits of EMR are we can track data over time which means we can follow all the information from the beginning until now. Secondly, EMR can identify patients who are due for preventive visits and screenings. Besides that, EMR also can monitor the patients reading measurement such as the vaccinations and blood pressure readings. Lastly, EMR can help to improve the overall quality of care in a group. The information and the data that have been stored in the EMR cannot be easily shared with the providers outsides the group. A patient's record might even have to print it out first and then delivered it using the mail to specialists and other members of the care team.

An EMR contains the standard of the medical and clinical data gathered in one provider's office. Electronic health records (EHRs) go beyond the data which have been collected at the provider's office and it includes more comprehensive patient history. For example, EHRs are designed to contain and share information from all providers involved in a patient's care. EHR data can be created, managed, and consulted by authorized providers and staff from across more than one health care organization.

Unlike EMRs, EHRs also allow a patient's health record to move with them—to other health care providers, specialists, hospitals, nursing homes, and even across states.

Figure 5.9 : Documentation style of an EMR.



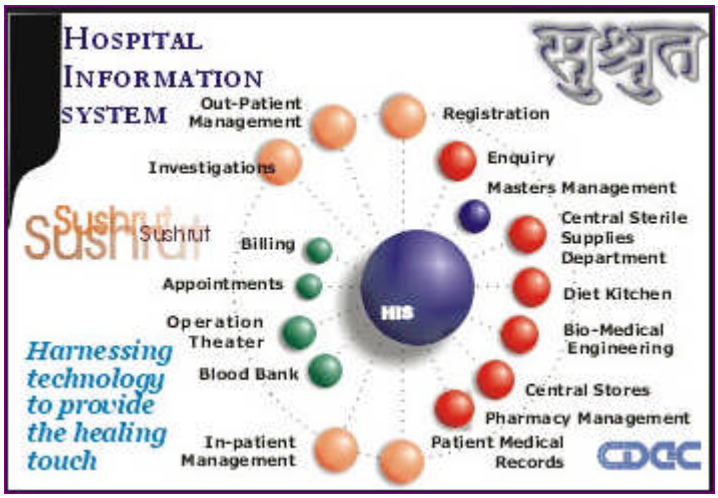
The goal of EMR is to improve the care quality, safety, efficiency, and reduce health disparities. The improvement can be done in the quality and safety of the measurement, the clinical decision support (automated advice) for providers and the patient registries (example : "a directory of patients with diabetes"). Furthermore, the EMR goal is to improve the care coordination and to engage the patients and families in their care. EMR also would like to improve the population and the public health regarding to these three things which are electronic laboratory reporting for reportable conditions (hospitals), immunization reporting to immunization registries and syndromic

surveillance (health event awareness). The last goal of EMR is to ensure adequate about the privacy and security protections.

- Hospital Information System (HIS)

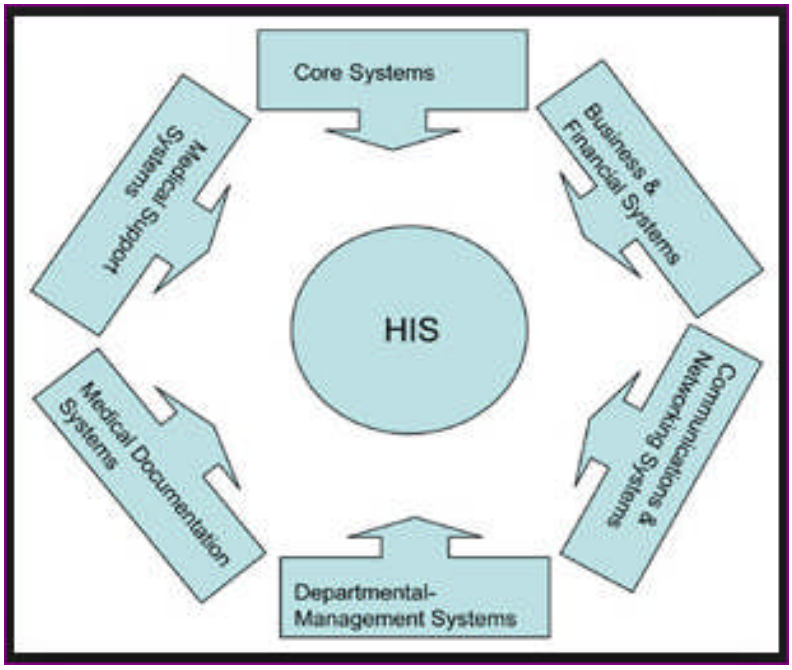
Hospitals are extremely a complex institution with large departments and lots of units care for the patients. Hospitals are becoming more dependent on the ability of hospital information system (HIS) to assist in the diagnosis, management and education for a better and to improve services and practices. In the health organization such as the hospitals, implementation of HIS as predictable due to many mediating and dominating factors such as the organization, people and technology. The HIS was designed to manage all the medical, administration, financial and legal aspects of a hospital and the process of the services. Hospitals provided a medical assistance to patients is one of the most important issues in health services. HIS was introduced in 2011 at the International Conference on Social Science and Humanity.

