Awareness of Hospital Information Systems Security: Perspective from King Saud University Hospitals

Saleh Al-Zahrani.Information Systems Department. Faculty of Computer and Information Science. Imam Mohammad Bin Saud Islamic University

DRsalehz@hotmail.com

Abstract

This paper provides an overview of the information security and risks associated with the use of hospital information systems in King Saud University Hospitals in Saudi Arabia. It highlights to what extent medical and ICT staffs are aware of possible consequences of releasing patient information. However, considering confidentiality and sharing password were examined. Types of information and data that access, update or share among staff in hospitals were identified. Usually, all originations protect their hospital computer systems against several misuse and malicious threats. This study attempt to find out the key issues that concern all professionals' staffs with the use of their hospitals Information Systems.

The findings of this paper draw our attention to the issues of Hospital Information Systems Security. These issues are of concern to all those involved with the introduction and utilizations of hospitals information systems. Literature indicates that threat to computer comes from insiders, On the contrary, this study report the most important dangers threat come from out side. It is clear that this study can be considered as pioneering in area of hospital information systems security in Saudi Arabia. It sets out to provide an attempt to fill the knowledge gap that exists in hospital information systems in the developing countries.

1. Introduction

Information and communication technology (ICT) have grate impact on health care organisations and all professionals' staffs. Yet, the advent of computer networks for health community has led to concern about information security. Doctors and other professionals are worried that making patient information more widely available may endanger patient confidentiality and privacy. It has become quite clear from studies undertaken by (Anderson,

Information Security Symposium, Taibah University. College of Computer Science and Engineering 2-4 May, 2006:159-173

and Brann 2000) that the security of health information and medical patient records are near the top of the concerns of patient and health care professionals all over the world. In addition, (Barber,et al 1998) state that data protection and information systems security have been part of the background of the development of Medical Informatics since the very early days. Moreover, informatics is developing very fast in the areas of networking and security threats and countermeasures.

Health information and medical records are among the most sensitive data that are acquired, used, and disclosed by government and the private sector. The increasing potential for disclosure of patient's information within a rapidly-developing national health information infrastructure, facilitated by massive computerization of records and other ICTdevelopments, presents significant risks to individual privacy. Authors such as (Claerhout and DeMoor 2005, Gritzalis et al 2004, Sciamanna et al 2005 and Couchman et al 2005) claim that health information privacy, of is a two-edge sword. While it is important in respecting the autonomy and dignity of individuals, excessive amounts of privacy can impede many of the goals of the health care system.

Computer networks alleviate communication among different parties or organisations in healthcare systems. Conversely, networks increase the danger of malicious access to confidential data. Exchange of medical information is very important among healthcare organisations for the benefit of both patients and society. However, it is hard to balance between the need for data exchange and the need to protect the information from alteration or misuse. Unfortunately, medical information sometimes might be misused and/or used for malicious purposes. For example, (Anderson and Brann 2000) presented some examples, such as one the case in which a physician in the USA sold patient records to a car dealer and state employees in Maryland who sold patient information from the state medical database. They also revealed that The Sunday Times reported that, in the UK, anyone's medical record could be obtained for £200.So, it is believed that the success of current technologies to protect information depends heavily on explicit policies, personal ethics and self-regulation.

ICT healthcare deployment in developed countries mainly started as an aid to increase the efficiency of the organisation, usually beginning (in the USA) with payroll and patient account functions. Nowday's computers have made wide inroads into the practice of medicine and currently developed countries using state of the art. On the bather hand, in the developing nations such as Saudi Arabia the amount of published work addressing ICT usage in healthcare and security issues is relatively low, although an increasing interest is being shown in the area.

The main goal of this study is to

1. Assess the current level of Hospital Information Systems security and risk issues associated with the adoption of computers in King Saud University hospitals.
2. To find out to what extent medical and ICT staff aware of information security?
3. Attempt to fill the knowledge gap that exists in hospital information systems in the developing countries in general and in Saudi Arabia in particular.

2. Literature review

Today hospital information security and patient information is hot issues and complex. Information security, patient confidentiality and privacy have attracted considerable attention in an academic and practical setting. Several authors have discussed and considered heath information security and confidentiality. They agree its one of the prime patient concerns, and one of the most important issues. They also, discussed different issues from different perspectives. Therefore, literature review will be divided to three parts as follow.

1. ICT Security in Health Care
2. Security threats to Hospital Information Systems
3. ICT security in Saud Arabia Hospitals

Each part of those elements will be explained briefly as follow

Information Security Symposium, Taibah University. College of Computer Science and Engineering 2-4 May, 2006:159-173

3.1.ICT Security in Health Care

The starting point of security investigation is usually a review of the security problems in a particular environment and the development of a statement of risks. A good number of such studies have been now done in health care environment.

