Confidentiality and Privacy of Medical Information

Alia Mohammed AlSulaimi
Department of Information Management, College of Computer and Information Sciences
Al-Imam Mohammad Ibn Saud Islamic University

المستخلص:

تهدف هذه الدراسة لتسليط الضوء على الوضع الحالي للحفاظ على سرية وخصوصية المعلومات الطبية في المستشفيات العامة السعودية مع التركيز على الجوانب التكنولوجية. خصوصية المعلومات الطبية والحفاظ على سرية المريض يعد واحدًا من أهم حقوق المرضى، وأيضًا نظرًا لعدم وجود أبحاث من هذا النوع الذي يركز على الجانب التقني في المملكة العربية السعودية فهذا يزيد من أهمية هذه الدراسة. لدراسة المشكلة، تم مسح ١٧٥ طبيباً وممرضاً وموظفاً إدارياً موظفو الدعم الفني بشكل عشوائي من سبعة مستشفيات عامة في الرياض. أظهرت النتائج أوجه قصور في إنشاء المعلومات الطبية والوصول إليها ومشاركتها، وواقع الوضع فيما يتعلق بالحفاظ على السرية والخصوصية والأساليب التكنولوجية (أرقام المرضى، وكلمات المرور وأمن أجهزة الكمبيوتر، وموظفي تكنولوجيا المعلومات). وواجهت صعوبات مختلفة في تحقيق المستويات التكنولوجية المرغوبة من السرية والخصوصية في جميع المراحل من

الإنشاء إلى التحكم في الوصول. بشكل عام، تدعم نتائج هذا البحث الاتجاهات العامة للنتائج الواردة في الدراسات السابقة، مما يعزز من مصداقية نتائج الدراسة وتماشيها مع المتوقع بناءًا على ما سبق.

Abstract:

The aim of this paper is to investigate upon the current status of maintaining confidentiality and privacy of medical information in Saudi public hospitals with focus on technological aspects. For this, 175 doctors, nurses and management/IT staff randomly selected from seven public hospitals in Riyadh were surveyed. The results showed inadequacies in creation, access and sharing of medical information, and reality of the situation regarding maintenance of confidentiality and privacy and technological methods (patient numbers, passwords and security of computers, IT staff). Various difficulties were encountered in achieving the desired technological levels of confidentiality and privacy at all stages from creation to access control. Overall, the results of this research support the general trends of results reported in previous studies, giving them adequate validity and robustness.

الكلمات المفتاحية:

سرية، خصوصية، معلومات طبية، الرياض، السعودية، تكنولوجيا، مستشفيات.

Keywords:

Confidentiality, Privacy, Medical Information, Riyadh, Saudi Arabia, Technology, Hospitals

Table of Contents

1. Introduction

The background

Ensuring not only quality healthcare but protecting confidentiality and privacy of patient medical information is becoming increasingly important. Victoria State Government, Australia, describes the legal status, access control, and patient rights on sharing information with others (Victoria State, 2015). Issues related to confidentiality, privacy, and security of health information in US healthcare system was discussed by Prater (2014). She discussed various acts and regulations in USA on these aspects. Liang (2002) points out that although laws and regulations provide limited exceptions for access to healthcare data, large scale breaches do occur. The four issues of privacy and confidentiality, security, and data integrity and availability of medical information in hospitals were discussed by Harman, Flite, and Bond (2012).

Thus, need and issues arising in the case of confidentiality and privacy of medical information are being examined at many levels. In the case of Saudi Arabia, Aldajani (2012), in his doctoral thesis, analysed the government policies on security issues of electronic patient records and found that security issues have not been serious consideration in the policies and healthcare staff also are not aware of these issues. In the studies by Alsulaiman and Alrodhan (2014) privacy policies were followed to a greater extent by healthcare sector than others. The authors also examined the laws and regulations relating to privacy and security issues.

But none of these papers discussed the technological issues or the perspectives of maintaining confidentiality and privacy of medical information in hospitals.

Technological issues of maintaining confidentiality and privacy of medical information in hospitals

When new technologies are integrated into the traditional systems, some security and privacy issues might surface. To address these issues, solutions like role-based access, encryption and authentication mechanisms are already being used in many hospitals. However, defining clear attributes to role based access, new policies for wider geographic areas of the country, patient privacy issues when monitoring health at home and rules authorising people for data mining and analysis, anonymising the collected data and technical methods to ensure compliance with these rules are required to be put in place when patient records are electronically stored and accessed in hospitals (Meingast, Roosta, & Sastry, 2006).

According to the survey results of Van Allen and Roberts (2011) the integration of certain technology advances like e-mail, electronic health records, and social-networking websites might have compromised patient privacy or confidentiality. The concerns of unauthorised access to EHRs, inappropriate distribution of patient information through technologies and concerns of patients with the use of social networks, were expressed by the survey participants.

The challenges to privacy and security of patients, when cloud computing is used for e-health (e-Health Cloud) were discussed and a few solutions were offered by AbuKhousa, Mohamed, and Al-Jaroodi (2012). The technical challenges include continuous data and service availability, adequate reliability of the services provided, data management, scalability with the rapid growth of data, flexibility to serve multiple customers of different requirements simultaneously, inter-operability between various agencies of services and providers, security and privacy as cloud has many vulnerabilities on these two issues and easy maintainability. The specific security and privacy challenges were access control, authentication, integrity, non-denial of having sent a particular data and audit. Collaborations among patients, service providers and cloud owners have been suggested as solutions to security and privacy problems.

Most of the technological issues related to security and confidentiality of patient data and some possible solutions have been covered in the three papers reviewed above. However, studies focusing on Saudi healthcare context had been rare.

The purpose of this current study was to fill this research gap, applied to the specific context of Saudi Arabia. Based on this, the following aim and research questions were framed for this research.

Aim of this research

The aim of this research was to investigate on the current status of maintaining confidentiality and privacy of medical information in Saudi public hospitals focused on technological aspects related to this issue.

The Research Questions-

1. What is the reality of maintaining the confidentiality and privacy of medical information?
2. What are the technological methods to maintain the confidentiality and privacy of medical information?
3. What are the difficulties in achieving confidentiality and privacy of medical information?
4. Are there any relationship between the responses and demographic variables and any significant differences among the responses?
5. What are the recommendations for enhancing the confidentiality and privacy of medical information?

The importance of this study

The security and privacy of patient data is the right of the patient. If these two aspects are ignored, chances of misusing patient data will be higher. If the patient is sensitive about his health problems, bringing it into public attention and debate with the patient name, it may affect the patient psychologically. Using patient data without consent, when he/she is not in a condition to respond to questions, is a breach of privilege and compromises many personal and regulatory aspects. Thus, protection of the privacy and confidentiality of any patient with adequate security from free access and manipulation is of great importance.

