Journal of Health Informatics in Developing Countries

www.jhidc.org
Vol. 9 No. 2, 2015

Submitted: August 14, 2015 *Accepted: November 4, 2015*

An Evaluation of Information Security from the Users' Perspective in Turkey

Pınar KILIÇ AKSU[1], Nur ŞİŞMAN KITAPÇI[2], R. Özgür ÇATAR[2], Leyla KÖKSAL[2], Gonca MUMCU[2]

[1]*Faculty of Health Sciences, Yeditepe University, Istanbul, Turkey*

[2]*Department of Health Informatics and Management, Division of Health Management, Faculty of Health Sciences, Marmara University, Istanbul, Turkey*

Abstract.
Information security is a critical issue for hospitals, and users play an active role in their security process. The aim of this study was to evaluate the information security in a hospital from the users' perspective. In this cross-sectional study 424 hospital staff (medical: 258 / administrative: 166) were included. Face-to-face interviews were used to gather data in answer to a scaled questionnaire regarding information security. Items in the questionnaire were coded by a 5-point Likert scale (ranging from 1 point: strongly disagree to 5 points: strongly agree). After the factor analysis, it was possible to identify five subgroups relating to information security: Access and Authorisation, Security Applications, Service Delivery, Organisational Security and Security Policy. The items in the Service Delivery subgroup were scored lower by the medical staff than the administrative staff (p<0.05). Both the medical and administrative staff educated in HIMS gave higher scores to the information security subgroup (p<0.05). The roles and responsibilities of staff and their being educated in HIMS are crucial factors for information security. Since information security is a critical issue in hospitals, it is necessary to develop and share information security policies for all staff in such organisations.

Keywords. Information security, hospital information management system, staff, health manager.

1. Introduction

Nowadays, healthcare is strongly influenced by technological developments and innovations that improve the gathering, storage, transmission and processing of information in the organisations [1] [2]. Health professionals commonly use these systems for medical imaging and laboratory results, electronic prescribing and the monitoring of patients [3]. However, there may be resistance toward the imposition of any new technologies due to technical, organisational or individual factors in clinical practice [3] [4]. If new technologies can be proved to have a positive effect on their workflow, they could be more easily accepted [5].

In healthcare, privacy is a principle factor in the patient-physician relationship, as well as in the sharing of data with other health professionals to facilitate correct diagnosis and treatment [6]. This becomes a matter of greater importance when it is remembered that data are recorded and shared by different healthcare professionals at

[1] Corresponding Author, E-mail: pinarkilicaksu@yahoo.com

different locations [5]. Healthcare outcomes and patient satisfaction are improved through the utilisation of new technologies that increase the accessibility and continuity of healthcare [7]. However, legal problems arising from the loss of patients' health data and the financial information of healthcare organisations must also be factored into any application of new technology [3]. In addition, malpractice could also occur if patient's records are not available or missing [8]. Therefore, information security is seen as an important topic in hospitals. They are complex organisations with different divisions and many of them use the Hospital Information Management System (HIMS) to provide continuous healthcare [3].

Information security is defined as the prevention of unauthorised or undesirable destruction, modification or use of information resources at both the individual and organisational level [8]. Information security is a critical point in healthcare [6]. The authorisation and proper use of data by staff are the key issues for organisations [5]. However, security problems could also be accidental or intentional [6]. Since users play an active role in the security process in organisations, insufficient awareness on the part of staff becomes a crucial matter [8].

According to the structure of healthcare system in Turkey, state hospitals and medical school hospitals are the main organisations. After the implementation of health transformation programme, private hospitals become a part of the system in the country. Large and small private ones providing patient care with specialized staff and equipment spread all over the country [9]. Many physicians and health administrators work in these organisations. Therefore, the aim of this study was to evaluate information security in a private hospital within the framework of the users' perspective.

2. Material and methods

In this cross-sectional study, 424 participants from the 489 employees of a private hospital using HIMS in their workflow were included in the study. The study was carried out from February 15 to May 28 in 2013. The response rate was found to be 86.7%. Data were collected with a constructed questionnaire form regarding socio-demographic characteristics, an information security scale and questions relating to information security applications in hospitals. The self-reported "ability to use of HIMS" and "security of the system" were evaluated by 100-mm visual analogue scale (0: very poor vs 100: very good).