There have been many debates in the developed nations on the issue of hospital information security and particularly that of patient information. In fact, health information is far more sensitive than the information holdings of just about every other industry and has the potential to cause much greater individual harm if it falls in the wrong hands (Amatayakul, 1999).Moreover, (Neame 1997) emphasized that the area of security is one where mistakes cannot be afforded for several reasons. There is the damage done by the mistake itself, the resultant fallout and the loss of trust in the system and its management.

It's hard to get hold of agreement among researchers and authors regarding definition of information security. Different authors come from different backgrounds and therefore, define information security from different perspective. In focus, we could define it as "The administrative, physical and technical services of mechanisms to protect the confidentiality of private information, to ensure the integrity of information so that it is accurate and complete, and make information easily available to those with legitimate right to access."

The goals of information security in healthcare were also summarised as follows by Brennan *et al.* (1997) and (Claerhout and DeMoor 2005) as well.

- to ensure the confidentiality of healthcare data and the privacy of the patient;
- to ensure the integrity of healthcare data; and,
- to ensure the availability of healthcare data for authorized persons.

Some writers, such as Claerhout and DeMoor (2005),(Yeoman 1998), (Brennan and Spours 2000), (Hojerbak 2000),(Gritzalis et al 2004), Sciamanna *et al* 2005)and (Couchman et al

Information Security Symposium, Taibah University. College of Computer Science and Engineering 2-4 May, 2006:159-173

2005) and (Furnell 1995), stressed that there is widespread agreement between physicians and managers on the need to protect sensitive information. They also believe that information security involves three main issues as follow:

- *Confidentiality*: This refers to making sure that information is only available to those who have the need to know and are properly authorised to do so.
- *Integrity*: This refers to the prevention of unauthorised change or modification of information. There is an implicit requirement for users to be able to trust the system and be confident that the same information can be retrieved as was originally entered.
- *Availability*: This refers to the information that should be made available and accessible where and when it is needed and in a suitable format to a properly authorised user.

Information is power and power demands responsibility. Therefore, all staffs in health care organisations (Doctors, physicians, nurses etc) need to be taught about the problems and ethical principal involved in handling electronic information. Medical information is very sensitive information and should be protected. Moreover, (Buchan 2001) states that the trust that exists between patients and healthcare professionals must be protected as we introduce modern decision-making tools, which are accessible world-wide, into clinical practice. He added that abuses could occur if the systems used and the policies adopted are not secure or perceived to be not secure by the public. Hospital information systems policy refers primarily to the people involved (such as patients, doctors, administrators, and health care authorities) and the data objects that should be protected (including medical records and communication data). This information security policy should be fully adopted to be effective; in addition, conformance to its regulations should be made mandatory for all members of staff. These principles and guidelines must also be complemented by measures, which are more specific. Also, when it's already exists in the hospitals. The main problem with information security in healthcare is not technology, but a lack of cohesive policy (Brennan, *et al*., 1997).In addition,

(Camp 2000) claims that many of the problems of network security in healthcare are based on the fact that networking has been integrated into healthcare but security has not. To

Information Security Symposium, Taibah University. College of Computer Science and Engineering 2-4 May, 2006:159-173

address some of the identified information security risks there are a number of solutions and techniques that can be applied, such as the following:

1. Firewalls: Firewall is a system, or a group of systems that enforces an access control policy between two networks. It is commonly used as a barrier between the secure corporate Internet, or other internal networks and the Internet, which is assumed to be unsecured (Turban *et al.*2001). However, there are three types of Firewall, such as packet filter gateways; circulate level gateways and application level gateways.
2. Public key infrastructure (PKI): This method uses a pair of keys (public and private) to encrypt and decrypt messages. Messages and data sent using PKI are encrypted and therefore, the message can only be decrypted using the private key.
3. Access control and authentication: There are different authentication methods used to increase security and access control to a network. An organisation can select one or more methods of authentication most suitable for their application. One of the most popular methods is security ID because it provides strong authentication and does not require special readers or hardware.

2.2. Security threats to Hospital Information Systems

As is well known, information systems are made up of many components that may be in several locations, each component being vulnerable to many potential hazards. Data, software, hardware and networks can be threatened by many internal and external hazards. Theoretically, there are hundreds of point can be subject to some threat. Yet these threats can be categorised as follows:

1. Unintentional threats: Unintentional threats can be divided into three major categories

- human error: This can occur in the design of the hardware programming, testing, data collocation, data entry, authorisation and instructions;
- environmental hazard: This include earthquakes, flood, fire, and power failure;
- computer system failure: This can be the result of poor manufacturing or defective materials.