As was shown above and further in the Review of Literature section, technologically focused studies have been rarely reported from Saudi Arabia. This point also justifies the importance of doing this research and locating it in Saudi Arabia.

In the case of Saudi Arabia, as in the case of many other countries, there are both public and private healthcare providers where a number of doctors, nurses, and management/IT staff work. In the Saudi context, the current status of patient data's privacy and confidentiality from a technological perspective is not known. This study aims to fill this gap. This point also justifies the importance of doing this research in the Saudi context.

The above three points amply demonstrate the importance of this research.

Organisation of this paper

The rest of this paper is organised in the following manner. The next section (2) reviews the related literature briefly. In section 3, the methodology followed for collection and analysis of data to answer the research questions are described. Section 4 describes the findings obtained from the data collected and analysed. In Chapter 5, the results obtained are explained, interpreted and the research questions are answered. This is followed by conclusions from this research, recommendations and some limitations of this research.

2. Literature Review

After setting the background for this research and defining the aim and the research questions in the previous section, a detailed review of recent researches done on maintaining confidentiality and privacy of medical information is attempted here.

2.1 Method Review

The appropriate research works were identified by searching academic databases using suitable search terms. The search was restricted to papers published from 2010, as technologies for electronic filing and storing of information in healthcare developed rapidly since 2010.

Respect for patient privacy and satisfaction are two important components of quality care. The extent of privacy observed and its relationship with patient satisfaction by survey of patients admitted to emergency department in a Teheran university hospital were studied by Nayeri and Aghajani (2010). For about half of the patients, the extent of respect for privacy was weak or average. Level of privacy was significantly associated with level of patient satisfaction.

One way in which confidentiality and privacy of patient information may be compromised is increasing use of social media by medical professionals. Mansfield, et al. (2011) suggested that such possibilities could be prevented by including this item in the standards and codes of ethics in Australia and New Zealand.

The recent trend of amalgamation of WBAN-based healthcare systems to cloud-based healthcare systems can compromise privacy of patients' data. The need for proactive steps for access identification and effective mitigation mechanisms was stressed by Sajid and Abbas (2016) in their review. Most technologies used for protecting privacy did not fully satisfy the privacy requirements.

For public health practices, population-based data are being evaluated at various levels. However, restrictions placed on access to these due to confidentiality and privacy concerns prevent researchers from using the large amounts of such data. Wartenberg and Thompson (2010) suggested necessary changes in these restrictions to enable both use of the data for research and protection of confidentiality and privacy to a satisfactory level.

The need for better security of medical information arises due to the adoption of digital technology for patient records, increased regulations, consolidation of healthcare providers and the increasing requirement of information exchange between patients, providers and payers. Appari and Johnson (2010) evaluated the research works done in these aspects. The authors provided a diagram of information flow in healthcare system, reproduced in Fig 2.1.

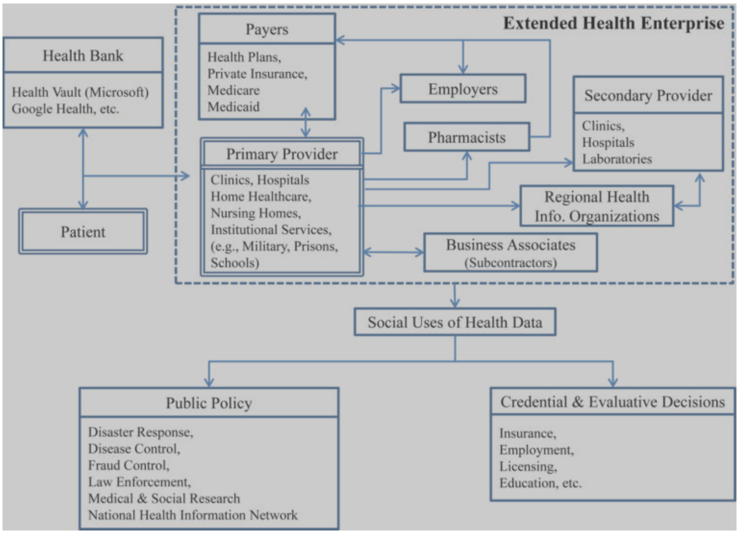

Figure 2.1. Information flow in healthcare systems (Appari & Johnson, 2010)

Many types of information security breaches were also discussed in their paper. There are organisational threats arising from inappropriate access of patient data by internal agents abusing their privileges. External threat from outside agents exploit vulnerability of the information systems. Systemic threat arises from an agent in the information chain or outsiders using the information other than for intended ones, mostly for illegal purposes. Professional hackers may be hired to hack the data. Accidental or unintentional disclosure of information by health professionals can occur to others like posting messages in communication sites. Insider curiosity leads to healthcare professionals using their accessibility to pry upon records of patients for exploitation or for spreading rumours in the media. Insiders may also breach the data for selling them outside. Hackers and other outsiders may intrude into the network of the hospital to access data. Threats from insiders are more serious.

Using a before-after survey, Perera, Holbrook, Thabane, Foster, and Willison (2011) showed support from either patients or from physicians for sharing of information on them among health professionals to provide clinical care. There was little support for sharing of de-identified patient information among health professionals. None agreed that computerised records are more controlled than paper records. Most agreed that benefits outweighed risks of computerisation.

According to Harman, Flite, and Bond (2012) the best way to ensure confidentiality is to limit access for authorised individuals only. They can also ensure that others do not have access and report any breach to the management immediately. Biometric identifier along with passwords gives double layer protection. Access to different types of information should be according the role of the staff in the hospital. Accountability of superiors on the actions of their staff is a part of these controls. Warning about legal and regulatory actions on security breaches should be given. Identifying security breaches from messages among healthcare professionals is difficult. There should be a separate information security department to look after the security levels of the hospital and revise them as and when required. Integrity of data is also as important as confidentiality, privacy and security. Some categories of information breaches were discussed in this paper also.

Multiple levels of controls at physical, technical and administrative levels ensure that researchers can access linked administrative patient data from Canadian Population Data BC (Pop data) without compromising confidentiality, privacy or security. Pencarrick Hertzman, Meagher, and McGrail (2012) described in detail how these controls work to ensure that there is no breach of any kind while researchers access the data.

The stigma associated with HIV make patients to shy away from sharing information even with medical professionals. Implementation of Health Information Exchanges (HIEs) in USA has led to widespread acceptability of HIV information sharing. Increasing trust with technologies protecting their privacy may be the reason for this observation in the survey results of Maiorana, et al. (2012).