Figure 5.10 : Hospital Information System



HIS can be defined as a massive and integrated systems that support the comprehensive information requirements of the hospitals which it include the patients, clinical, ancillary and financial management. The aim of HIS is to achieve the best possible support of patient care and administration by presenting the data where it needed and acquired. It also helps to keep doctors, nurses, and other hospital personnel informed and up-to-date. Hospital information systems are implemented through various IT companies that specialize in health informatics.The HIS requires correct storage of data, reliable for the usage, fast for reaching the data, secure to keep the data and lower in cost for the storage. HIS systems also help with the collaboration between different hospitals in order to reduce duplicate testing. Time is also saved by looking at previous data instead of having to re-write it every time the patient goes to a different hospital. The HIS provided a common source of information about the health history of the patient.

Figure 5.11 : Functional Model of a Hospital Information System



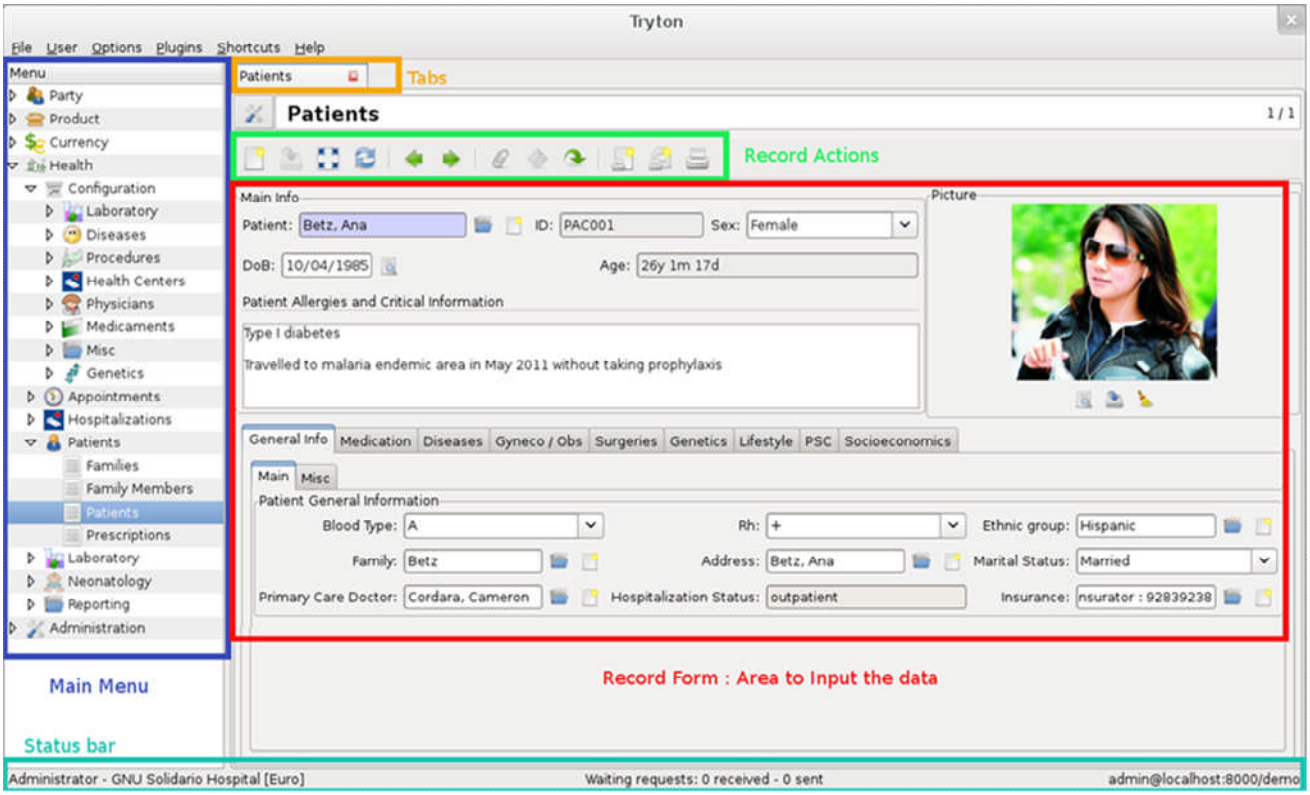
HIS are programmed to collect, process, and retrieve patient care and administrative information ensuring better ROI and delivery of the service. If the hospital authorities have more relevant information they can make better decisions. HIS in leverage is a highly optimized core library that ensures the delivery of operational and administrative information required by users. A centralized information system can be customized according to the specific requirements of a hospital. A hospital can tell the solution by providing its needs and the applications can then be moulded to deliver exactly who was demanding it. For instance, you can demand a solution for easy retrieval of information. You can also ask the vendor for a HIS that has user friendly features and a multilingual interface that can be used by a diverse workforce.