Information Security Symposium, Taibah University. College of Computer Science and Engineering 2-4 May, 2006:159-173

2. Intentional threats: computer system may be damaged as result of intentional threats such as inappropriate use of data, theft of equipment or programmes, transfer of data, sabotage or malicious damage to computer resources. It can also, occur as result of destruction from viruses, miscellaneous computer abuse and hackers.

The main threats to privacy and confidentiality arise from within institution that provide patient care as well as from institution that have access to patient data for secondary purpose. Most computer security problems are come from insider. For example, Anderson and Brann (2000) state by one estimate, 85% of all computer security involve employee in the organisation. Also, problem was studied by US government office of technology assessment. It confirmed that the main threats to privacy in computerised clinical record system come from insiders rather than out side, and that they are exacerbated by the data aggregation which networked computer systems encourage(Anderson 1996).Moreover, he add that the British government admits that wide access to indefinable clinical records has no ethical basis. We can conclude that the success of technology to protect patient information depends deeply on policies, person ethics, and organisations regulation

2. 3. ICT security in Saud Arabia Hospitals

Saudi Arabia government has paid great attention to adopt ICT in healthcare institutions. Therefore, some hospitals have implemented advanced technology to provide high standards of healthcare such as King Faisal Specialist Hospital (KFSH). Also, some private hospitals have made extensive use of computers and have already obtained reasonable experience. Some public and private hospitals lag behind many other organisations in the use of computer and on-line technology. Some hospitals are working alone to adopt technology without taking advantage of each other' experiences.

Although several researchers in the UK and USA have studied the Information security in the hospital environment as mentioned above. Just a few studies (Al-Zahrani 2001, 2002, and 2003, Al-Rawas and Millmore2002 and Leung2001) are known to have been carried out or related to health care in developing countries in general and Saudi Arabia in particularly. Al-

Zahrani (2001) recommends researchers to examine issues of data security in healthcare and develop suitable security methods to protect health information in developing countries overall and in Saudi Arabia in particular.

Al-Zahrani (2002) investigates the provision of a national computer network system to link Saudi hospitals electronically in order to exchange medical information. Findings show that it is accepted that the time has come to plan and implement a nationwide computer health system for Saudi Arabia. Its also, indicates that a very large proportion of respondents (92%) were aware of confidentiality and security measures when sending medical information. Physicians were very aware of this matter, with (94.7%) responding to the need for confidentiality and security, as were the computer staff (97%). This result was not surprising, as it is these two groups who are the most sensitised to the awareness of these issues.

Furthermore, Al-zahrani (2003) studied the use of ICT in Saudi Arabian hospitals. Finding show that many of the issues and problems associated with ICT reflect the problems elsewhere in the world. Difficulties with information security and patient confidentiality were in the top all health care professionals. We conclude that the Literature on the use of computers and computer security in healthcare in developing countries is relatively scarce, in spite of some of these countries such as Saudi Arabia having implemented computer systems since the 1960s.

This study was carried out recently to investigate several issues relating to hospital information systems security in two university hospitals in Saudi Arabia. It represents an initial attempt to fill the gap in knowledge about hospital information systems in developing countries in general, and about Saudi Arabia specifically.

3. Data Collection Methods

The main goal of this study is to assess the current level of Hospital Information Systems security and issues associated with the adoption of computers in practice in tow university

hospitals in King Saud University. To obtain rich picture four methods were adopted as follow

1. **Questionnaires**: A total of 200 questionnaires were distributed on October, 2004, and collected on various dates in December 2004. One hundred and fifty questionnaires were distributed in King Khalid University Hospitals (KKUH) and a further 50 questionnaires were distributed in King Abdulaziaz university hospital (KAUH). Questionnaire distributed and collected via the head of department to encouraged staffs to complete them in order to raise the response rate. In addition several steps were taken to encourage a satisfactory response rate such as: the front page emphasised the assurance of respondent's confidentiality, the number of questions was limited to fit a four-page layout, and, colour of paper was unusual and attractive. Also, only necessary and relevant questions were asked to avoid redundancy and to maintain reliability

2. **Structured interview**: structured interview was adopted with hospital information system director for more data collection about the current status of ICT services. The interview was started with a brief description of the research conducted and continued with general questions about the organisation and then go to more specific questions about information security issues associated with the use of ICT. The interview questions focused on six elements in order to satisfy the aim and objectives of this research, as follows:

- Current status of current ICT services in the academic environment
- ICT policy, plan and funding
- Problems and obstacles with the use of ICT in the university hospitals
- problems associated with security in the university hospital
- patient confidentiality and security while sending medical information
- Security issues such as sharing password, spy, hocking, misuse or virus.

