Sağlık Akademisyenleri Dergisi
www.saglikakademisyenleridergisi.com

Araştırma / Research Article

HIPAA standartları açısından elektronik sağlık kayıtlarının güvenlik ve mahremiyet uygulamaları: Türkiye'de bir vaka çalışması

Security and privacy practices of electronic health records in terms of HIPAA standards: A case study in Turkey

Vedat Mehmet Paksoy

Marmara University, Institute of Health Science, İstanbul

Anahtar Kelimeler:
Sağlık Bilgi Sistemleri, Bilgi Güvenliği, Elektronik Sağlık Kayıtları, Mahremiyet, HIPAA

Key Words:
Health Information Systems, Information Security, Electronic Health Records, Privacy, HIPAA

Yazışma Adresi/Address for correspondence:
Vedat Mehmet Paksoy,
Marmara University, Institute of Health Science, PhD Student
vedatpaksoy@gmail.com

Gönderme Tarihi/Received Date:
29.12.2018

Kabul Tarihi/Accepted Date:
11.01.2019

Yayımlanma Tarihi/Published Online:
31.03.2019

ÖZET

Bu araştırmada; genel ve dal olmak üzere özel hastanelerde elektronik sağlık kayıtlarının (ESK) güvenlik ve mahremiyetinin HIPAA ilkeleri kapsamında değerlendirilmesi amaçlanmıştır. Araştırma Kayseri ilinde bulunan genel ve dal hastanesi olmak üzere altı özel hastanenin çalışanlarını kapsamaktadır. Elektronik sağlık kayıt sistemini kullanan idari ve sağlık çalışanı olmak üzere 447 kişiye, yüzyüze görüşme yöntemi ile anket uygulanmıştır. Ölçekteki maddeler 5'li Likert ölçeği (1: kesinlikle katılmıyorum - 5: kesinlikle katılıyorum) ile değerlendirilmiştir. Faktör analizi sonucunda elektronik sağlık kayıtlarının güvenlik ve mahremiyeti ile ilişkili üç alt grup tanımlanmıştır.

Elektronik sağlık kayıtlarının güvenlik ve mahremiyeti puanının genel hastanelerde (78,54±23,5), dal hastanelerine (68,49±26,8) göre yüksek olduğu saptanmıştır (p=0.002). Ayrıca ESK kullanım becerisinin idari birim çalışanlarında (75,99±22,5), tıbbi birim çalışanlarına (70,93±25,7) göre yüksek olduğu belirlenmiştir (p=0.037). Genel hastanelerde görev yapan personelin %69,8'inin (n=264) ESK eğitimi aldığı, dal hastanelerin ise % 34,8'inin (n=24) ESK eğitimi aldığı belirlenmiştir (p=0,000). Yaş ortalamasının yüksek olduğu gruplarda ve ESK eğitimi alan bireylerin almayanlara göre alt boyut puanlarının yüksek olduğu saptanmıştır. Ayrıca; kadın çalışanların (3,91±0,68), erkek çalışanlara (3,76±0,80) göre "Örgütsel Güvenlik" boyutu ortalama puanının anlamlı bir şekilde daha yüksek olduğu tespit edilmiştir (p=0,042). Çalışanlar ve yöneticiler arasında tüm alt boyutlarda anlamlı bir farklılık tespit edilmemiştir (P>0.05).

Sağlık kurumlarında, elektronik sağlık kayıtlarının güvenlik ve mahremiyetinin HIPAA standartlarını tam olarak karşılamadığı görülmektedir. Genel hastanelerin, dal hastanelerine göre ESK'nın güvenlik ve mahremiyeti konusunda daha başarılı uygulamaları olduğu söylenebilir. Ayrıca idari birim çalışanlarının tıbbi birim çalışanlarına göre, belirlenen politikalara uyum ve uygulama düzeylerinin daha yüksek olduğu belirlenmiştir. Bununla birlikte; güvenlik önlemlerinde insan faktörü ve eğitim uygulamalarının oldukça önem arz ettiği sonucuna varılabilir.

ABSTRACT

In this study; It is aimed to evaluate the safety and privacy of electronic health records (EHR) with HIPAA rules in general and branch special hospitals. Six private hospitals participated the research in the province of Kayseri, Turkey. A questionnaire was applied to 447 people, including administrative and health practitioners using the electronic health record system, using a face-to-face interview method. The items in the scale were evaluated with a 5-point Likert scale (1: strongly disagree - 5: strongly agree). As a result of factor analysis, three subgroups related to EHR security and privacy are defined.