The information security scale developed by Upfold and Sewry was not intended for the health sector [10] [11]. Ethical permission was taken from the developers to apply it in this study. Twenty-one items of the scale were selected according to their suitability with regard to the health professionals in the hospital, and 6 items regarding literature were also added. Four statements were converted to "positive" to be compatible with the other statements in the questionnaire. The final form of the questionnaire was used in backward and forward translations with cross-cultural adaptation guidelines [12]. The questionnaire was scored with a five-point Likert scale (1: strongly disagree, 2: disagree, 3: neutral, 4: agree, 5: strongly agree). A pilot study was conducted with 10 employees to evaluate their comprehension of the questionnaire form. Construct validity was evaluated by explanatory factor analysis.

The study was performed according to the principles of the Declaration of Helsinki and was approved by the Ethical Committee of Marmara University Health Institute.

3. Statistical Analysis

An unpaired T test was used in the comparison of scores whereas Mann-Whitney U test was used in non-normal distribution of data. The multi-dimensional properties of the information security scale were tested by factor analysis. During the research, the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and the Barlett's Test of Sphericity (BTS) were conducted on the data prior to factor extraction to ensure that the characteristics of the data set were suitable for the explanatory factor analysis to be conducted. The KMO analysis yielded an index of 0.90, indicating that the data satisfied the criteria for the factor analysis. The principal component analysis produced five distinct factors with eigen values of >1, thereby explaining 63.26% of the variance. The subscales were security policy, organisational security, security applications, service delivery and access and authorisation in the information questionnaire (Table 1). The mean subgroup scores were calculated in the scale and the data were analysed according to these scores.

The Cronbach's alpha values were 0.8157, 0.8185, 0.8017, 0.9019 and 0.8963, demonstrating a high internal reliability for all subscales. Intra-observer reliability could be analysed in of 10% of the staff (n=43). No significant difference was seen in the scores of the group.

Table 1: The Distribution of Items in Information Security Questionnaire According to Factor Analysis

	Factors				
	Access and Authorisation (n=9)	**Security Applications (n=5)**	**Service Delivery (n=4)**	**Organisational Security (n=5)**	**Security Policy (n=4)**
1. Users may not logon / gain access to our systems without being formerly registered with their own user account.	0,790				
2. We ensure that information processing facilities are only used for authorised business purposes.	0,732				
3. Our organisation controls access to information via an access control policy which specifies which users have access to what data.	0,699				
4. Despite being connected to public networks, we are confident that our systems are adequately protected by our internet service provider's security and /	0,680				

	or our own firewalling systems.			
5.	Our systems are updated / upgraded according to a structured plan and not in an ad-hoc fashion.	0,663		
6.	We are confident that our anti-virus systems are up to date and in the event of a virus outbreak, we should be able to protect our systems as best as possible.	0,608		
7.	In the event of a security incident, procedures clearly define what to do and who to call for assistance.	0,581		
8.	A password management system is in place which specifies the frequency of password changes as well as the minimum password complexity.	0,547		
9.	Appropriate mechanisms are in place to authenticate users logging onto our systems.	0,460		
10.	There is a formal disciplinary process for employees who have violated our security policies and processes.		0,761	
11.	Staff have been trained to secure their computers at all times, when moving away from their work stations.		0,701	
12.	Staff are aware that security incidents must be reported to management immediately.		0,629	
13.	Expertise on information security is available internally and where not, external advice is sought.		0,550	
14.	We are confident that in the event of equipment failure, theft or site disaster, our data backups and storage would enable us to retrieve our information with minimal business interruption		0,521	
15.	Changes in the workflow with computer use, do not prevent the granting of the necessary importance to information security.			0,907