3. **Document analyses:** Document analysis provides an opportunity to examine documents that will be used extensively. It will be used in the preliminary stages in the investigation of this study. The examination and evaluation of existing documents relate to ICT in the university hospitals and more generally in health service provision in university hospitals over the last five years. From these studies an outline of the current state of healthcare can be gleaned. Documents examined include policy documents, annual plans and, operational guidelines, and reports of various committees. Also, information on the organisation, such as staff hierarchies, organisational charts, job descriptions showing the lines of responsibility and reporting are available and are invaluable as an initial 'map' of the organisation's culture.

4. **Direct observations:** It is essentially a technique for gathering data about the subjects involved in a study. It is an effective way of gathering several kind of descriptive information. It is also effective in situations where the researcher wishes to study specific areas of human behaviour (Saunders *et al.*, 2000). For example, in this study the interaction between medical staff and computers was of interest. Once more, this study use direct observation to enable the researcher to collect direct information about human activities. Observations allowed us to collect data at the time they occur in their natural setting.

4. Data analysis

The data collected from tow University hospitals were coded and processed into a statistical software package (SPSS) .Altogether, 200 questionnaires were distributed in October 2004. Of these71questionnaires were returned giving a response rate of 36%.Descriptive statistics were used to characterise the response to each question in the questionnaire.

Information Security Symposium, Taiban University. College of Computer Science and Engineering 2-4 May, 2006:159-173

4. 1. Demographic data

Within the University Hospitals, the questionnaires were distributed in five departments. participants were asked to specify their departments. The analysis of the responses indicates that the majority come from medical records department (30 =42 %), followed by pharmacy departments (15 =21 %) and computer departments (13 =18 %) and (8=11%) from x ray department as shown in Table 1.

job Descriptions	Departments					Total
	x-ray	Computer	Admission	pharmacy	medical records	
Physicians	-	-	-	2	4	6
Nurse	1	-	1	1	1	4
Paramedical	7	-	-	1	8	16
Pharmacist	-	-	-	11	-	11
Administrator	-	-	4	-	13	17
IT/ Computer staff	-	13	-	-	4	17
Total	8	13	5	15	30	71
Percent%	**11%**	**18%**	**7%**	**21%**	**42%**	

Table1. Respondents by department

The participants were then asked to specify their job description. The results in Table 2 show that most of respondents were computer staffs and administrators each of them were (17 = 24%) followed by paramedical (16 =22 %) and (11=16%) pharmacists. There was (6=8%) physicians and (4=6%) were nurses.

Departments						Total	%
job Descriptions	**X-ray**	**Computer**	**Admission**	**Pharmacy**	**Medical record**		
Physicians	-	-	-	2	4	6	**8%**
Nurse	1	-	1	1	1	4	**6%**
Paramedical	7	-	-	1	8	16	**22%**
Pharmacist	-	-	-	11	-	11	**16%**
Administrator	-	-	4	-	13	17	**24%**
IT/ Computer staff	-	13	-	-	4	17	**24%**
Percent%	8	13	5	15	30	71	**100%**

Table 2. Respondents by job description

Information Security Symposium, Taiban University. College of Computer Science and Engineering 2-4 May, 2006:159-173

Participants were asked about their highest academic qualification. The responses were grouped into five classes. Table 3 shows that slightly less than half of respondents (40 =56 %) possess bachelor degree, followed by less than bachelor degree (11 =16 %) and (10=14%) had obtained a master's degree. Only (3=4%) of respondents had a Ph.D. degree.

qualification	Departments						
	x-ray	Computer	admission	pharmacy	medical record	Total	%
Less than Bachelor degree	2	1	-	-	8	11	**16%**
Bachelor Degree	3	10	5	11	11	40	**56%**
Master's Degree		2		4	4	10	**14%**
PhD		-	-	-	3	3	**4%**
other	3	-	-	-	4	7	**10%**
Total	**8**	**13**	**5**	**15**	**30**	**71**	**100%**

Table3. Respondents by department and qualifications

For the purpose of this study the respondents were grouped according to their age into four classes. They were asked to specify their age group and gender. Most respondents (33 =47%) were aged between 31-40 years old, followed by (18 =25%) aged between 41-50.Result shows that (31=44%) of respondents are male. It was found that (40=56%) are female. Table 4 shows these results .It was expected that female respondents would outnumber their male counterparts as the healthcare sector is one of the most suitable places for female workers in Saudi Arabia due to religious, cultural regulations and might other issues.