Concern about data breach, when protected health information was exchanged between healthcare providers, were expressed by a majority of patients in the survey conducted by Agaku, Adisa, Ayo-Yusuf, and Connolly (2013) and by Wilkowska and Ziefle (2012). Sometimes, patients withheld some information fearing security loss. Females and healthy adults wanted the highest levels of security and privacy standards compared with males and the ailing elderly.

The need to consider privacy and security issues before moving patient records to third party cloud services, was stressed by Rodrigues, De La Torre, Fernández, and López-Coronado (2013). The authors suggested role-based access, network security mechanisms, data encryption, digital signatures, access monitoring and compliance with various certifications and third-party requirements, such as SAS70 Type II, PCI DSS Level 1, ISO 27001, and the national data security regulations.

US Federal response to security of health records is better than conflicting state laws. However, compared to US, the privacy laws of EU give more choices to patients in electronically recording their medical information for treatment and more control over sharing the information. EU is better with respect to the combined protection given to the privacy of the patients through technological and legal methods. These observations were made by Hiller, McMullen, Chumney, and Baumer (2011) using the five Fair Information Practices (FIP) principles used by Federal Trade Commission of USA.

Protection of privacy in 20 mobile health applications (mHealth) was evaluated by Adhikari, Richards, and Scott (2014). Only one application allowed users to delete personal information completely. Personal details were required in 13 applications, but only two of them required password log in. Half of the applications stored their data in cloud. Most of them had a privacy policy, but only a few of them said about data privacy and security.

The survey results obtained by Househ, Grainger, Petersen, Bamidis, and Merolli (2018) revealed that balancing between patient needs of health information and privacy concerns was influenced by the extent of cross-cultural understanding, awareness of clinicians and patients, de-identification of data and commercialization of patient data. Patient empowerment, connecting participatory health enabling technologies with clinical records, open data sharing agreement and e-consent were some opportunities identified to achieve the desired balance.

Patients in Turkey were unsure of protection of their privacy and confidentiality in the electronic health record systems due to low level of awareness. They trusted their doctors, health researchers in universities, pharmacist, nurses and other hospital staff for protection of their privacy. But they did not trust insurance companies, government, private sector health researchers, information technology specialists and government health researchers. These results were obtained in a master thesis by ÖZKAN (2011).

Awareness of privacy and confidentiality were low to moderate among most Iranian patients surveyed by Mohammadi, et al. (2018). Over 75% of patients could define privacy correctly and knew about privacy violations. Most of them also knew about confidentiality of physicians, examination results and medical consultations. In Saudi hospitals, most patients were not aware of their rights including privacy and confidentiality (Almoajel, 2012).

2.2 Summary

The foregoing review focused on patient perceptions of confidentiality and privacy in their healthcare contexts and problems associated with use of some technologies in ensuring confidentiality, privacy and security. Very little work has been done specifically on these aspects in Saudi contexts. This necessitates some urgent research works on this topic and therefore justifies the current research.

3. Methodology

The aim of this study and the research questions have already been given in the Introduction chapter. The methods used for collection and analysis of data required for answering the research questions are described in this chapter.

3.1 Research design

Many standard textbooks describe the methods of conducting research works of different types. Some of these are: Creswell and Creswell (2017), Saunders, Lewis, and Thornhill (2009) and Sekaran and Bougie (2016). The description of the methodology of this research is based on the principles outlined in these books.

In this research primary data were collected using the quantitative questionnaire survey. This method was selected due to the need for precise information and for identifying causal relationships between promising variables.

3.2 Population and Sample Sizes

According to the statistics (Ministry of Health, 2018) as on 2018, there were 274 public (MOH), in Saudi Arabia. Seven hospitals from Riyadh were chosen for selecting survey participants for convenience.

Survey participants were doctors, nurses and management/IT department of the seven hospitals. According to Ministry of Health (2017) in 2016, there were 42768 physicians and 101256 nurses in the public hospitals. There were 57474 allied healthcare personnel in public hospitals, which may include the IT staff. With the availability of such large number of healthcare personnel in Saudi public hospitals, obtaining adequate sample size even with only seven hospitals, should not have been difficult.

From each of the seven hospital, samples of doctors/nurses/management or IT staff were separately choses for the survey, using simple random sampling method. No inclusion or exclusion criteria was used. The participants were selected only if they gave written consent.

The final sample count, based on the above method of sampling, was 61 Nurses, 79 management/ IT staff and 35 doctors, totalling 175. But the total number of 175 participants did not support this expectation. According to Calculator.Net (2021), the minimum sample size for the total population of 201298 in the seven hospitals, is 384. This was one limitation of this study.

3.3 Survey Questionnaire

A draft survey questionnaire was prepared based on literature review and opinion of experts and it was pilot tested with 10 potential participants. The feedbacks from the pilot participants were used for finalisation of the questionnaire to administer to the participants. A sample of the final survey questionnaire is appended.

The questionnaire was structured in the following manner.

No	Scale	No of items
A	Demographic	6
B	Storage of patient information	1
C	Creation, access and sharing of patient information	14
D	Research Question 1: What is the reality of maintaining the	5

No	Scale	No of items
	confidentiality and privacy of medical information?	
E	Research Question 2: What are the technological methods to maintain the confidentiality and privacy of medical information?	4
F	Research Question 3: What are the difficulties in achieving confidentiality and privacy of medical information?	8
G	Research Question 4: Are there any relationship between the responses and demographic variables and any significant differences among the responses?	By data analysis
H	Research Question 5: What are the recommendations for enhancing the confidentiality and privacy of medical information?	Derived from findings

There were two open questions. But only a few participants responded with very brief comments. So, these did not represent a major source of recommendations in the final version appended; most of the recommendations are derived from findings.

The survey was done by direct contact of the participants in the hospital.

3.4 Data Analysis Methodology

3.4.1 Aims of Data Analysis

The aims of this data analysis are:

1. To provide a demographic profile of the sample.
2. To establish if the four scales used in the survey (i.e., Creation, access and sharing of patient information; reality of maintaining the confidentiality and privacy of medical information; technological methods to maintain the confidentiality and privacy of medical information; and difficulties in achieving confidentiality and privacy of medical information) are internally consistent and reliable.
3. To summarise the participant responses relating to the four scales and examine internal consistency and reliability.

4. To test whether there are any significant associations between any pairs of the four scales and their internal consistency and reliability.
5. To test differences between the responses of the nurses, management/IT and doctors for significance with regards to the four scales and their internal consistency and reliability.

3.4.2 Data Analysis

Quantitative analysis was conducted using SPSS statistical software version 24.

The frequency counts were tabulated for all questions with a categorical response. The trends were summarized, based upon whether the majority of the responses were located. Summary statistics (minimum, maximum, means and Standard Deviations (SD) have been reported for continuous variables.

