ORIGINAL PAPER

An Assessment of Health Information Systems Through the Perspective of Computer Engineering Students and Medical Students

Esra Sevimli[1], Elif Naz Altingoz[2], Nur Şisman Kitapci[2], Okan Cem Kitapci[2], Leyla Koksal[2], Meral Yay[3], Pınar Kilic Aksu[4], Gonca Mumcu[2]

[1]İstanbul Arel University, Istanbul, Turkey
[2]Marmara University, Istanbul, Turkey
[3]Mimar Sinan Fine Arts University, Istanbul, Turkey
[4]Yeditepe University, Istanbul, Turkey

Corresponding author: Esra Sevimli, Instructor, Department of Health Institutions Administration, Istanbul Arel University, Turkey, E-mail: esra.sevimli429@gmail.com. ORCID ID:http://www.orcid.org/0000-0001-7119.

ABSTRACT

Introduction: Computer Engineering Students (CES) and Medical Students (MS) will actively participate in the management of health information system in the future. **Aim:** The aim of the study was to evaluate the views of CES and MS about the patient privacy and security of health information systems. **Methods:** The participants of this cross-sectional study were the 3rd and 4th year CES of Marmara University, (n=163, F/M:71/92) and the 5th and 6th year MS of Marmara University (n=65, F/M:38/27). The data were collected via questionnaire comprising questions and statements about patient information security and confidentiality. Responses were prepared on the basis of 5 Point Likert Scale. **Results:** During the assessment of the questionnaires, it was observed that the statement *"Health records should be accessible to the other health workers besides the physician"* discomforted more CES (93,3%) than MS (78,5%) (p=0.003). A similar proportion was observed about *"On-line communication with the physician"* more CES (87,1%) prefer to communicate with the physician via electronic media than do the MS (66,2%) (p=0.001). Another significant point to be noted about the questionnaire results was that slightly more CES (40,5%) favor restrictions on the accessibility of *"personal correspondance information"* than MS (35,4%) (p>0.05). **Conclusion:** In the future, CES, who will be both internal and external stakeholders of the multi-disciplinary structure of healthcare management, thought that problems regarding security and privacy may occur. Therefore, the relation between health information system and the occupational education and training of CES and MS are extremely important through the perspective in healthcare management.

Keywords: Information Security, Privacy, Confidentiality, Health Information System.

1. INTRODUCTION

In our globalizing world, the increasing need for communication and developments in the computer science has been playing an important part in the introduction and implementation of Information Technologies (IT) in healthcare (1, 2).

Healthcare services are information-based and most clinical practices require accumulating, processing and associating the collective data to carry out their practices effectively. In order to render healthcare services more efficient, enormous amounts of information must be managed. Nowadays like all the other organizations, healthcare organisations also keep their data in an electronic environment and process this information by using IT systems (2, 3, 4).

Establishing a well-organized flawless healthcare system necessitates a well-managed IT system in the digital age (5). The use of IT with appropriate data processing systems for health-

care services assists and supports patient care at all its stages effectively; therefore, electronic records and e-health applications form the basis of the modern healthcare sector practices (2, 6). In this manner, computerised and digitized information improves the quality of health information management, owing to increased speed, integration of data and easy access to all sources; however, this advantage may be undermined by the developments in current technologies.

One of the major issues in IT is information security, ie, ensuring the safe storage and exchange of Electronic Health Records (EHR) without the intervention of external factors. Information security can be defined as; the prevention of unauthorised use and taking protective measures against the exploitation, modification or disruption of data at individual or organisational level (7). Therefore, information security is a serious issue which should be strictly considered while exchanging and safeguarding all relevant information (8, 9, 10). Since health data is personal and the patients' privacy must be protected at all costs, the secure management of patient information is an indispensible and highly sensitive issue.

2. AIM

This study aimed to assess the opinions of CES and MS about the privacy, security and confidentiality of health information systems, as these students will be an active part of the system in the future.