Age	Gender		Total	Percent%
	Female	Male		
Less than 30 years	11	4	15	**21%**
31- 40 years	19	14	33	**47%**
41- 50 years	9	9	18	**25%**
51 or over	1	4	5	**7%**
Total	40	31	71	**-**
Percent%	**56%**	**44%**		**100**

Information Security Symposium, Taiban University. College of Computer Science and Engineering 2-4 May, 2006:159-173

Table 4. Respondents by age and gender

4. 2. Usage of computers and computer networks

Respondents were asked to indicate if they use a computer at work. In this way it is hoped to find the extent to which networked computers have penetrated the university hospitals environment. Table 5 shows that all respondents use a computer at work. From the responses it appears that KKUH and KAUH are fully networked.

job Description	computer experience					Total
	Over 15	10 - less than15	5 – less than10	One year to 4	Less than one year	
Physician	1	3	2	-	-	6
Nurse	-	1	2	1	-	4
paramedical	-	5	4	7	-	16
Pharmacist	-	2	5	3	1	11
Administrators	1	8	5	2	1	17
IT/ Computer staff	1	7	7	2	-	17
Total	3	26	25	15	2	71
Percent %	**%4**	**%37**	**%35**	**%21**	**%3**	**% 100**

Table 5. Responses by job description and computer experience

Participants were asked to specify their computer experience in terms of number of years since their first computer use. Responses indicate that just (2=3%) of the sample had less than one years of using computer. Also, (15=21%) have less than 4 years experience of using them. However, (25=35%) have experience from 5 years to 10years.The result in table 6 indicates that employees of the king Saud university hospitals are likely to have the basic skills required for the advanced use of ICT. This means medical staffs in King Saud university hospitals have had rapid growth in experience in use of ICT. Furthermore, it was found that physicians, administrators and ICT staffs are the heaviest users of computers and they have long experience.

Information Security Symposium, Taibah University. College of Computer Science and Engineering 2-4 May, 2006:159-173

job Description	computer experience					
	Over15	10 - less than15	5 - less than10	One year - to 4	Less than one year	Total
Physician	1	3	2	-	-	6
Nurse	-	1	2	1		4
paramedical	-	5	4	7	-	16
Pharmacist	-	2	5	3	1	11
Administrator	1	8	5	2	1	17
IT/ staff	1	7	7	2	-	17
Total	**%3**	**%26**	**%25**	**%15**	**% 2**	**71**

Table 6. Responses by job description and long of computer experience

A variety of software applications were assessed in term of their frequency of use, measured by the following five indicators: daily, weekly, monthly, irregular, and never in terms of daily use. Results indicate that all medical personnel have ready Internet access and make much use of it. It is worth noting that staff in each sites use computer network facilities more often for such activities as e-mail, word processing, data transfer. This survey showed generally lower levels of networking activities in KAUH. Additionally, results indicate that large portion of response use computers daily for maintenance of the patient record. It was not surprisingly, nurses and medical technicians were the main users

4.3. Computer security and patient confidentiality

Respondents were asked about awareness of patient privacy and confidentiality when releasing patient medical information. The intention was to assess awareness of the sample and their knowledge regarding importance of respecting patient information.Table7 indicates that a very large proportion of respondents (67=94%) is aware of consequences releasing patient medical information. There were only (3=4%) not aware of it**.** Physicians were very aware of this matter, with (6 =100%) responding to the need for confidentiality and security,

Information Security Symposium, Taibah University. College of Computer Science and Engineering 2-4 May, 2006:159-173

as were the computer staff (17 = 100%)This result is not surprising, as it is these two groups who are the most sensitised to the awareness of these issues.

Job Description	Are you aware of possible consequences of releasing patient information				
	Yes	No	%	%	Total
Physician	6	0	100	0	6
Nurse	4	0	100	0	4
paramedical personnel	16	0	100	0	16
Pharmacist	10	1	90	10	11
Administrator	15	2	88	22	17
IT/ Computer staff	17	0	100	0	17
Total	**67**	**3**	**-**	**-**	**71**
Percent %	**%94**	**%4**			**%100**

Table.7. Respondents by job desecration and awareness of possible consequences of releasing patient information.