To ensure consistency of scales, reliability tests were done on the scale items using Cronbach Alpha as a measure. A value of approx. 0.7 or above alpha value was considered reliable (Reynaldo & Santos, 1999).

Variable scores were created from the scales used in the survey as the average of the scores associated with the items belonging to the respective scale. The conceptual and operational definitions of the score are provided below.

Table 1: Conceptual and operational definitions of four scores

Variable	Conceptual Definition	Operational Definition		
		Number of Items	Computation	Interpretation of Scores
Creation, access and sharing of patient information score	The status of the creation, access and sharing of patient information	14	Average of the responses to 14 items	1=Low levels 5=High levels
Reality of maintaining the confidentiali	The reality of maintaining the	5	Average of the responses to 5 items	1=Low levels 5=High levels

Variable	Conceptual Definition	Operational Definition		
		Number of Items	Computation	Interpretation of Scores
ty and privacy of medical information score	confidentiality and privacy of medical information			
Technological methods to maintain the confidentiality and privacy of medical information score	The use of technological methods to maintain the confidentiality and privacy of medical information	4	Average of the responses to 4 items	1=Low levels 5=High levels
Difficulties in achieving confidentiality and privacy of medical information score	The difficulties in achieving confidentiality and privacy of medical information	8	Average of the responses to 8 items	1=Low levels 5=High levels

The multivariate analysis technique used for testing the hypotheses in this research included Pearson's correlation analysis and one way ANOVA. Correlation analysis is a suitable technique to test for significant associations between pairs of continuous variables (Katz, 2011; Tabachnick & Fidell, 2007). ANOVA is a suitable test to compare the mean scores of two or more samples (Katz, 2011; Tabachnick & Fidell, 2007).

A .05 level of significance was used as the criteria for statistical significance for all multivariate analysis. The results obtained from the analyses of data are described in the Results chapter.

3.5 Summary

The methods used for collecting and analysing the data required to answer the research questions were described in this chapter. Primary data was collected using a quantitative questionnaire survey. The scales and items included demographic information, method of storage of medical information in the hospitals of the participants, creation, access and sharing of medical information, real situation in maintaining confidentiality and privacy, technological methods used for the purpose, difficulties in achieving this purpose and two open questions on their recommendations to the hospital and to the government on maintaining confidentiality and privacy of medical information. The data were converted to variable scores, frequencies of responses, descriptive statistics, reliability analysis, correlations and ANOVA were done in line with the research questions.

4. Results

The results obtained by collecting and analyzing the data as described in the previous (Methodology) chapter are described under different sections in this chapter.

4.1 Sample profile

The final sample consisted of 175 people. A profile of the sample is summarised in Table 4. 1. A majority of the participants were males (n=122, 69.7%). The two largest groups of people by age were people less than 35 years (n=78, 44.6%) and people between 35-50 years (n=71, 40.6%). A vast majority of the people surveyed had attained a maximum of a Bachelor's degree or less (n=140, 80%). A vast majority of the people had more than 10 years of work experience (n=114, 65.1%). There was no clear trend with regards to the experience people had with medical information systems. Between a quarter and thirds of people had less than 5 years, between 5-10 years and more than 10 years of experience with medical information systems. The two largest groups of participants with regards to their position were Management/IT (n=79, 45.1%) and nurses (n=61, 34.9%). Doctors (n=35, 20%) represented the smallest group. A majority of the participants indicated that the patient information is stored both electronically and in paper (n=106, 60%).

Table 4.1: Sample profile

		Frequency	Percent
Gender	Male	122	69.7
	Female	53	30.3
	Total	175	100

Age	Less than 35 years	78	44.6
	35-50 years	71	40.6
	More than 50 years	26	14.9
	Total	175	100
Education	Bachelor's or less	140	80.0
	Master's	17	9.7
	Doctorate or more	18	10.3
	Total	175	100
Experience	Less than 5 years	17	9.7
	5-10 years	44	25.1
	More than 10 years	114	65.1
	Total	175	100
Experience with Medical Information Systems	Less than 5 years	69	39.4
	5-10 years	45	25.7
	More than 10 years	61	34.9
	Total	175	100
Position	Nursing	61	34.9
	Management/IT	79	45.1
	Doctor	35	20.0
	Total	175	100

Patient Information Storage Medium	Paper	33	18.9
	Electronically	36	20.6
	Both	106	60.6
	Total	175	100

The most important trend from these results is that a significant percentage of all surveyed participants had experience with medical information system. The other significant point is that most Saudi hospitals are storing patient information both electronically and in paper.

4.2 Reliability analysis

The Cronbach's alpha values for the four scales are shown in Table 4.2. Since all these Cronbach's alphas are close to or greater than 0.7 alpha value, the items from the scales were deemed fit (reliable) to be used in subsequent the analysis.

Table 4.2: Reliability analysis

Scale	Number of Items (N)	Cronbach's Alpha
Creation, access and sharing of patient information score	14	.633
Reality of maintaining the confidentiality and privacy of medical information score	5	.863
Technological methods to maintain the confidentiality and privacy of medical information score	4	.680
Difficulties in achieving confidentiality and privacy of medical information score	4	.864

4.3 Multivariate analysis

The mean scores for the four scale scores are shown in Table 4.3. Since the means for all the scores are more than the midpoint of the Likert scale (i.e., 3), it would be safe to say that patient confidentiality is reasonably protected. However, there are also above average levels of difficulties in ensuring that patient confidentiality is reasonably protected.

Table 4.3: Summary statistics - scale scores

	Min.	Max.	Mean	SD
Creation, access and sharing of patient information score	2.64	3.93	3.25	0.35
Reality of maintaining the confidentiality and privacy of medical information score	1.00	4.80	3.50	0.91
Technological methods to maintain the confidentiality and privacy of medical information score	2.00	4.75	3.60	0.86
Difficulties in achieving confidentiality and privacy of medical information score	1.25	4.38	3.35	0.95

The Pearson's correlations between the four scores are shown in Table 4.4. The results indicate that there are significant inter-correlations between the four scores.

Table 4.4: Pearson's correlations

	1	2	3	4
Creation, access and sharing of patient information score (1)	1			
Reality of maintaining the confidentiality and privacy of medical information score (2)	.253**	1		
Technological methods to maintain the confidentiality and privacy of medical information score (3)	.265**	.661**	1	
Difficulties in achieving confidentiality and privacy of medical information score (4)	.246**	.239**	.410**	1

**. Correlation is significant at the 0.01 level (2-tailed).

Technological methods have the highest correlation with reality of maintaining confidentiality and privacy. Thus, if technological methods are used, there is higher likelihood of maintaining confidentiality and privacy of medical information. As a reasonable level of maintenance of confidentiality and privacy has been ensured, it may be safely assumed that reasonable level of technology is being used.