16. Information security process does not adversely affect the quality of service			0,888		
17. Information security is a priority issue among daily works.			0,881		
18. Having more workload in a organisations does not prevent the granting of the necessary importance to information security			0,876		
19. A director (or equivalent) member of our staff has responsibility for information security.				0,799	
20. Directors take care to improve information security in the organisation.				0,780	
21. There is a nominated person in our organisation who is expertise on information security.				0,606	
22. Staffs take care to improve information security in the organisation.				0,532	
23. Staff are well informed as to what is considered to be acceptable and unacceptable usage of our information systems.				0,429	
24. Staff are aware of our information security policy.					0,738
25. We have a documented information security policy.					0,737
26. Roles and responsibilities for information security in our organization are well defined.					0,723
27. All staff are given adequate and appropriate information security education and training.					0,715
Variance (%)	**35,03**	**11,81**	**6,96**	**5,09**	**4,35**
Cronbach's alpha values	**0.8157**	**0.8185**	**0.8017**	**0.9019**	**0.8963**

4. Results

In this study, 424 staff were included. 60.8% of the group were administrative staff (F / M: 118 / 48; mean age: 26.9 ± 5.5 years) and 39.2% were medical staff (F / M: 148 / 110; mean age: 30.4 ± 7.8 years). There were no significant differences between groups with regard to period of employment within the organisation, experience and education in HIMS (medical staff: 27.4±18.39 months; 37.74±41.05 months; 3,97±8,04 hours vs administrative staff: 25.53±19.67 months; 37,02±46,01 months; 4.62±7.26 hours, respectively) (p>0.05). The self-reported scores of the administrative staff with regard to "***ability to use HIMS***" (76.39±18.23) and "***security of system***" (65.01±23.52) were significantly higher compared to those of the medical staff (71.68±20.01; 58.69±16.77, respectively) (p=0.016 and p=0.04, respectively).

According to the items in the "***Security Policy***" subgroup, the medical staff score for "***Roles and responsibilities for information security in the organisation***" was significantly higher (3.49±0.82) than that of the administrative staff (3.31±0.97) (p=0.047). Scores for "***Being aware of security policy***", "***Documentation of information security policy***" and "***Giving information security education***" were similar in both staff groups (p>0.05) (Table 2).

Table 2: Scores of Items in Security Policy and Organisational Security Subgroups According to Medical and Administrative Staff

	Medical Staff		Administrative Staff		
Security Policy	**Mean**	**SD**	**Mean**	**SD**	**p***
Roles and responsibilities for information security in our organization are well defined.	3,49	0,82	3,31	0,97	**0.047**
We have a documented information security policy.	3,45	0,85	3,28	0,99	0.054
Staff are aware of our information security policy.	3,25	0,93	3,22	1,04	0.803
All staff are given adequate and appropriate information security education and training.	3,16	0,92	3,09	1,08	0.472
Organisational Security					
A director (or equivalent) member of our staff has responsibility for information security.	3,71	0,83	3,6	0,98	0.212
There is a nominated person in our organisation that is expertise on information security.	3,46	0,91	3,27	1,04	0.500
Staff take care to improve information security in the organisation.	3,37	0,83	3,34	1,07	0.189
Directors take care to improve information security in the organisation.	3,56	0,89	3,63	0,93	0.477
Staff are well informed as to what is considered to be acceptable and unacceptable usage of our information systems.	3,44	0,96	3,45	1,03	0.885

*Unpaired t tets was used

Similar results were found for "***Organisational Security***" items regarding "***A director's role and responsibility in security***", "***Having nominated person on***

information security", and "***Staff role and responsibility for information security***" (p>0.05) (Table 2).

The administrative staff scored "***Having education for safety computer use***" were higher, but scored "***Having expertise on information security***" lower compared to the medical staff (p = 0.036 and p = 0.038, respectively). No significant difference between the groups was seen in the other "***Security Applications***" related items (p > 0.05). The medical staff scored the "***Service Delivery***" subgroup items including "***Having more workload***", "***Effect on quality of service***", "***Priority of information security***" and "***Changes in workflow***" lower in comparison to the administrative staff (p < 0.05) (Table 3).