- Health Information System

The health information system is referring to any systems that captures, stores, manage and transmit information which it is related to the health of individuals or a group or organizations. Health information systems is an integrated effort in collecting, processing, reporting, and the use of health information and knowledge. This is to influence the policy and decision making , programme action, individual and public health outcomes It is designed to be multi-platform software, so it can be installed in different operating systems such as GNU/Linux, Free BSD, MS Window and different database management systems (PostgreSQL). It's written in Python and using Tryton framework.

What is Tryton? Tryton is an ERP application framework. It is written in Python Programming Language. During the research at United Nations University, Tryton was selected as the base ERP application framework for modelling HIS modules. Tryton already contains 181 Modules that cover most important business functions within organizations.

Figure 5.12 : Tryton user interface



The main application are discussed by the colour of the box. For the blue box, it contains a hierarchy menu item that allows different departments to manage the information in a shared database. For the orange box, it is the list of the menus that users opens via the menu option and in the green box it is the shared toolbar that allows users to to access to the information. Buttons are general buttons that can do general commands. For example, the first button can create a new

record and second one can save records , etc. In the red box, it is the main part of the page that represents the information in a form.

Figure 5.13 : Tryton

List of modules that using the Tryton :

1. Standard Core Modules
2. Tryton Business Modules (ERP System)
3. GNU Health Modules (Hospital Information System)
4. United Nations Modules (Optimizing the Solution)
5. Your Hospital Modules (Customizing the Solution)

CONCLUSION

In essence, security and privacy concerns within every healthcare and hospital must always crucially be updated especially to protect the health care system management, their clinical data and also their patients 'confidential personal data. Therefore, it has been acknowledged that security planning should be implemented to the hospital information system which has a place in charge of the protecting the data available within the hospitals. In fact, many security techniques and plans have been established to secure those private and confidential data. This includes the Pseudonymization Techniques, Health IT Security, and Security Review Framework which have been personally made up to cover this problem.

Pseudonymization Techniques has been purposed to protect the health records of every patient from any unauthorized access which has the same objective that is to keep securing the patients' personal data and their confidential records of health. The methodology of Pseudonymization Techniques was to prevent any data disclosure that might negatively influence a patient's life by having denied of health insurance or employment. It could clearly be seen that this technique was mainly focusing to protect the patients' personal privacy by having it replaced with another name, symbols or code.

Meanwhile, the Health IT Security basically has put their focus on the security aspects of management of health information across the computerized systems in the organizations. Therefore, Health Information Technology (HIT) has been viewed as the most promising tool to improve the quality, safety and the efficiency of a health management system. This security system has helped the hospitals, clinic and pharmacies in managing the data of health

information through a software namely; GNU Health software. Instead of managing collected data in a more proper way, the software also can help to improve the privacy and the security of the data.