4.3.1 ANOVA

Four one-way ANOVA were conducted to establish if there are significant differences between the mean scores for nurses, management/IT, and doctors. The mean scores are shown in Table 4.5. The ANOVA found that there are significant differences between the creation, access and sharing of patient information score by the position of the respondent (F(2, 172)=28.750, p<.001)); the reality of maintaining the confidentiality and privacy of medical information score by the position of the respondent (F(2, 172)=11.559, p<.001)); and the mean technological methods to maintain the confidentiality and privacy of medical information score by the position of the respondent (F(2, 172)=26.594, p<.001)). However, no significant difference was found between the mean difficulties in achieving confidentiality and privacy of medical information score by position of the respondent (F (2, 172) =2.797, p=.064)).

A Tukey HSD post-hoc test was conducted to see which means differ significantly. The results are shown in Table 6. The results indicate that for creation, access and sharing of patient information score, the means significantly differ for the pairs nurses and management/IT; and doctors and management/IT. For the reality of maintaining the confidentiality and privacy of medical information score, the means significantly differ for the pairs nurses and management/IT; and nurses and doctors. For the technological methods to maintain the confidentiality and privacy of medical information score, the means significantly differ for the pairs of nurses and management/IT; and nurses and doctors.

Table 4.5: Mean scores by position

		N	Mean	SD
Creation, access and sharing of patient information score	Nursing	61	3.44	0.20
	Management/IT	79	3.06	0.28
	Doctor	35	3.36	0.47
	Total	175	3.25	0.35

		N	Mean	SD
Reality of maintaining the confidentiality and privacy of medical information score	Nursing	61	3.09	0.62
	Management/IT	79	3.65	1.10
	Doctor	35	3.88	0.54
	Total	175	3.50	0.91
Technological methods to maintain the confidentiality and privacy of medical information score	Nursing	61	3.06	0.94
	Management/IT	79	3.80	0.62
	Doctor	35	4.11	0.66
	Total	175	3.60	0.86
Difficulties in achieving confidentiality and privacy of medical information score	Nursing	61	3.22	0.83
	Management/IT	79	3.30	1.14
	Doctor	35	3.68	0.50
	Total	175	3.35	0.95

Table 4.6: Post-hoc test results

Dependent Variable			Mean Difference (I-J)	Std. Error	Sig.
Creation, access and sharing of patient information score	Nursing	Management/IT	.37646*	.05213	<.001
		Doctor	.07876	.06485	.446
	Management/IT	Nursing	-.37646*	.05213	<.001
		Doctor	-.29770*	.06210	<.001
	Doctor	Nursing	-.07876	.06485	.446
		Management/IT	.29770*	.06210	<.001
Reality of maintaining the confidentiality and privacy of medical information score	Nursing	Management/IT	-.56136*	.14646	.001
		Doctor	-.78820*	.18221	<.001
	Management/IT	Nursing	.56136*	.14646	.001
		Doctor	-.22684	.17448	.397
	Doctor	Nursing	.78820*	.18221	<.001
		Management/IT	.22684	.17448	.397
Technological methods to maintain the	Nursing	Management/IT	-.74642*	.12852	<.001
		Doctor	-1.04977*	.15989	<.001

Dependent Variable			Mean Difference (I-J)	Std. Error	Sig.
confidentiality and privacy of medical information score	Management/IT	Nursing	.74642*	.12852	<.001
		Doctor	-.30335	.15311	.120
	Doctor	Nursing	1.04977*	.15989	<.001
		Management/IT	.30335	.15311	.120
Difficulties in achieving confidentiality and privacy of medical information score	Nursing	Management/IT	-.07979	.16022	.872
		Doctor	-.45574	.19933	.060
	Management/IT	Nursing	.07979	.16022	.872
		Doctor	-.37595	.19087	.123
	Doctor	Nursing	.45574	.19933	.060
		Management/IT	.37595	.19087	.123

*. The mean difference is significant at the 0.05 level.

These results indicate the relative roles of different categories of hospital staff in the four functionalities related to maintenance of confidentiality and privacy of medical information at various levels. Evidently, nurses and doctors are the creators of patient records and Management/IT are concerned with their secure storage and access mechanisms to ensure privacy and confidentiality.

4.4 Summary

The survey results showed that most of the Saudi hospitals store medical information both electronically and in paper. Most of the staff interviewed, had experience in medical information systems irrespective of their service experience. A reasonable level of technology is used in Saudi hospitals to ensure confidentiality and privacy of patient information. Relationships between the scales closely followed the roles of the survey participants in their hospitals. Nurses and doctors are creators of medical records and management/IT look after confidentiality and privacy through storage and access decisions.

5. Discussions and Conclusions

5.1 Discussions

The overall findings can be summarised as follows-

As most Saudi hospitals used both paper and electronic records, there was a clear role differentiation of hospital employees. Doctors and nurses were creators of medical information. Management/IT department looked after confidentiality and privacy concerns. There were inadequacies of technology use in collecting, storing and accessing medical information at various levels. This is clear from the mean response of 3.25 obtained, short of agreement and nearer to disagreement. This response may represent a hesitation on the part of respondents to determine what should be their response to items related to items under creation, access and storage of medical information. If these were done perfectly, there no room for doubting the maintenance of confidentiality and privacy of medical information. In the absence of a perfect system, there is always chances of inadequacies in maintaining confidentiality and privacy of medical information, which the items on the three research questions can answer.

1. What is the reality of maintaining the confidentiality and privacy of medical information?

There were five items related to this research question. As presented in Table 4.3, the minimum value was 1.00, the maximum was 4 and mean was 3.5 on a scale of 1- Don't know, 2-strongly disagree, 3-disagree, 4- agree, 5- strongly agree. The respondents' most positive response (maximum score of 4.8) was nearer to strongly agree. There were a few "who did not know" who gave the lowest mean response of 1.0. The mean of 3.5 indicates a position between disagree and agree. If it was not a waited average, half the participants would have agreed to the statement and the other half disagreed. This shows absence of clear idea on whether confidentiality and privacy of medical information were truly maintained well.

Answer to this research question- there is inadequate knowledge about whether confidentiality and privacy were maintained by the hospitals.

2. What are the technological methods to maintain the confidentiality and privacy of medical information?

There were four items related to this question. The lowest response of 2.00 indicates strong disagreement. The maximum and minimum were close to the values for the first research question. Thus the only difference, in this case, was a few respondents strongly disagreed with all the suggestions of technological methods to maintain confidentiality or privacy.