Participants were asked if they consider confidentiality and security when they send medical information to others. The purpose of this question was to assess the knowledge respondents to how much attention they pay to respect patient information. Table 8 indicates that a very large number n of respondents (64 =94 %) take confidentiality and security in their account when they send medical information to others. On the other hand, just only (7 =10 %) they not think about confidentiality and security. Physicians were very considerable of this matter, with 6 (100%). as were the computer staff (17 = 100%). However, 25% of nurses don't take to confidentiality and security in their mind when they send medical information to others This result is expected because medical and computer staff ,are the most sensitised to the possible consequences of exploring medical information .

job Description	Do you take in to consideration confidentiality and security when you send medical				
	%	No	%	Yes	Total
Physician	0	0	100	6	6
Nurse	25	1	75	3	4
paramedical personnel	12	2	88	14	16
Pharmacist	9	1	91	10	11
Administrator	18	3	82	14	17
IT/ Computer staff	0	0	100	17	17
Total	10	7	90	64	71
Percent %		**10%**	**-**	**90%**	**100%**

Table 8. Respondent by job description and consideration confidentiality when they send patient medical information

Its not acceptable for group to share password such abuses could cause serious harm. For the purpose of this study, participants were asked to point if they share their password with their colleagues, measured by the following indicators: Never, rarely, used to but no any more and usually. Aim of this question was to evaluate user's ability to share information and respect medical information. Table 9 shows that (57=80 %) of sample never share password and (7 = 10%) share it rarely. However, (6 = 90 %) usually share it and only(1 = 1%)used to but no any more. 0ver all we can conclude that medical and computer staff don't share password and use technologies ethically.

job Description	Do you share password with your colleagues?				
	Usually	I used to but no any more	Rarely	Never	Total
Physician	1	0	1	4	6
Nurses	0	0	2	2	4
paramedical	3	1	1	11	16
Pharmacist		0		11	11
Administrator	2	0	1	14	17
IT/ Computer staff	0	0	2	15	17
Total	6	1	7	57	71
Percent%	**9%**	**1%**	**10%**	**80%**	**-**

Table 9 respondent by job description and sharing password

Respondents were asked to rank up a list of reasons that computer systems protect against. The purpose of this question was to give an indication of the most impotent reasons that hospital management protect their computer systems against because management need to resolve such issues before further implementation of ICT**.** Result shows the most respondents (33 =46 %) rated misuse from outside threat as the major reason to protect their computers system, followed by misuse from staffs(20=28 %).It was expected misuse from inside will be ranked as the most impotent reasons as indicated in the literature. We can explain this result because of religious and cultural regulations.

Table 10 shows the highest rated reasons to protect system against. It can be concluded that more attention should be paid to train and educate staffs to protect computer against any hazards. So, more training program on computer security is needed. Respondents were asked to add any issues or problems that they felt should be considered. Respondents raised other issues such as, viruses, patient privacy, security problems such as spy, hocking, misuse or virus, patient right and patient consent for the sharing of personal health information and basic ethical principle.

Job Description	**Your computer system protects against**					
	Destroying medical records	**Fraud**	**For patient confidentiality**	**Misuse from outside threat**	**Misuse from staff threat**	**Total**
Physician	-	-	1	4	1	**6**
Nurse	-	1	-	2	1	**4**
Paramedical	1	-	1	9	5	**16**
Pharmacist	3	-	-	6	2	**11**
Administrator	-	4	1	6	6	**17**
IT/ Computer	3	1	2	6	5	**17**
Total	7	6	5	33	20	**71**
Percent%	**%10**	**%8**	**%7**	**%46**	**% 28**	

Table 10. Respondent by job description and reasons to protect computer systems

Information Security Symposium, Taibah University. College of Computer Science and Engineering 2-4 May, 2006:159-173

4.4. Sharing information and information that should be shared among staffs

In fact information is power and assets. People who have information must take responsibility of their resources. Therefore, all staffs in health care originations (Doctors, physicians, nurses etc) need to be taught about the problems and ethical principal involved in sending and sharing patient and medical information. Respondents were asked to identify which information they share with his or her work mate .The largest proportion of respondents ranked information about patient records (45 = 63%), patient care diagnosis (34= 48%), hospital laboratory results(30 =42 %), and hospital news (11 =16 %). Table 11 shows these results in more detail.

Job description	New trends in treating specific diseases	Research information	Patient index	Hospital lab result,	Medical society announcement	Hospital statistics/ Financial	Hospital news	Patient record	Patient care/ Diagnosis	Others
Physician	1	1	3	4	1	1	2	5	3	-
Nurses	-	1	2	2	-	1	-	3	3	-
Paramedical-	-	3	2	9	2	-	2	10	4	-
pharmacist	3	2	5	3	1	-	1	7	8	-
Administrator	-	5	6	3	-	-	2	8	7	-
IT/ Computer	3	7	10	9	3	9	4	12	9	5
Total	7	19	28	30	7	11	11	45	34	5
%	**10**	**27**	**40**	**42**	**10**	**16**	**16**	**63**	**48**	**7**

Table 11. Opinions on the distribution of information and information sharing

5. Study finding and discussions

This study show considerable enthusiasm for the use of computers and advanced technology, with evidence taken from the questionnaire responses, interviews, document analysis and direct observation studies. Hospitals staffs were largely satisfied with the computer services regardless of some problems and issues. Problems were seen to be a lack of training, as well as security issues associated with technical, behavioural ad structural factors. So, Medical

Information Security Symposium, Taiban University. College of Computer Science and Engineering 2-4 May, 2006:159-173

staffs and computer director expressed concerns regarding hardware/software compatibility, and security issues. Several difficulties surrounding the cost security, security recovery and patient privacy and confidentiality and patient consent were mentioned frequently.