3. METHODS

The sample group of this study consisted of Marmara University Computer Engineering 3rd and 4th year students (CES; n=163, F/M:71/92; mean age: 22,44±1,42 years); whereas, the control group includes 5th and 6th year students of the Faculty of Medicine (MS; n=65, F/M:38/27; 23,38±1,20 yrs) of the same university. Data were collected by face to face interviews using the questionnaire based on previous studies [Anderson (2007), Appari and Johnson (2010), Gebrasilase and Lessa (2011), Kılıç Aksu et al. (2015), Lekkas and Gritzalis (2007) and Aldosarı (2012)].

The questionnaire consisted two sections; participants' socio-demographic characteristics and participants' knowledge and opinions about security issues regarding he-

alth information systems and patient privacy. In the study, items in the questionnaire were assessed by a Likert 5-point Scale (1 point: strongly disagree vs 5 points: strongly agree).

Statistical Analysis

The collected data were analyzed by SPSS 25. In this descriptive study, Chi-Square Test was used in the anaysis of the categorical data. The statements used in the questionnaire and assessed according to the Likert 5-point Scale, were analysed with ANOVA and Unpaired Student's T-Test, since they matched with the normal distribution. As a criterion for its statistical significance level, $p<0.05$ was accepted as a standard.

4. RESULTS

In the present study, It was observed that more CES (93,3% n=152) than MS (78,5% n=51) expressed a sense of discomfort or unease regarding the access to health data by the health service personnel, besides the physicians (p=0.003). However, a lower proportion of CES (44,2% n=72) than MS (60,0% n=39) thought that e-health data included incorrect or missing information (p=0.031). In addition, the CES who wanted more frequent on-line contact with the physician regarding health issues (87,1% n=142) outnumber the MS (66,2% n=43) demanding this sort of contact (p= 0.001) (Table 1).

When the responses to the statement *"the personal information I confided in the health institution may be revealed to another institution that I would not wish to share it with"* were compared according to whether the study group had received any health care within the last 6 months. The CES who have received any health care within the last 6 months (1,56±0,95) scored higher than those who have not (1,25±0,56) (p=0.009). Similarly, the statement *"healthcare institutions may allow third parties to access my personal data without my permission"* received higher

Information accessible on the system		Faculty/Department				p*
		Computer Engineering Students		Medical Students		
		n	%	n	%	
Would access to your health data by health staff other than your physician/doctor disturb/ discomfort you?	Yes	152	93,3	51	78,5	0.003
	No	11	6,7	14	21,5	
	Total	163	100,0	65	100,0	
Do you think that your health data on the EHR system may be inaccurate or incomplete?	Yes	72	44,2	39	60,0	0.031
	No	91	55,8	26	40,0	
	Total	163	100,0	65	100,0	
Would you like to contact your physician /doctor on line?	Yes	142	87,1	43	66,2	0.001
	No	21	12,9	22	33,8	
	Total	163	100,0	65	100,0	

Table 1. Opinions of the Study Group Regarding the Health Information System. * Analyzed by Chi-square Test

points from the students who have received any health care within the last 6 months (1,40±0,82) than those who have not (1,15±0,36) (p=0.011). The statement *"it is easy for a physician to set a treatment plan with the patient by using information and communication technologies"* also received higher points from the students who have received any health care in the last 6 months (3,98±0,88) than those who have not (3,52±1,02) (p=0.004). However, the statement *"patients' relatives have information about the right of privacy"* received slightly more points from students who have not received any health care recently (2,52±0,94) than those who have (2,20±0,93) (p=0.034). Another statement that revealed similar results was *"unauthorized persons do not have access to patients' health data"*. It was agreed on by more students who have not received any health care recently (4,12±1,04); than those who have (3,70±1,34) (p=0.026). The other results did not indicate statistically differences (p>0.05) (Table 2).

In general, the overall responses of the MS, who have or have not received any health care in the last 6 months indicate no statistically significant differences in the mean scores from the other items in the questionnaire (p>0.05) (Table 2).

When the responses of the students who had received health care within the last 6 months were compared, the statement *"the unauthorized personnel do not have access to the patients" health records'* was observed to be rated higher by the MS (MS: 4,49±0,61 vs CES: 3,70±1,34) (p=0.000).