Answer to this research question- Patient number and password protection are good, but they do not assure that no security breach happens.

3. What are the difficulties in achieving confidentiality and privacy of medical information?

There were eight items for this research question. The questions progressed from micro-level, in-hospital measures to macro-level adequacy of government policies and strategies. The minimum, maximum and mean response values were 1.25, 4.38 and 3.35. There was a weaker "don't know", but a stronger "strongly disagree" response. The maximum and mean value were lower than those for the first two aspects, but within the ranges of strongly agree and less than agreement ranges. The lower values may indicate lower strength of these responses. Possibly, quite a few did respond more negatively than the mean scores indicated.

Answer to this research question- There were difficulties in achieving confidentiality and privacy of medical information at all stages of creation, storage and access, whether paper, electronic or both, which could be partly due to the policies of the hospital and/or government.

4. Are there any relationship between the responses and demographic variables and any significant differences among the responses?

This is an implied question to get the complete picture about the current status in maintaining confidentiality and privacy of medical information. Pearson's correlations were highly significant and positive between all pairs of response scales. The strongest correlation coefficient of 0.661 was obtained for the relationship of Technological methods to maintain the confidentiality and privacy of medical information score with Reality of maintaining the confidentiality and privacy of medical information score. This means, actual position regarding the maintenance of confidentiality and privacy of medical information depended upon the nature and extent of technologies used. Technology use was less than satisfactory. Therefore, better use of proper technologies should improve maintenance of confidentiality and privacy of medical information to the required level.

A further support comes for this contention from the next strong relationship (r=0.410) between Difficulties in achieving confidentiality and privacy of medical information score and Technological methods to maintain the confidentiality and privacy of medical information score. As difficulties increase, better technologies need to be used to achieve the best possible confidentiality and privacy of medical information.

ANOVA tests had shown significant differences between doctors, nurses and IT staff for the first three scales. The difficulties in maintaining confidentiality and privacy were similar for all positions. This is possible if the technological limitations affect all positions similarly in keeping the information confidential. Further probing showed that creation, access and sharing of information were similar for nurses and doctors. Doctors and nurses are the primary level f data creation and they have more or less equal access and share the data for care requirements of patients. IT staff are not involved in creation of medical information. They are involved only to store and control access and use the data for various administrative purposes. In the case of the real position regarding maintenance of confidentiality and privacy of data, the involvement of nurses and differed significantly from doctors and management/IT. Once created, they have very little role in determining who else are accessing and sharing information. Between doctors and management/IT also similar differences, interpretable similarly, existed. Doctors are involved in using the technology given to them. Thus, these two have similar involvement in technology use. Nurses are not part of it and their involvement is at user interface only. Therefore, the differences between nurses and doctors and between nurses and management/IT are significant. Thus, once the data reaches the management/IT, nurses and doctors are not involved in determining who else access and share them. Indirectly, it may mean, the inability to maintain confidentiality and privacy of medical information may arise from errors at the management/IT stage. Management/IT determine the technology to be used for recording, storing and accessing information.

Answer to this research question- There were highly significant relationships of technology used with reality of maintenance of confidentiality and with difficulties of maintaining confidentiality. Some differences among nurses and doctors and management/IT were noted.

5.1.1 General discussions about the findings

The responses were obtained from doctors, nurses and IT staff. Generally, the patients are suspicious of maintenance of confidentiality and privacy of their data according to (Nayeri & Aghajani, 2010) and (Agaku, Adisa, Ayo-Yusuf, & Connolly, 2013). Patients withhold information due to this suspicion (Maiorana, et al., 2012), (Agaku, Adisa, Ayo-Yusuf, & Connolly, 2013) or low awareness (Mohammadi, et al., 2018); (Almoajel, 2012); but cooperate with the doctors when assured of confidentiality (Wilkowska & Ziefle, 2012). In the survey of (Perera, Holbrook, Thabane, Foster, & Willison, 2011), patients did not find any difference between electronic or paper records in the level of confidentiality and privacy offered.

Many types of security breaches can occur and as was noted by (Appari & Johnson, 2010) both from internal and external agents. Inadequacies of current use of technologicies and methods to address them were discussed by (Sajid & Abbas, 2016), (Appari & Johnson, 2010), (Rodrigues, De La Torre, Fernández, & López-Coronado, 2013) and (Adhikari, Richards, & Scott, 2014),

The need for standards and codes (Mansfield, et al., 2011), effectiveness of policies and regulations (Appari & Johnson, 2010) and standards and guidelines (Hiller, McMullen, Chumney, & Baumer, 2011), (Rodrigues, De La Torre, Fernández, & López-Coronado, 2013) and levels of controls on access (Wartenberg & Thompson, 2010), (Harman, Flite, & Bond, 2012), (Pencarrick Hertzman, Meagher, & McGrail, 2012) have also been studied.

5.2 Conclusions

Thus, more problems in maintenance of confidentiality and privacy of medical information occur due to technological and access control issues. This research also obtained the same results. This research further validates previous studies already done as it shows the same trends present in the sample group studied.

5.3 Recommendations

a) The Saudi government must review its policies and regulations, focusing more on the technological aspects of maintaining confidentiality and privacy of medical information in their hospitals.

b) The current technological status of maintenance of confidentiality and privacy need to be investigated by an expert committee in all hospitals and solutions need to be suggested by the committee.

c) Research to evaluate most modern technologies like cloud storage and block technology needs to be intensified to identify the best possible technology to prevent any type of security breach at any level.

d) Hospitals need to review their current methods of storage and access of electronic health records against incidences of security breaches and make suitable modifications in their technologies as required.

5.4 Limitations of this study

Only seven hospitals were sampled. The sample size of 175 was much smaller than the ideally required 384 minimum sample size. The study did not include patients’ views. The data collection was limited to brief examination of maintenance of confidentiality and privacy and possible factors only. No suitable survey framework was available and hence own framework was used, thus limiting the scope for comparisons.