The study indicated that maintain privacy, protect scattered and isolated systems are not an easy task because it might lead to significant organisational change and spent more money. Furthermore, integration may perhaps lead to a change in the balance of power among departments within the hospitals. Patients have right to expect that involved staffs will not pass on any personal information which he/she learn in the course of his /her professional duties unless they agree.

Physicians are powerful players in the hospitals, while ICT specialists are conversant in ICT in medicine. This might lead to a potential conflict in who owns the system and controls it. The study indicates that it will be not easy task to estimate network security cost because information is found in many different places and the cost of ICT can change very quickly. University hospital computer director remarked on the shortage of consultants who will deal with ICT issues and computer application in medicine. The reliability of the system and system security and patients privacy were bring up several time during interview.

There are evidences that issues and problems concerning the policy and organisation structure were crucial. Computer director felt that top management was often inadequately informed about ICT policy and developments. Finding from interview and documents indicated that there is a need to develop a high level security policy to guide health professionals and ICT personnel who are involved in the processing and management of sensitive health care information. It should provide a set of mandatory regulations to ensure adequate security of personal health information processed by health information systems. Such policy should be used as a reference for a wide variety of information security and privacy activities, including establishing user access privileges, and investigating security and privacy threats. University management recommend periodically to revisits its ICT policy to see whether it should be modified or augmented. However, such policy should based on a detailed study of the existing framework in the advanced countries, such as USA, UK, European Union and Canada. Accordingly, a possible solution for reaching a reasonable

Information Security Symposium, Taiban University. College of Computer Science and Engineering 2-4 May, 2006:159-173

balance between privacy protection, patient confidentiality and the use of health information for the good of society is needed.

Although several researchers in the UK and USA have studied computer systems threats in the hospital environment. They report the majority of malicious attacks carried out by insiders. In contrast, this study however reports malicious attacks occur by outsiders. It was not expected to discover such result but we believe this is because of religious and cultural regulations. Therefore, further study is needed to examine and analyse the impact of a developing country's cultural, religion, social and political system on the use of ICT.

Literature revealed that most current systems utilise passwords for authentication purposes and in the health care environment, at least, passwords have often been shared or even recorded on or close to the computer terminals. This study indicated clearly passwords are the simplest form of authentication of users of information systems in the university hospitals. Study show that no sharing of passwords, no easily guessed passwords and great portion of staffs don't share their password with others.

Evidences from documents and interview reveal that hospital information systems in King Saud university have not been undergone systematic evaluation. Comparisons between electronic medical records systems and legacy system have not been made .Their hospital computer systems were mainly used for reading patient data, and doctors used the systems for less than half of the tasks for which the systems were functional. We can conclude that the success of the current technology to protect patient information depends heavily on multi damnation factors such as policies, person ethics, organisation regulation and self discipline.

Finally, this study expands the literature base on use of computer to consider security issues and exchange information in health system by focusing on security issues and exchange patients information such as hospital lab test results, patient care, patient record and patient index. It is clear from the literature that this study can be considered as pioneering in area of

hospital information systems security in Saudi Arabia. It sets out to provide an attempt to fill the knowledge gap that exists in hospital information systems in the developing countries.

6. Future studies

Based on the findings found in this study, suggestions could be made for further research. Future studies need to be carried out in order to explore the following areas:

1. To examine issues of data security in healthcare and develop suitable security methods to protect health information in developing countries overall and Saudi Arabia in particular.
2. To examine the impact of using computer information systems on paint confidentiality and the work of medical professionals in the healthcare sector in Saudi Arabia
3. To examine to what extent the Internet is being used by physicians and patients to use e-mail to obtain specific test results.
4. To exam security architecture for interconnecting health information systems in Saudi
5. To exam some of the privacy-protection problems related to classical and genomic medicine, and highlights the relevance of trusted third parties and of privacy-enhancing techniques (PETs) in health care sector in Saudi Arabia

6. Conclusion

ICT in Saudi Arabia is needed for rapid economic development. Saudi commitment to ICT can be traced back to the late 1960s. Saudi Arabian universities hospitals already make extensive use of technology. King Saud University hospitals have invested great amount of money and are moving towards integrated hospital information systems.