5. DISCUSSION

Healthcare organisations as information-intensive institutions collect, classify, organize, share, store and transmit health data to improve the quality of the healthcare services (5, 11, 12). The existence of personal health data in the electronic environment poses a threat to patient privacy and information confidentiality (13, 14). To eliminate this threat, information security is a vital issue for all institutions that provide healthcare services (8, 15). It is significant for the hospitals to determine what kind of data the health personnel is authorized to have access to (13). This study aimed to asses the opinions of CES and MS on health information systems in the perspective of data security and privacy because these students are the potential inner and outer components of the multidciplanary structure of healthcare services in the future.

In the health sector, the privacy of patient information is a fundamental factor in establishing a trust-based physician-patient relationship (16). There were statistically significant differences be-

| Variables | Have you undergone a medical treatment in the last 6 months? | Faculty/Department | | | | | |
| | | Computer Engineering Students | | | Medical Students | | |
		Mean	Std. Deviation	p*	Mean	Std. Deviation	p*
The personal information I confided in the health institution may be revealed to another institution that I would not wish to share it with.	Yes	1,56	0,95	0.009	1,37	0,49	0.397
	No	1,25	0,56		1,25	0,45	
Health institutions might allow third parties to access my personal information and EHR.	Yes	1,40	0,82	0.011	1,55	0,74	0.421
	No	1,15	0,36		1,38	0,81	
I feel unprotected during an E-health transaction on the system.	Yes	3,18	1,17	0.141	2,92	1,30	0.448
	No	2,92	0,99		2,69	0,95	
I do not think that E-Health transactions can be done securely.	Yes	3,09	1,12	0.604	3,00	1,21	0.274
	No	3,00	1,08		2,63	1,09	
It is easy for the physician to make a treatment plan with the patient by using ICT (Information and Communication Technologies).	Yes	3,98	0,88	0.004	3,82	0,97	0.056
	No	3,52	1,02		3,25	1,13	
The doctors can easily exchange information by using ICT.	Yes	3,97	1,00	0.289	4,10	0,80	0.151
	No	3,80	0,99		3,56	1,36	
Using ICT in the exchange of patient health data would not pose a threat to patient privacy and information confidentiality.	Yes	2,67	1,29	0.601	2,67	1,21	0.889
	No	2,57	1,17		2,63	1,15	
Patients are well-informed about their privacy rights.	Yes	2,29	0,96	0.175	2,14	1,02	0.359
	No	2,49	0,94		1,88	0,96	
Patients' relatives are well-informed about privacy rights.	Yes	2,20	0,93	0.034	2,06	0,90	0.809
	No	2,52	0,94		2,13	0,96	
Health institutions take the required measures against violations of privacy rights.	Yes	2,60	0,96	0.358	2,67	1,09	0.127
	No	2,74	0,87		2,19	1,11	
Patients' health data are securely recorded and kept.	Yes	2,61	1,02	0.279	2,84	1,09	0.089
	No	2,78	0,94		2,31	0,95	
Unauthorized personnel cannot access patients' health data.	Yes	3,70	1,34	0.026	4,49	0,62	0.256
	No	4,12	1,04		4,25	1,00	
Using mobile technology does not have an adverse effect on information security and confidentiality.	Yes	2,64	1,23	0.887	2,78	1,19	0.525
	No	2,62	1,18		2,56	1,03	

Table 2. The Comparisons of the Statements in Groups According to Whether They had Undergone a Medical Treatment in the Last 6 Months. *Analysed by Unpaired T-Test

tween the responses of the two groups as regards to data security. When the responses of the study group regarding access and protection of electronic health data were studied, it can be seen that the CES expressed more discomfort than the MS about the accessibility of health data by the health personnel other than the physician. Another difference to be noted was that the number of CES who thought that *"E-health records may contain wrong or missing info"* was lower than that of MS. The MS could be considering the issue from a service-based perspective; while the CES could be evaluating the same issue from a technical stand point. Accurate and detailed information is mandatory in order to provide an efficient and timely as well as high-quality healthcare service (1). Undoubtedly patients and their families expect the most effective treatment decisions to be made according to accurate medical data. In this respect, it is vital to ensure that the patients' complete medical records be kept safely and accurately in line with the patients' and their families' expectations (17, 18).