For the same reasons, the Security Review Framework has been proposed to be implemented within the Hospital Information System (HIS) in order to keep the data management in the hospitals, clinics and pharmacies from leaking out and to make sure that it will always be firmly protected. In the other words, the Security Review Framework was proposed with some principles and guidelines that can be used in understanding the goals of implementing the Software Development Life Cycle (SDLC) process in HIS. This is due to the needs of the organization to keep improving the organizations' security systems as well as achieving their goals to develop their security standards, effective security management practices, and to build the confidence in inter-organizational activities while managing their organizations' data privacy and security.

REFERENCES

1. (March, 2012) CMS.gov,Center for Medicare and Medicaid Services : Electronic Health Records. Retrieved from http://www.cms.gov/Medicare/EHealth/EHealthRecords/index.html?redirect=/ehealthrecords/

2. Oxford Dictionaries : Definition of pseudonymous in English. Retrieved from http://oxforddictionaries.com/definition/english/pseudonymous?q=pseudonymous

3. Cambridge Dictionaries Online : Pseudonym. Retrieved from http://dictionary.cambridge.org/dictionary/british/pseudonym?q=pseudonymous

4. Creative Commons Attribution-ShareAlike License (March, 2013). Wikipedia : Pseudonymization. Retrieved from http://en.wikipedia.org/wiki/Pseudonymization

5. A.R. Yahya, S. Shahrin & A.G. Mohd Khanapi (2012). Pseudonmization Techniques for Privacy Study with Clinical Data. Retrieved from http://article.sapub.org/10.5923.j.ijis.20120206.02.html

6. D. Lazarus, A tough lesson on medical privacy: Pakistani transcriber threatens UCSF over back pay, San Francisco Chronicle Wednesday, October 22, 2003.

7. Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

8. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of per-sonal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

9. M. Caloyannides, Society cannot Function without Privacy, IEEE Security and Privacy, vol. 1, No. 3, May—June 2003.

10. F. De Meyer, B. Claerhout, G.J.E. De Moor, The PRIDEH project: taking up privacy protection services in e-health, in: Proceedings MIC 2002 ‘‘Health Continuum and Data Ex-change”, IOS Press, 2002, pp. 171—177.

11. G.J.E. De Moor, B. Claerhout, F. De Meyer, Privacy en-hancing techniques: the key to secure communication and management of clinical and genomic data, Meth. Inf. Med. 42 (2003) 148—153.

12. D.J. Solove, M. Rotenberg, Information Privacy Law, Aspen Publishers, New York, 2003.

13. [8] First draft of AURTAF, Anonymity User Requirements for Trusted Anonymisation Facilities. CEN/TC 251/WG III N 02- 018 (2002-07-17).

14. L. Peter, M. Micheal, P. Kryzsztof, P. Steffen. Privacy Enhancing Techniques : A Survey and Classification. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.69.2460&rep=rep1&type=pdf

15. Andrew R. Mark. (2000). The Development of Destination-Specific Biometric Authentication. Computer, Freedom & Privacy Conference 2000. 77-80. http://www.cfp2000.org/papers/mark.pdf

16. HIS Hospital Information Systems Solutions. (n.d.) Retrived from website Goomedic.com website http://www.goomedic.com/his-hospital-information-systems-solutions-and-software-free-open-source-and-commercial

17. Hospital Information System (HIS). (2013). Retrieved from EMR Consultant website: http://www.emrconsultant.com/education/hospital-information-systems

18. Kwangsoo Lee , Thomas T. H. Wan and Hyuk Jun Kwon. (2012). The relationship between healthcare information system and cost in hospital. Personal and Ubiquitous Computing© Springer-Verlag London Limited 2012. doi: 10.1007/s00779-012-0574-6.