Table 3: Scores of Items in Security Applications and Service Delivery Subgroups According to Medical and Administrative Staff

	Medical Staff		**Administrative Staff**		
Security Applications	**Mean**	**SD**	**Mean**	**SD**	**p***
Staff are aware that security incidents must be reported to management immediately.	3,54	0,95	3,62	1,04	0.411
Staff have been trained to secure their computers at all times, when moving away from their work stations.	3,53	0,97	3,75	1,07	**0.036**
There is a formal disciplinary process for employees who have violated our security policies and processes.	3,38	0,99	3,41	1,22	0.828
Expertise on information security is available internally and where not, external advice is sought.	3,27	1,05	3,04	1,13	**0.038**
We are confident that in the event of equipment failure, theft or site disaster, our data backups and storage would enable us to retrieve our information with minimal business interruption	3,63	0,94	3,52	1,1	0.303
Service Delivery					
Having more workload in a organisation does not prevent the granting of the necessary importance to information security.	2,87	1,36	3,21	1,27	**0.010**
Information security process does not adversly affect the quality of service.	2,49	1,24	2,95	1,22	**0.000**
Information security is a priority issue among daily works.	2,46	1,27	2,76	1,32	**0.023**
Changes in the workflow with computer use, do not prevent the granting of the necessary importance to information security.	2,59	1,28	2,92	1,14	**0.007**

* Unpaired t test was used.

No significant difference was seen in the groups' scores of the "***Access and Authorisation***" subgroup related items (p>0.05) (Table 4).

Table 4: Scores of Items in Access and Authorisation Subgroup According to Medical and Administrative Staff

	Medical Staff		Administrative Staff		
	Mean	**SD**	**Mean**	**SD**	**p***
Our systems are updated / upgraded according to a structured plan and not in an ad-hoc fashion.	3,59	0,9	3,42	1,04	0.088
In the event of a security incident, procedures clearly define what to do and who to call for assistance.	3,67	0,94	3,52	1,03	0.142
We are confident that our anti-virus systems are up to date and in the event of a virus outbreak, we should be able to protect our systems as best as possible.	3,59	0,9	3,67	0,95	0.397
Despite being connected to public networks, we are confident that our systems are adequately protected by our internet service provider's security and / or our own firewalling systems.	3,65	0,89	3,53	0,99	0.205
Appropriate mechanisms are in place to authenticate users logging onto our systems.	3,96	3,32	3,67	1,04	0.266
Users may not logon / gain access to our systems without being formerly registered with their own user account.	3,87	0,93	3,95	0,98	0.408
A password management system is in place which specifies the frequency of password changes as well as the minimum password complexity.	3,54	1,07	3,6	1,07	0.566
Our organisation controls access to information via an access control policy which specifies which users have access to what data.	3,7	0,98	3,74	0,97	0.750
We ensure that information processing facilities are only used for authorised business purposes.	3,8	0,94	3,78	1,07	0.884

* Unpaired t tets was used

When the influences of HIMS on the information security related subgroups were examined, all of the subgroup scores of the medical staff who had HIMS education were higher than those who had not ($p < 0.05$). In the administrative staff, the subgroups for "***Access and authorisation***", "***Security applications***" and "***Organisational security***" were scored higher by those with HIMS education ($p < 0.05$). However, education in HIMS produced no significant differences in the administrative staff scores for "***Service delivery***" and "***Security policy***" (p = 0.787 and p = 0.208, respectively) (Table 5).

Table 5: Scores of Subgroups in Medical and Administrative Staff According to Education Status for HIMS