References:

- AbuKhousa, E., Mohamed, N., & Al-Jaroodi, J. (2012). e-Health cloud: opportunities and challenges. Future internet, 4(3), 621-645.
- Adhikari, R., Richards, D., & Scott, K. (2014). Security and privacy issues related to the use of mobile health apps. 25th Australasian Conference on Information Systems, 8-10 December 2014, Auckland, New Zealand, ACIS2014 (pp. 1-11). ACIS.
- Agaku, I. T., Adisa, A. O., Ayo-Yusuf, O. A., & Connolly, G. N. (2013). Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. Journal of the American Medical Informatics Association, 21(2), 374-378.
- Aldajani, M. (2012). Electronic Patient Record Security. Faculty of Technology. Software Technology Research Laboratory.
- Almoajel, A. M. (2012). Hospitalized patients' awareness of their rights in Saudi governmental hospital. Middle-East Journal of Scientific Research, 11(3), 329-335.
- Alsulaiman, L. A., & Alrodhan, W. A. (2014). Information Privacy Status in Saudi Arabia. Computer and Information Science, 7(3), 102-124.
- Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. International journal of Internet and enterprise management, 6(4), 279-314.
- Calculator.Net. (2021). Sample Size Calculator. Retrieved August 26, 2021, from Calculator Net: https://www.calculator.net/sample-size-calculator.html?type=1&cl=95&ci=5&pp=50&ps=16814&x=6&y=17
- Creswell, J. W., & C. J. (2017). Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.). Sage Publications.
- Hair, J. J., Anderson, R. E., Babin, B. J., Tatman, R. L., & Black, W. C. (2010). Multivariate data analysis (7th ed.). New Jersey: Prentice Hall.

- Hair, J., Tatham, R. l., & Anderson, R. E. (2010). Multivariate Data Analysis. Upper Saddle River: Prentice Hall.
- Harman, L. B., Flite, C. A., & Bond, K. (2012). Electronic health records: privacy, confidentiality, and security. AMA Journal of Ethics, 14(9), 712-719.
- Hiller, J., McMullen, M. S., Chumney, W. M., & Baumer, D. L. (2011). Privacy and security in the implementation of health information technology (electronic health records): US and EU compared. BUJ Sci. & Tech, 17(1), 40 pp.
- Househ, M., Grainger, R., Petersen, C., Bamidis, P., & Merolli, M. (2018). Balancing between privacy and patient needs for health information in the age of participatory health and social media: a scoping review. Yearbook of Medical Informatics, 27(1), 29-36.
- Hoyle, R. H. (1995). Structural Equation Modeling: Concepts, Issues, and Applications. Thousand Oaks: SAGE.
- Katz, M. H. (2011). Multivariable Analysis. Cambridge: Cambridge University Press.
- Lehmann, E. L., & D'Abrera, H. J. (2006). Nonparametrics: statistical methods based on ranks. Springer.
- Liang, B. A. (2002). Medical information, confidentiality, and privacy. Hematology/oncology clinics of North America, 16(6), 1433-1447.
- Lynn, M. R. (1986). Determination and quantification of content validity. Nursing research, 35(6), 382-386.
- Maiorana, A., Steward, W. T., Koester, K. A., Pearson, C., Shade, S. B., Chakravarty, D., et al. (2012). Trust, confidentiality, and the acceptability of sharing HIV-related patient data: lessons learned from a mixed methods study about Health Information Exchanges. Implementation Science, 7(1), 34.
- Mansfield, S. J., Morrison, S. G., Stephens, H. O., Bonning, M. A., Wang, S.-H., Withers, A. H., et al. (2011). Social media and the medical profession. Medical journal of Australia, 194(12), 642-644.
- Meingast, M., Roosta, T., & Sastry, S. (2006). Security and privacy issues with health care information technology. International Conference of the IEEE Engineering in Medicine and Biology Society, 30 Aug.-3 Sept. 2006, New York, NY, USA (pp. 5453-5458). IEEE.

- Ministry of Health. (2017, June 15). Health Indicators for the Year of 1437 H. Retrieved March 2, 2019, from Ministry of Health: https://www.moh.gov.sa/en/Ministry/Statistics/Indicator/Pages/Indicator-1437.aspx
- Ministry of Health. (2018). Kingdom of Saudi Arabia: Health Overview 2018. Ministry of Health.
- Mohammadi, M., Larijani, B., Razavi, S. H., Fotouhi, A., Ghaderi, A., Madani, S. J., et al. (2018). Do patients know that physicians should be confidential? study on patients' awareness of privacy and confidentiality. Journal of medical ethics and history of medicine, 11, 1.
- Nayeri, N. D., & Aghajani, M. (2010). Patients' privacy and satisfaction in the emergency department: a descriptive analytical study. Nursing ethics, 17(2), 167-177.
- Oppenheim, A. N. (1992). Questionnaire design, interviewing and attitude measurement. London: Continuum International Publishing Group.
- ÖZKAN, Ö. (2011). ATTITUDES AND OPINIONS OF PEOPLE WHO USE MEDICAL SERVICES ABOUT PRIVACY AND CONFIDENTIALITY OF HEALTH INFORMATION IN ELECTRONIC ENVIRONMENT. THE GRADUATE SCHOOL OF INFORMATICS, THE DEPARTMENT OF MEDICAL INFORMATICS . THE MIDDLE EAST TECHNICAL UNIVERSITY.
- Pardoe, I. (2012). Applied Regression Modeling. New Jersey: Wiley.
- Pencarrick Hertzman, C., Meagher, N., & McGrail, K. M. (2012). Privacy by Design at Population Data BC: a case study describing the technical, administrative, and physical controls for privacy-sensitive secondary use of personal information for research in the public interest. Journal of the American Medical Informatics Association, 20(1), 25-28.
- Perera, G., Holbrook, A., Thabane, L., Foster, G., & Willison, D. J. (2011). Views on health information sharing and privacy from primary care practices using electronic medical records. International journal of medical informatics, 80(2), 94-101.
- Prater, V. S. (2014, December 8). Confidentiality, privacy and security of health information: Balancing interests. Retrieved March 6, 2019, from Health Informatics, University of Illinois,

Chicago: https://healthinformatics.uic.edu/blog/confidentiality-privacy-and-security-of-health-information-balancing-interests/

- Preacher, K., & Hayes, A. (2008). Asymptotic and resampling strategies for assessing and comparing indirect effects in multiple mediator models. . Behavior Research Methods, 879-891.
- Reynaldo, J., & Santos, A. (1999). Cronbach's Alpha: A Tool for Assessing the Reliability of Scales. Extension Journal, 37(2), 2TOT3.
- Rodrigues, J. J., De La Torre, I., Fernández, G., & López-Coronado, M. (2013). Analysis of the security and privacy requirements of cloud-based electronic health records systems. Journal of medical Internet research, 15(8), e186.
- Royston, P., & Sauerbrei, W. (2008). Multivariable Model - Building. West Sussex: John Wiley and Sons Ltd.
- Sajid, A., & Abbas, H. (2016). Data privacy in cloud-assisted healthcare systems: state of the art and future challenges. Journal of medical systems, 40(6), 155.
- Saunders, M., Lewis, P., & Thornhill, A. (2009). Research Methods For Business Students. Prentice Hall.
- Sekaran, U., & Bougie, R. (2016). Research methods for business: A skill building approach (7th ed.). John Wiley & Sons.
- Smith, L. F., Gratz, Z. S., & Bousquet, S. G. (2009). The Art and Practice of Statistics. Belmont: Cengage Learning.
- Tabachnick, B. G., & Fidell, L. S. (2001). Using Multivariate Statistics. Boston: Pearson.
- Tabachnick, B. G., & Fidell, L. S. (2007). Using Multivariate Statistics. Pearson.
- Van Allen, J., & Roberts, M. C. (2011). Critical incidents in the marriage of psychology and technology: A discussion of potential ethical issues in practice, education, and policy. Professional Psychology: Research and Practice, 42(6), 433-439.
- Victoria State. (2015, October). Confidentiality and privacy in healthcare. Retrieved March 6, 2019, from Better Health, Victoria State Governent: https://www.betterhealth.vic.gov.au/health/servicesandsupport/confidentiality-and-privacy-in-healthcare