19. Margaret Rouse. (2008). Nonrepudiation. Retrieved from SearchSecurity website: http://searchsecurity.techtarget.com/definition/nonrepudiation

20. Sarah Landolt, Jürg Hirschel, Thomas Schlienger, Walter Businger, Alex M Zbinden. (2012). Assessing and Comparing Information Security in Swiss Hospital. Interactive Journal of Medical Research, Interact J Med Res | vol. 1 | iss. 2 | e11 | p.1. http://www.ncbi.nlm.nih.gov/pubmed/23611956

21. Takeshi Yamazaki. (2005). Unauthorized Access Control Apparatus between Firewall and Router. United States Patent Application Publication Yamazaki Pub. N0.: US

2005/0144467 A1. Retrieved from http://www.google.com/patents?hl=en&lr=&vid=USPATAPP10858854&id=QuOWAAAAEBAJ&oi=fnd&dq=the+firewall+and+the+router&printsec=abstract#v=onepage&q=the%20firewall%20and%20the%20router&f=false

22. Tim Fisher. (n.d.). Hard Disk Drive. Retrieved from About.com Guide website: http://pcsupport.about.com/od/componentprofiles/p/p_hdd.htm

23. Tim Fisher. (n.d.) Random Access Memory (RAM). Retrieved from About.com Guide website: http://pcsupport.about.com/od/componentprofiles/p/p_ram.htm

24. Appari, A. & Johnson, M. E. (2010). *Information security and privacy in healthcare; current state of research.* Retrieved from http://abouthipaa.com/wp-content/uploads/Information-security-and-privacy-in-healthcare_Current-State-of-Research.pdf

25. Ann E.K. Page. (n.d.) *Chapter 22. Practice Implications of Keeping Patients Safe.* Retrieved from http://www.ahrq.gov/professionals/clinicians-providers/resources/nursing/resources/nurseshdbk/PageA_PIKPS.pdf

26. Australian Government, Department of Foreign Affairs and Trade. (2013). *Fraud Control Plan 2013.* Retrieved July 19, 2013, from http://www.dfat.gov.au/publications/fraud-control-plan/executive-summary.html

27. Beth Burmahl & Suzanna Hoppszallern. (2012). 2012 Hospital security survey. High-tech security system installation and operation requires a team effort. HFM Magazines. Retrieved from website Health Facilities Management:

http://www.hfmmagazine.com/hfmmagazine/jsp/articledisplay.jsp?dcrpath=HFMMAGAZINE/Article/data/10OCT2012/1012HFM_CoverStory

28. Boonstra, A. & Vries, J.D. (2004). *Analyzing inter-organizational systems from a power and interest perspective*. Retrieved from http://som.eldoc.ub.rug.nl/FILES/reports/themeA/2004/04A12/04A12.pdf

29. Children's Hospital of Eastern Ontario Research Institute (2011, May 17). Secure protocol for medical data disclosure developed. *ScienceDaily*. Clifton, C. & Bishop, M. (2003). *Systems with Assurance Evaluation Auditing.* Retrieved from http://www.sis.pitt.edu/~jjoshi/IS2935/Lecture10.pdf

30. Cutler, D.M. (1996). *Public Policy for Health Care.* Retrieved from http://www.nber.org/papers/w5591

31. David Blumenthal. (2011). Wiring the Health System — Origins and Provisions of a New Federal Program. The New England Journal of Medicine. N Engl J Med 2011; 365:2323-2329. DOI: 10.1056/NEJMsr1110507.

32. Devon M. Herrick, Linda Gorman & John C. Goodman. (2010). Health Information Technology: Benefits and Problems. National Center For Policy Analysis. ISBN #1-56808-203-7. Retrieved from National Center for Policy Analysis website: http://www.ncpa.org/pdfs/st327.pdf

33. Internet Users in the World Distribution by World Regions. (2012). Internet World Stats. Usage and Population Statistics. Miniwatts Marketing Group. Retrieved from the Internet World Stats website: http://www.internetworldstats.com/stats.htm.

34. Judith Hurwitz, Robin Bloor, Marcia Kaufman & Fern Halper. (2012). What Is Cloud Computing? Hybrid Cloud For Dummies. ISBN: 978-1-118-12719-3.