		Education status for HIMS	**Mean**	**SD**	**p**
Medical Staff	Access and Authorisation	Education (+) (n=203)	3,788	0,64879	**0.000**
		Education (-) (n=49)	3,337	0,73070	
	Security Applications	Education (+) (n=203)	3,553	0,70136	**0.001**
		Education (-) (n=49)	3,167	0,72841	
	Service Delivery	Education (+) (n=203)	3,525	1,15302	**0.000**
		Education (-) (n=49)	2,862	0,99224	
	Organisational Security	Education (+) (n=203)	3,609	0,68151	**0.001**
		Education (-) (n=49)	3,265	0,57211	
	Security Policy	Education (+) (n=203)	3,428	0,671	**0.000**
		Education (-) (n=49)	2,994	0,802	
Administrative Staff	Access and Authorisation	Education (+) (n=109)	3,792	0,728	**0.001**
		Education (-) (n=50)	3,351	0,816	
	Security Applications	Education (+) (n=109)	3,620	0,806	**0.001**
		Education (-) (n=50)	3,144	0,864	
	Service Delivery	Education (+) (n=109)	3,016	1,094	0.787
		Education (-) (n=50)	3,065	0,969	
	Organisational Security	Education (+) (n=109)	3,592	0,733	**0.004**
		Education (-) (n=50)	3,208	0,819	
	Security Policy	Education (+) (n=109)	3,286	0,828	0.208
		Education (-) (n=50)	3,110	0,797	

5. Discussion

Since information technology is an important factor in the improvement of health service quality [13][14][15][16], information security is a critical issue for HIMS [17]. It is defined as confidentiality, integrity and accessibility of electronic data regarding both the clinical and financial information held by the organisation [18]. However, information security is not well evaluated according to roles and responsibilities of hospital staff. In the present study, information security in a hospital was evaluated within the framework of the users' perspective.

Although both the medical and administrative staff within the organisation had similar periods of employment, as well as similar levels of education and experience in HIMS, the administrative staff gave higher scores regarding their ability to use the system. They also gave higher scores to the security of HIMS. Users play an important role in the information security performance of organisations due to their security awareness and behaviour [19]. Several stakeholders: physicians, nurses and administrators have different experiences in the hospitals [7]. Since information technology is at the center of the workflow of the administrative staff, these results could be predicted.

According to the Security Policy subgroup, the medical staff scored “Roles and responsibilities for information security in the organisation” more highly than the administrative staff. However, both staff groups gave similar scores to the other items in the Security Policy subgroup. A different user pattern could be produced by a wider application of HIMS. If various technical, legal and policy issues are recommended, clinical databases that are critical for medical staff can be protected [15][20][22]. Therefore, information security policies regarding processing, receiving, modifying, disseminating, sending, storing and disposing of patients’data are needed for information security culture in the organisations [18]. The responsibilities and procedures should be reported to staff, and a continuing improvement plan for both administrative and medical applications should become part of the information-security culture in an organisation [23].

The scores regarding the organisational security items were similar in both staff groups. If information security applications in organisations could focus on employee behaviour, an information security-aware culture will reduce the risks caused by employee misbehaviour. Both managers and staff could affect the process of information security in their organisation. Therefore, guidance from directors or experts is required to establish an information security culture. Compliance depends upon employee behaviour and acceptable conditions [19]. Developing information security guidelines and assigning a specific person or team who can take full responsibility for information assets are necessary for hospitals in the short-term, but formulating health information security policy by involving all stakeholders from the health sector will be required in the in long-term [6] [5].

In comparison with the medical staff, the administrative staff scored “Education in safe computer use” more highly than “Having expertise in information security” in the Security Applications subgroup. The other scores were similar in both staff groups. These differences could be predicted by taking into account the the roles of the staff. Misuse of computers is increasing with a million patients’ data currently stored in the system. Good end user security-related behavior as a core component provides effective information security within organisations [19]. Cleaning desks and locking computers when leaving the workspace are necessary to eliminate unauthorised access [8]. Security management programs must include security incidents and evaluations of their impact, as an organisation’s processes and operations are directly influenced by its security policies [24].

Similar scores were obtained for the “Access and authorisation” subgroup. Although technical protection methods are important, user-related faults remain a major problem for information security in organisations [6]. Access control to unauthorized software programs as well as using password policies virus scanners and firewalls [5] [6] are commonly used to improve security [8]. Yet, the weakness of password protection is also known [5]. If passwords are too short or simple, they are useless for the system [25]. Users should have a unique identification since authentication is based on a personal password [5]. Moreover, the access rules cannot be standardised [5]. In healthcare, the critical point is to determine who has access to the data, especially in emergency cases. The role-based access control is the most common method for access criteria in the system [26]. In contrast, staff could inspect the patient records of family members, friends, colleagues and famous persons even though it is not allowed within the framework of information security policies. The other important point is that portable devices such as laptops are often less protected than desktops [25]. Therefore, staff should be regularly reminded of their obligations [8].