The research also revealed that the CES are more willing to establish e-contact with the physician in case of health problems than the MS. This expected difference can be attributed to the nature of the CES' profession. During the assessment of the questions and statements regarding security violations in the hospitals, it was observed that a majority of CES marked the reasons for this violation as *"faults originating from the personnels' lack of qualification"* and *"carelessness"*; whereas the MS marked the items *"workload"* and *"systemic flaws"*. Due to the fact that healthcare is a multidisciplinary system, which enables access to the electronic system from different terminals, information security and patient privacy expected to be provided by the system have become critical issues throughout the process (19). Meanwhile, electronic data users assume an active role in the system, which also makes their attitudes and approaches to the information security vitally important for the healthcare organizations they work for (13).

Another criterion considered in the study is the personal experiences of the student groups. When the mean scores of the study group were compared according to *"whether they had received any health care service within the last 6 months or not"*, the scores of the CES who have received it were observed to be higher than those who have not for the following statements: *"it is easy for a physician to make a treatment plan with the patient by using information and communication technologies"* and *"the data that I gave to the health center might be shared with other institutions that I would not not be willing to share any data with under different circumstances"*. Similar results were obtained for the statement *"healthcare organisations might allow third parties to access my personal data without my permission"*. On the other hand, the CES who have not received any health care within the last 6 months scored higher on the following statements: *"patients' relatives have information about the right of privacy"* and *"unauthorized persons do not have access to patients' health data"*. Based on these results, it can be suggested that the CES seem to be unaware of the fact that electronic data can be accessed by other health service personnel than the authorized physician because these students did not have in-depth intrinsic knowledge about the ongoing processes regarding healthcare facilities. On the other hand, these students also assumed that technology-based health systems may pose a threat to the security of patient information because they had extensive knowledge about the technical processes which can be applied to healthcare facilities.

On the other hand, when the mean scores of the MS regarding the same points were evaluated, no statistically significant differences were observed between the students who have received any health care within the last 6 months and those who have not.

Developments in communication technologies continuously lead to the development of computer networks in healthcare services, which in turn, enable the users to access a wide range of information about the services and medical technologies provided by hospitals (1). As a convenience provided by these computerized networks, E-health applications provide real-time data, directly affecting the quality of the health care. These applications enable multiple-users to communicate simultaneously and share e-data easily and swiftly (13). As for the urgent demands of the health personnel, the prompts of the physicians can imediately be responded on line and medical errors significantly decreased, thanks to information technologies (20, 21, 22, 23). Moreover, the necessary structural modifications in the ongoing education and training of the medical staff can conveniently be made and updated as frequently as needed.

6. CONCLUSION

To conclude, MS believe that providing healthcare services without using information technologies is not feasible in this age of technology. They also think that too much workload and technical problems may affect information security and patient privacy adversely. Acting on this point, awareness of the staff about the potential technical disruptions and the significance of immediate action during the provision process of healthcare services should be raised. On the other hand, CES assert that information and communication technologies should be widely used while providing healthcare services; however, this practice may lead to doubts about information security and patient privacy due to misuse and access by unauthorized personnel.

Considering that healthcare services can only be provided efficiently with the coordinated efforts of the health personnel and CES who will be part of the system, relevant education and training programs should include all aspects of E-health data and the importance of security and privacy. In this respect, the multi-disciplinary structure of E-health services necessitate that CES are stakeholders of all healthcare services, in which they will actively be taking part in the future. From the perspective of information security and privacy, the vocational education and training of CES and MS should be compounded with subjects including E-health services and their relevant fields. At this point, the prospect physician and computer engineers should be brought together at a common platform, and the required educational programs to manage the synchronization process of the two disciplines should be organized to obtain the best results. Acting on this purpose, the CES should be offered elective courses regarding medical sciences to realize the synchronization process and manage it effectively.