- Wartenberg, D., & Thompson, W. D. (2010). Privacy versus public health: the impact of current confidentiality rules. American journal of public health, 100(3), 407–412.
- Wikimedia. (2006, December 26). Asia Sub-regions. Retrieved September 8, 2015, from Wikimedia: https://commons.wikimedia.org/wiki/File:Asia_subregions.png
- Wilkowska, W., & Ziefle, M. (2012). Privacy and data security in E-health: Requirements from the user's perspective. Health informatics journal, 18(3), 191-201.
- Wynd, C. A., Schmidt, B., & Schaefer, M. A. (2003). Two quantitative approaches for estimating content validity. Western Journal of Nursing Research, 25(5), 508-518.
- Yan, X., & Su, X. G. (2009). Linear Regression Analysis: Theory and Computing. Singapore: World Scientific Publishing Co. Pte. Ltd.

Appendix – Survey:

A. DEMOGRAPHIC INFORMATION

1. Gender: Male/Female
2. Age: <35, 35-50, >50
3. Educational qualifications: bachelor or less – master - doctorate
4. Total experience: less than 5 years, from 5-10 years, more than 10 years
5. Experience in medical information systems: less than 5 years, from 5-10 years, more than 10 years
6. Position in the hospital: Nursing, Management/IT, Doctor

B. STORAGE

7. How is the patient information stored:
   a. Paper
   b. Electronically
   c. Both

C. CREATION, ACCCESS AND SHARING OF PATIENT INFORMATION

8. The patient information is first written on paper and then filed 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
9. The patient information is first written on paper and transferred to computer later 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree

10. We use paper system and the information first written on paper is filed is immediately 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
11. The patient information written on a paper is filed later by an office staff 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
12. Doctors and/or any other hospital staff discuss other similar cases with patients? 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
13. Doctors and/or nurses or any other staff discuss cases of other patients when treating a particular patient? 1- Don't know, 2- strongly disagree, 3- disagree, 4- agree, 5- strongly agree
14. Doctors or nurses or any other staff discuss any patient information in presence of outsiders? 1- Don't know, 2- strongly disagree, 3- disagree, 4- agree, 5- strongly agree
15. I am fully involved in preparation of patient information in this hospital. 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
16. I am partially involved in preparation of patient information in this hospital. 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
17. I have unrestricted and full access to all patient information. 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
18. I have need-based access to patient information only. 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
19. I can demand information on any patient from the concerned officer and get it. 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
20. I cannot get patient information unless I justify it by explaining why I need it. 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
21. I don’t mind discussing the information with a patient anywhere in presence of others. 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree

Research Question 1: What is the reality of maintaining the confidentiality and privacy of medical information?

Assume that- confidentiality and privacy of patient information are not maintained in the hospitals properly. Inefficient and ineffective systems of information creation, storage and unrestricted access to those who have no relevant use do not ensure adequate maintenance of confidentiality and privacy of medical information.

22. In my opinion, confidentiality and privacy of medical information are maintained well by the hospitals 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
23. The current systems of creation, storage and access to medical information are adequate for their maintenance of confidentiality and privacy 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
24. The current systems of creation, storage and access to medical information are efficient in maintaining their confidentiality and privacy 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
25. The current systems of creation, storage and access to medical information are effective in maintaining their confidentiality and privacy 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
26. It is always ensured that only those for whom the information relevant to them can access medical information to their protect confidentiality and privacy 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree

Research Question 2: What are the technological methods to maintain the confidentiality and privacy of medical information?

Electronic recording by directly entering the information in the computer by the attending doctor or nurse can be done using a page per patient with an appropriate numbering system for patient identification. No paper system to be used.

Proper storage of medical information in a password protected master computer transmitted only to the computers of the relevant persons, which are also password protected. Adequate steps to protect malware attack and computer crashing to be given everywhere. Better to have an ICT specialist to take care of all hardware and software problems which can occur in any computer from time to time.

The electronic information is accessible only to the people for whom it has relevance to use recording system through their computers only. For a better safety, computers provided by the hospital only will have this facility.

27. Use of a distinct patient number is the safest method to identify the patient for access of information stored in the computer by valid users only 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree

28. Password protection of access to medical information data is an essential requirement for protection of confidentiality and privacy of medical information 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
29. All the computers of my hospital are frequently checked and updated on their security systems to prevent malware attacks and computer crashing 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
30. We have an ICT specialist in the hospital to take care of all hardware and software problems of any computer 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree

Research Question 3: What are the difficulties in achieving confidentiality and privacy of medical information?

When the above requirements of information generation, storage and access are not met, problems of maintaining confidentiality and privacy arise. Any other barriers and factors like hospital policies and strategies, employers, insurance, legal and regulatory policies, interference by influential people.

31. There are difficulties in ensuring that all records are made electronic in my hospital affecting confidentiality and privacy of medical information 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
32. There are difficulties ensuring that the current paper system is able to fully protect confidentiality and privacy of medical information 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
33. There are difficulties in ensuring that all paper records are filed or entered in the computer promptly leading to chances of loss of data, affecting confidentiality and privacy of medical information 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
34. There are difficulties of ensuring fool-proof storage system for medical information affecting confidentiality and privacy of medical information 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
35. There are difficulties of ensuring that only valid users can access the medical information stored in computer or files 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree

36. The hospital has loose policies and strategies for protection of confidentiality of medical information 1- Don't know, 2- strongly disagree, 3- disagree, 4- agree, 5- strongly agree
37. There is risk of losing confidentiality and privacy when information is shared with relatives, friends, employers or insurance people 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree
38. The government policies are inadequate, unclear or totally absent to protect confidentiality and privacy of medical information. 1- Don't know, 2-strongly disagree, 3- disagree, 4- agree, 5- strongly agree

المجلة السعودية لدراسات المكتبات والمعلومات

The Saudi Journal of Library and Information Studies