The medical staff scored “Service Delivery” lower in comparison to the administrative staff. It is known that the awareness and behavior of staff is perceived as one of the most common problems in information security [8] [26]. The medical staff scored “Service delivery” lower in comparison to the administrative staff. It is known that the awareness and behavior of staff is perceived as one of the most common problems in information security [7]. Therefore, the acceptance of new technologies for medical staff is affected by their clinical requirements and their workflows. Moreover, emergency plans should be developed to eliminate system-related technical problems and loss of patients’ data in clinical practice because continuity of healthcare is critical in hospitals [8]. Medical staff should not be affected by new technologies in information security applications producing greater workloads or changes to their workflows. Consequently, medical staff, as end-users, could be informed about the security applications for the organisational culture [27].

Education for HIMS was observed to be a critical point to improve information security in the organisation. End-user satisfaction with the system depends on user acceptance and usability issues. Increases in the efficiency of staff could be improved by healthcare education [28]. Education is a critical component of successful management of information security [23] because information security awareness could change user behavior [6].

Health managers should actively support an information-security culture [5,6,23] and protect different information sources by applying regulations to their organisations [23]. Since insufficient awareness among staff is the most common problem [8], having an information security coordinator and written policies for a disaster recovery plan, controlling access to different levels of electronic data, testing backups, protecting against viruses, installing firewalls and undertaking routine maintenance of hardware and software are necessary to resolve security issues [29]. Moreover, risk assessment is also critical for health managers. Information-security policies, standards and guidelines should be published and delivered to all staff to produce an information-security culture. These applications should be reviewed regularly to eliminate weaknesses in HIMS [23].

The presented, information security questionnaire focused on health care may help improving the awareness for information security and decision-making process in information security management in organisations, especially in developing countries.

In conclusion, the roles and responsibilities of staff and being educated in the use of HIMS are crucial factors for information security. With regard to the information security questionnaire, internal reliability was observed to be very high. Intra-observer variations were not seen. The questionnaire could be useful for the evaluation of information security within the framework of the users’ perspective and in the production of information security policies in hospitals. Yet, further studies using this questionnaire for healthcare are necessary.

References

[1] Borzekowski, R., Measuring the cost impact of hospital information systems: 1987 1994. *J Health Econ*, 2009. **28**(5): p. 938-49.

[2] Kluge, E.H., Ethical and legal challenges for health telematics in a global world: telehealth and the technological imperative. *Int J Med Inform*, 2011. **80**(2): p. e1-5.

[3] Civelek, A.C., Patient safety and privacy in the electronic health information era: medical and beyond. *Clin Biochem*, 2009. **42**(4-5): p. 298-9.

[4] Anderson, J., et al., Testing the validity, reliability and utility of the Self-Administration of Medication (SAM) tool in patients undergoing rehabilitation. *Res Social Adm Pharm*, 2014. **10**(1): p. 204-16.

[5] Bakker, A.R., The need to know the history of the use of digital patient data, in particular the EHR. *Int J Med Inform*, 2007. **76**(5-6): p. 438-41.

[6] Gebrasilase T, L.L., Information security culture in public hospitals: The case of Hawassa Refferal Hospital *The African Journal of Information Systems*, 2011. **3**(3): p. 72-86.

[7] Lapointe, L., M. Mignerat, and I. Vedel, The IT productivity paradox in health: a stakeholder's perspective. *Int J Med Inform*, 2011. **80**(2): p. 102-15.

[8] Wirken, Information Security in Dutch Hospitals:Master thesis Content and Knowledge. *Engineering Faculty of Science*, 2012: p. 41-53.

[9] Health, M.o., http://www.saglik.gov.tr/.

[10] Upfold CT, S.D., An investigation of information security in small and medium enterprises in the Eastern Cape AND MEDIUM ENTERPRISES (SME'S)IN THE EASTERN CAPE. http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/082_Article.pdf, Accessed November 2014.