REFERENCES

1. Cortes LP, Cortes GE. Hospital Information Systems: A Study of Electronic Patient Records. Journal of Information Systems and Technology Management. 2011; 8(1): 131-154.
2. Box D, Pottasa D. Improving Information Security Behaviour in the Healthcare Context. Procedia Technology. 2013; 9: 1093-1103.
3. Lee ML. Ethics and Subsequent Use of Electronic Health Record Data. Journal of Biomedical Informatics. 2007; 71: 143-146.
4. Bose R. Knowledge Management-Enabled Health Care Management Systems: Capabilities, İnfrastructure and Decision-Support, Expert Systeam with Applications. 2003; 24(1): 59-71.
5. Mumcu G, Köksal L, Şişman N, Çatar RÖ. The Effectiveness and Outcomes of Computerized Provider Order Entry in Emergency Care Department of Private Hospitals. Journal of Marmara University Institute of Health Sciences. 2013; 3(2): 83-90.
6. Kleinpeter E. Four Ethical Issues of "E-Health", IRBM. 2017; 38: 245-249.
7. Kluge EH. Secure e-Health: Managing Risks to Patient Health Data. International Journal of Medical Informatics. 2007; 76: 402-106.
8. Gebrasilase T,, Lessa FL. Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital. The African Journal of Information Systems. 2011; 3(3): .71-86.
9. Kluge EH. Ethical and Legal Challenges for Health Telematics in a Global World: Telehealth and the Technological Imperative. International Journal of Medical Informatics. 2011; 80: 1-5.
10. Anjum A, Malik RM, Choo R, Khan A, Haroon A, Khan S, Ahmad N, Raza B. An Efficient Privacy Mechanism for Electronic Health Records. Computers & Security. 2018; 72; 196-211.
11. Spike JP. Principles for Public Health Ethics. Ethics, Medicine and Public Health. 2018; 4: 13-20.
12. Woodward Z, Argent P V. Patient Confidentiality. Current Obstetrics and Gynaecology. 2005; 15: 211-214.
13. Kılıç Aksu P, Kitapçı Şişman N, Çatar RÖ, Köksal L, Mumcu G. An Evaluation of Information Security from the Users' Perspective in Turkey. Journal of Health Informatics in Devoloping Countries. 2015; 9(2): 55-67.
14. Masic I, Ridjanovic Z. Health ethics and data protection, AVICENA, Sarajevo, 2001: 128 pp.
15. Senor C, Aleman JL, Toval A. Are Personel Helathcare Records Safe? A Review Free Web-Accessible Personal Health Record Privacy Policies. Journal of Medical Internet Research. 2012; 14(4): 1-14.
16. Appari A, Johnson M E. Information Security and Privacy in Healthcare: Current State of Research. Int. J. Internet and Enterprise Management. 2010; 6(4): .279-314.
17. Croll P.R, Croll J. Investigating Risk Exposure in E-Health Systems. International Journal of Medical Informatics. 2007; 76: 460-465.
18. Safran C, Goldberg H. Electronic Patient Records and Impact of the Internet. International Journal of Medical Informatics. 2000; 60: 77-83.
19. Lekkas D, Gritzalis D. Long-Term Verifiability of Healthcare Records Authenticity. International Journal of Medical Informatics 2007; 76: 442-448.
20. Aldosarı B. An Evaluation of EHR System Audit Functions in a Saudi Arabian Hospital. Journal of Health Informatics in Devoloping Countries. 2012; 6(2: .496-508.
21. 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: .1-4.
22. Mumcu G, Köksal L, Kopmaz B, Gök M, Bulu B, Şişman N, Kılıç Aksu P, Tarım M. The Healthcare Quality and Hospital Information Management System: A Sample from Turkey. Acıbadem Üniversitesi Sağlık Bilimleri Dergisi. 2014; 5(1): 31-37.
23. Anderson JG. Social, Ethical and Legal Barriers to E-Health. International Journal of Medical Informatics. 2007; 76: .480-483.