This study presents an overview of information security and risks associated with the use of hospital information systems in (KSUH) in Saudi Arabia. This paper reports that the most important dangerous threat come from outside. This result dissimilar with finding in the literature in the developed nation which indicates that threat comes from insiders. All those involved with the introduction and utilizations of hospitals information systems are very keen and concern regarding patient privacy and confidentially issues. This study can be regarded

as pioneering in area of hospital information systems security in Saudi Arabia. Moreover, It s provide an attempt to fill the knowledge gap in hospital information systems in Saudi Arabia.

7. References:

1. **Al-Rawas A.**and **Millmore, S.**2002. Information security risks on a university campus.Science and technology, **(7)**, 31-43

2. **Al-zahrani, S.** 2001, Computer Network System for University Hospitals in Saudi Arabia, PhD thesis, Loughborough University.

3. **Al-zahrani, S.** 2002, Use of Information and communications in healthcare organizations, Perspective from Saudi Arabia. British Journal of Healthcare Computing and Information Management, **19(10),** 17-19.

4. **Al-zahrani, S.** 2003, The attitudes of healthcare personnel towards computers in Saudi Arabian university hospitals. British Journal of Healthcare Computing and Information Management, **20(2):** 38–42.
5. **Amatayakul, M.,** 1999. Security and privacy in the health care information age. MD Computing, **16. (6),** 51-53.

6. **Anderson, J.,** and **M. Brann**, 2000. Security of medical information: the threat from within. MD Computing, **17(2),** 15-17

7. **Anderson, Ross. J., 1996**. Security in clinical information systems. University of Cambridge. Un published paper
8. **Barber,Barr Kees Louwerse**, and **John Davey** ,1998. Implementing Secure Healthcare. NHS Executive's Information Management Centre, Telematics Applications in Europe UN published paper
9. Barber1998

10. **Brennan, P., S. Schneider** and **E. Tornquist,** eds., 1997. Information networks for community health. New York: Springer.

11. **Brennan, S**. and **A. Spours,** 2000. Barriers to the successful and timely implementation of electric prescribing and medicines administration. British Journal of Healthcare Computing and Information Management, **17(8),** 22-25.

12. **Buchan, R.**, 2001. Security measures in open communication systems. (URL: http:// www. medinfo. cam.ac.uk/miu/ papers/misc/ brighton1.htm),[2.2.2001]

13. **Camp, J**. 2000. Computer security when data = life. In: S. Laxminarayan, ed. Proceeding of third ITAB 2000. Piscataway. NJ: IEEE, P 3.

14. **Claerhout B.** and **DeMoor** 2005.Privacy protection for clinical and genomic data International Journal of Medical Informatics .**74 (2-4),**257-265

15. **Couchman, R, Samuel N. Forjuoh, Terry G. Rascoe, Michael D. Reis, Bruce Koehler** and **Kimberly L. van Walsum,** 2005**.** E-mail communications in primary care: what are patients' expectations for specific test results? International Journal of Medical Informatics **(74), (1)**, 21-30

16. **Furnell, Steven,** 1995. Data security in European health care information systems, PhD thesis, University of Plymouth.

17. **Gritzalis ,Dimitris** and **Costas Lambrinoudakis** 2004**. Security architecture for interconnecting health information systems.** International Journal of Medical Informatics. (**73),(3)**305-309

18. **Hojerbak, P.,** 2000. Biometrics-security with convenience. British Journal of Healthcare Computing and Information Management, **17(8),** 46.

19. **Leung G, Johnston J, Wong FK, Cameo** 2001**,** Computerization of clinical practice in Hong Kong**.** International Journal of Medical Informatics.;**62(2):**143-54

20. **Neame, R.,** 1997. Health information privacy and confidentiality. British Journal of Healthcare Computing and Information Management, **14(2),** 31-35.

21. **Saunders, M., P. Lewis** and **A Thornhill,** 2000. Research methods for business students Harlow: Financial Times/Prentice Hall.

22. Sciamanna, Christopher N., Scott P. Novak and **Bess. Marcus** 2005**.** Effects of using a computer in a doctor's office on patient attitudes toward using computerized prompts in routine care. International Journal of Medical Informatics **(74), (5)**, 345-422

23. **Turban,E., R. Kelly Rainer JR** and **Richard E . Potter,** 2001. Introduction to information technology. New York: John Wiley.

24. **Yeoman, R.,** 1998. Connecting to NHS net: the role of code of connection. British Journal of Computing and Information Management, **15(1),** 27-30.