[11] Yildirim EY, A.G., Aytac S, Bayram N., Factors influencing information security management in small- andmedium-sized enterprises: A case study from Turkey. *International Journal of Information Management* 2011. 31: p. 360-365.

[12] Beaton, D.E., et al., Guidelines for the process of cross-cultural adaptation of self-report measures. *Spine*, 2000. **25**(24): p. 3186-3191.

[13] Mumcu G, Köksal L, Korkmaz B, Gök MM, Bulu B, Kitapçı-Şişman N, Kılıç-Aksu P, Tarım M., The Healthcare Quality and Hospital Information Management System: A Sample From Turkey. *Acıbadem Health Sciences Journal*, 2014. 5: p. 31-37.

[14] Aldosarı, B., An evaluation of EHR system audit function in a Saudi Arabian Hospital. *Journal of Health Informatics in Developing Countries*, 2012. **6**(2): p. 496-508.

[15] Abdullah I. Alkraiji, O.E.-H., Fawzi A. Amin, Health Informatics Opportunity and Chalanges: Preliminary Study in the Cooperation council for the Arab States of the Gulf. *Journal of Health Informatics in Developing Countries*, 2014. **8**(1): p. 36-45.

[16] Saleem, T., Implementation of EHR/EPR in England: a Model for Developing Countries. *Journal of Health Information in Developing Countries*, 2009. **3**(1): p. 10-12.

[17] Mumcu G, Köksal L, Şişman N, Çatar RÖ, Tarım M., The effect of pharmacy information management system on safety medication use: A study from private hospitals in İstanbul. *Marmara Pharmaceutical Journal*, 2014. 18: p. 1-4.

[18] Schattner, P., et al., Guidelines for computer security in general practice. *Inform Prim Care*, 2007. **15**(2): p. 73-82.

[19] Stanton JM, S.K., Mastrangelo P., Analysis of end user security behaviors. *Computers & Security*, 2005. **24**(2): p. 124-133.

[20] Kralewski, J.E., et al., Factors influencing physician use of clinical electronic information technologies after adoption by their medical group practices. *Health Care Manage Rev*, 2008. **33**(4): p. 361-7.

[21] Malin, B., D, Karp. and R.H. Scheuermann, Technical and policy approaches to balancing patient privacy and data sharing in clinical and translational research. *J Investig Med*, 2010. **58**(1): p. 11-8.

[22] Moonian, O., A Distributed Electronic Patient Record System for the Mauritian Healthcare Service. *Journal of Health Informatics in Developed Countries*, 2009. **3**(2): p. 37-43.

[23] Landolt, S., et al., Assessing and comparing information security in swiss hospitals. *Interact J Med Res*, 2012. **1**(2): p. e11.

[24] Ohki E, H.Y., Kawaguchi S, Shiozaki T, Kagaua T., Information Security Governance Framework. ttp://www.yumpu.com/en/document/view/9533455/information-security-governance-framework-jhu-department-of-, 2013.

[25] Mole, D.J., C. Fox, and G. Napolitano, Electronic patient data confidentiality practices among surgical trainees: questionnaire study. *Ann R Coll Surg Engl*, 2006. **88**(6): p. 550-3.

[26] Carrion Senor, I., J.L. Fernandez-Aleman, and A. Toval, Are personal health records safe? A review of free web-accessible personal health record privacy policies. *J Med Internet Res*, 2012. **14**(4): p. e114.

[27] Ayatollahi, H., et al., What factors influence emergency department staff attitudes towards using information technology? *Emerg Med J*, 2013. **30**(4): p. 303-7.

[28] Bey HY, W.T., Marcelo C, Jong MH, Chieh YL, Ting TL., Evaluation of computerized physician order entery system – A satisfaction survey in Taiwan. *Journal of Medical Systems*, 2012. 36: p. 3817-3824.

[29] Schattner, P., P.C., Bhend H, Brouns J., Guidelines for computer security ingeneral practice. *Informatics in Primary Care*, 2007. 15: p. 73-82.