35. Margaret Rouse. (2010). Health IT Definition. Retrieved from SearchHealthIT website: http://searchhealthit.techtarget.com/definition/Health-IT-information-technology

36. Nexus. (n.d). *Physical Security for Healthcare.* Retrieved July 19, 2013 from http://www.nexusis.com/industries/healthcare/healthcare-physical-security/

37. Pittsburgh. UPMC. (n.d). *Privacy and Security Awareness; Self-Directed Learning Course for All UPMC Staff.* Retrieved July 19, 2013 from http://www.upmc.com/healthcare-professionals/education/advance-practice-providers/education/Documents/HIPAA%20Training%20Manual.pdf

38. PMI Healthcare Community of Practice. (2010). *About This Community: About Us.* Retrieved July 19, 2013 from http://healthcare.vc.pmi.org/Public/AboutthisCommunity.aspx

39. PMI Healthcare Community of Practice. (2010). *PMI Privacy Policy.* Retrieved July 19, 2013 from http://healthcare.vc.pmi.org/Public/PrivacyPolicy.aspx

40. PMI Healthcare Community of Practice. (2010). *Welcome to the PMI Healthcare Community of Practice.* Retrieved July 19, 2013 from http://healthcare.vc.pmi.org/Public/Home.aspx

41. Rath, A.T. & Colin, J.N. (2013). *Towards enforcement of purpose for privacy policy in distributed healthcare.* Retrieved from http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6488578&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6488578

42. Reassessing Your Security Practices in a Health IT Environment: A Guide for Small Health Care Practices. (n.d.). Retrieved from Health IT website: http://www.healthit.gov/sites/default/files/small-practice-security-guide-1.pdf

43. Rostad L. (2009). *Access Control in Healthcare Information Systems.* Retrieved from http://ntnu.diva-portal.org/smash/get/diva2:134515/FULLTEXT02.pdf

44. Schlienger, T. & Teufel, S. (n.d). *Information Security Culture-from Analysis to Change.* Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.7158&rep=rep1&type=pdf

45. SearchHealthIT. (n.d.) *Guide: Health care data interoperability.* Retrieved July 19, 2013, from http://searchhealthit.techtarget.com/guides/Guide-Health-care-data-interoperability#content

46. Study on Patient Privacy & Data Security Ponemon Institute, December 6th, 2012. (2012). Retrieved from the Ponemon Institute website: http://www2.idexpertscorp.com/ponemon2012/

47. Suzy A Buckovich, Helga E Rippen & Michael J Rozen. (1999). A Goal for Privacy, Confidentiality, and Security of Health Information. *J Am Med Inform Assoc* 1999;**6**:122-133 doi:10.1136/jamia.1999.0060122.

48. Symantec: Internet Security Threat Report 2013. (2013). Symantec Corporation Internet Security Threat Report 2013, pg.19 :: Volume 18. Retrieved from https://scm.symantec.com/resources/istr18_en.pdf

49. United Kingdom. NHS choices. (2012). *Consent to treatment.* Retrieved July 19, 2013 from http://www.nhs.uk/Conditions/Consent-to-treatment/Pages/Introduction.aspx

50. U.S. Department of Health & Human Services.(n.d.) *Health Information Privacy*. Retrieved July 19, 2013, from http://www.hhs.gov/ocr/privacy/

51. Fragopoulos, A. Glialelis, J. & Serpanos, D. (2008). *Security Framework for Pervasive Healthcare Architectures Utilizing MPEG-21 IPMP Components*. Retrieved from http://www.hindawi.com/journals/ijta/2009/461560/

52. University of California Santa Cruz. (2012). *Information Technology Services; Security Review* .Retrieved July 1, 2013, from http://its.ucsc.edu/itsm/securityrev.html

53. Blanchard, C.W. (2000). *3G Capabilities and Security Review Framework (Draft).* Retrieved from http://www.3gpp.org/ftp/tsg_sa/wg3_security/TSGS3_11_Mainz/Docs/PDF/S3-000175.pdf

54. Kurniawan, R. (2013). *Hospital Information System (HIS): Implementation, Challenges and Security Planning.* Indonesia: Health IT Security Forum.

55. Glynn, F. (2013). *Software Development Life Cycle (SDLC).* Retrieved from http://www.veracode.com/security/software-development-lifecycle

56. Samy, N.G. Ahmad, R. Ismail, Z. (2009). *Threats to Health Information Security*. Retrieved from http://www.ccf.org.cn/resources/1190201776262/2011/06/30/P10138301.pdf

57. Whitteker, M. (2010). *Building a Comprehensive Security Architecture Framework.* Retrieved from http://raleigh.issa.org/downloads/Building_a_Security_Architecture_Framework.pdf

58. *Security Development Lifecycle: SDL Threat Modeling Tool* (2013). Retrieved July 10, 2013, from http://www.microsoft.com/security/sdl/adopt/threatmodeling.aspx

59. Opdahl, A.L. Sindre, G. (2009). *Experimental comparison of attack trees and misuse cases for security threat identification.* Retrieved from http://www.sciencedirect.com/science/article/pii/S0950584908000773

60. California Department of Health Care Services. (2012). *Health Insurance Portability and Accountability Act.* Retrieved July 10, 2013, from http://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00%20WhatisHIPAA.aspx

61. Jack, A. (2012). *Vendor Evaluation in MM-PUR.* Retrieved from http://wiki.sdn.sap.com/wiki/display/ERPSCM/Vendor+Evaluation+in+MM-PUR

62. International Organization for Standardization (ISO). (2008). *ISO/IEC 27002:2005; Information technology-Security techniques-Code of Practice for Information Security Management.* Retrieved July 10, 2013, from http://www.iso.org/iso/catalogue_detail?csnumber=50297

63. *Penetration Testing Guide* (n.d.). Retrieved July 10, 2013, from http://www.penetration-testing.com/home.html

64. (2011), GNU Operating System : About the GNU Operating System. Retrieved from http://www.gnu.org/gnu/about-gnu.html

65. (2013), GNU Operating System : Overview of the GNU system. Retrieved from http://www.gnu.org/gnu/gnu-history.html

66. (July, 2013) GNU Health. Retrieved from http://en.wikipedia.org/wiki/GNU_Health.

67. Jen, (March, 2013) Open Source : Success of GNU Health goes beyond free software. Retrieved from http://opensource.com/health/13/3/interview-luis-falcon-gnu-health

68. Creative Commons Attributions ShareAlike License, (June, 2013) Hospital Information System. Retrieved from http://en.wikipedia.org/wiki/Hospital_information_system

69. GobiernoUSA.gov, Benefits of EHR : What is an electronic medical record (EMR). Retrieved from http://www.healthit.gov/providers-professionals/electronic-medical-records-emr

70. Creative Commons Attributions ShareAlike License, (July, 2013) Electronic Medical Record (EMR). Retrieved from http://en.wikipedia.org/wiki/Electronic_medical_record

71. R. Maria, slideshare : Managemant Information System in Health Care. Retrieved from http://www.slideshare.net/NewNurseMaria/management-information-system-in-health-care

72. Creative Commons Attributions ShareAlike License, (July, 2013) Health Informatics. Retrieved from http://en.wikipedia.org/wiki/Health_information_system

73. (May, 2013) Social Security : Health Information Technology (Health IT). Retrieved from http://www.ssa.gov/hit/our-initiative.html

74. (2013) Heavy Reading IP Service Insider : Healthcare Sector Turns to MLPS VPNs for a Data Cure. Retrieved from http://www.heavyreading.com/entvoip/details.asp?sku_id=2804&skuitem_itemid=1381

75. AuthenticationWorld.Com, Hutington Ventures Ltd. (2006) The Business of Authentication : Authentication – Biometrics. Retrieved from http://www.authenticationworld.com/Authentication-Biometrics/

76. IBM : Role Based Security Model. Retrieved from http://pic.dhe.ibm.com/infocenter/op/v6r2m0/index.jsp?topic=%2Fcom.ibm.swg.ba.cognos.administrators_guide.6.2.0.doc%2Fc_adm_about_role-based_security_models.html

77. R. Margeret (2006) PKI (public key infrastructure). Retrieved from http://searchsecurity.techtarget.com/definition/PKI

78. (n.d) wiseGeek, clears answer for commoners : What are Cryptographic Algorithms? Retrieved from http://www.wisegeek.com/what-are-cryptographic-algorithms.htm

AUTHOR'S PROFILES

Associate Professor Dr. Zuraini Ismail

Associate Professor Dr. Zuraini Ismail is the Head of Department (Information Security) at the Advanced Informatics School (AIS), Universiti Teknologi Malaysia. She obtained her PhD. in Information Systems from the International Islamic University of Malaysia, Masters in Computer Information System at the University of New Haven, Connecticut, USA as well as her Bachelors in Science (Information Systems) at the University of Southern New Hampshire, New Hampshire, USA. Her area of specialization are in the field of Information Security Management System, Operational and Physical Security, Information Security Governance, IT Security Policy, Computer Ethics & Privacy, Business Continuity Planning, Disaster/Business & Recovery Planning, Cyber Security and IT Outsourcing.

Dr. Nurhizam Safie, Research Fellow (UNU-IIGH)

Dr Nurhizam Safie is a Research Fellow whose research and professional consultancy focuses on open source healthcare and Hospital Information Systems (HIS) in developing

countries, green computing and sustainability, ICT security & privacy and e-learning. Nurhizam Safie is a member of the Malaysian National Computer Confederation as well as member of numerous international programme committees and editorial review boards. Nurhizam Safie holds a Ph.D. in Management Information Systems, Master in Information Technology, B.HSc. in Psychology and a Diploma in Human Development. His other major research projects include ICT project and change management in healthcare information systems and e-learning for healthcare professionals.

Mr. Yahaya Abd. Rahim, Lecturer and PhD. Candidate (UTeM)

Mr. Yahaya Abd. Rahim holds a Masters Science in Information Technology from Universiti Teknologi Malaysia (UTM) , BSc (Honors) Information Technology from Universiti Utara Malaysia (UUM) and currently is pursuing his PhD at Universiti Teknikal Malaysia Melaka (UTeM), He joined Universiti Teknikal Malaysia Melaka (UTeM) in 2003 as a Lecturer at the Faculty of Information and Communication Technology. Yahaya has been active at all levels of the faculty initiating and building the teaching and incorporation of research methods in both design research and design practice. Current interests also include green computing, e-waste management, design of research methods, technology and performance

Hadi Syahrial, Researcher and Lecturer, PhD Student at Binus University

Hadi Syahrial is a researcher and lecturer at the Master of Computer Science Program Budi Luhur University (Jakarta, Indonesia). He holds a Master in Computer Science from Budi Luhur University, Master in Management from STIE Trianandra (Jakarta, Indonesia), Master of Business Administration from STIE Trianandra – Hogeschool van Utrecht (Netherland) and currently pursuing his PhD at Binus University (Jakarta, Indonesia). He also holds the CEH, CHFI, and ISO 27001 LA certifications. Hadi Syahrial is the founder of Pesantren - Cyber Security Incident Response Team (Pesantren CSIRT). Pesantren CSIRT is Islamic Boarding School for Cyber Security Research. Current interests also include Business Intelligence, Enterprise System, Information Security Management System, Business Continuity Management, Nanotechnology, and Spiritual Computing.

Seyed Mohammad Motahar, PhD. Candidate (UKM)

Seyed Mohammad Motahar is an ICT researcher and inventor. He holds an Executive Master in Open Source Computing from Asia e University (AeU) and currently pursuing his PhD in UKM. He has more than ten years professional experience in software engineering and testing in the Business Information Systems using various open source frameworks and programming tools. He has received national and international prizes for his

innovative ICT solutions and inventions and he is collaborating and contributing to open source software communities in the industry and leading academic bodies. His research interest focuses on topics related to enterprise application development frameworks. He is conducting on-going researches on evaluation of open source enterprise resource planning (ERP), particularly in virtualisation and their adoption in vertical market with the focus on healthcare and sustainability.

Riza Kurniawan

Riza Kurniawan holds Bachelor of Mechanical Engineering from ITN Malang. Interested in the programming since 8 years old and the first known language is "Basic". Since 1998 began active in Open Source. In 2002 founded R-Tech Softmedia, which is of IT consulting firm with specialization Audit Security System and Open Source ERP Implementation. Had a lot of handling problems-problems in the field of security and system integration, both at the Company and at Hospital. Currently focusing on developing Integration HIS base on Open source under the name Open Sikes and O-Health.