Security and privacy scores of electronic health records were higher in general hospitals (78,54±23,5) compare to branch hospitals (68,49±26,8) (p=0.002). Moreover, it is seen that electronic health record use ability is higher in administrative units (75,99±22,5), compare to medical units (70,93±25,7) (p=0.033). it was determined that 69.8% (n = 264) of the staff working in general hospitals were trained and 34.8% (n = 24) of branch hospitals were trained (p=0.000). It is seen that the subscale scores are high in the individuals who are trained and in the groups who have higher age averages. Moreover, it was found that the average score of "Organizational Security" sub-dimension of female employees (3,91±0,68) was significantly higher than male employees (3,76±0,80) (p=0.042). There were no significant differences in all sub-dimensions that the security and privacy of electronic health records between the managers and other employees (p> 0.05).

It is seen that healthcare institutions do not completely comply with HIPAA rules. General hospitals are more successful than branch hospitals in terms of security and privacy of electronic health records. Moreover, the level of consciousness of the administrative unit employees is higher than medical unit employees. Human factors and educational practices are very important in security measures.

INTRODUCTION

The Electronic Health Record (EHR) is a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting. Patient demographics, progress notes, problems, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports are types of information included (www.himss.org). It also serves as a patient data source digitally and securely stored, and accessed by multiple authorized users (Kohli and Swee-Lin Tan, 2016). Preventive measures, treatment of acute illnesses and life-long health services in chronic diseases are presented effectively within EHR **(Hartley and Jones, 2012).** It is useful in terms of time and cost by preventing repetition of diagnosis and treatment methods (Aldosari, 2017).

In addition to the benefits of electronic health records, breaching into the computer systems should be closely monitored. In this respect, the safety and privacy of electronic health records are considered as an important issue in health care services. Ethical and legal problems such as unauthorized recording, loss and theft of health data, lack of information and approval unauthorized sharing of health data, software-based threats and cyber attacks may arise (Shahmoradi et all., 2017).

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 mandates that the privacy, security and electronic transaction standards for maintaining the patient information for all healthcare providers. HIPAA safeguards the privacy of medical records of patients by preventing unauthorized disclosure and improper use of patients' Protected Health Information (PHI). Security and privacy standards have been established to ensure the integrity, privacy and accessibility of personal information. The security standards require compliance actions in the five categories: Administrative safeguards, Physical safeguards, Technical safeguards, Organizational requirement, Policies, procedures and documentation requirements (Mishra et all., 2011).

Along with the implementation of health transformation programme in Turkey, private hospitals become an important part of the system in the country. General and branch private hospitals providing patient care with specialized staff and equipment spread all over the country (Aksu Kılıç et all., 2015) The aim of this study was to evaluate security and privacy of electronic health records in terms of HIPAA principles in general and branch private hospitals within the framework of the users' perspective.

MATERIALS AND METHODS

In this study, 447 medical and administrative staffs who are using electronic health record system from 6 private hospitals were included. The study was carried out between 01 June 2017 - 30 July 2017. A constructed questionnaire was applied with a face-to-face interview method. The questionnaire includes socio-demographic characteristics, questions about electronic health record experience, and a scale about the security and privacy of electronic health records. The self-reported "ability to use of EHR" and "security and privacy of the system" were evaluated by 100-mm visual analogue scale (0: very poor vs 100: very good). The scale developed by Mishra et al. Upon getting ethical permission the use of the scale was communicated to the developers by e-mail. The scale adaptation process was implemented to cross-cultural adaptation (Lukaschyk et all., 2016; Bohu et all., 2014). 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 designed with 10 employees to evaluate their comprehension of the questionnaire form. The questionnaire were revised and the final version of the questionnaire was obtained. 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.

STATISTICAL ANALYSIS

Construct validity was evaluated by explanatory factor analysis. Kaiser-Meyer-Olkin (KMO) was assessed to determine the sampling adequacy (0,917). Accordingly, the sample size for factor analysis was satisfied. Barlett's Test of Sphericity was performed to determine the sample test size (p= 0.000). The results show that data are sufficient for factor analysis (Vignola and Tucci, 2013). Principal Component Analysis and Varimax Rotation method were used in the analysis of factor structure. As a result of analysis; multiple items have been identified in more than one factor. For this reason, factor analysis was repeated three times with the items removed from the scale. The principal component analysis produced three distinct factors with eigen values of >1, thereby explaining 56,93% of the variance. The subscales were security and privacy policy, organisational security, education and security applications.

Internal consistency reliability was investigated using Cronbach's alpha and a value of 0.70 or above indicates good reliability (Cronbach, 1951). The estimated Cronbach's alpha was 0.920 in the overall sample. The Cronbach's alpha values for each factors were 0.879, 0.871 and 0.804. An unpaired T test was used in the comparison of scores whereas Mann-Whitney U test was used in non-normal distribution of data. In addition, the categorical subscale scores (gender, age, education level) were compared with the One-Way

Table 1. The Distribution of Items of Security and Privacy Applications of Electronic Health Records Questionnaire According to Factor Analysis

No	Items	Factors		
		Security and Privacy Policy	Organisational Security	Education and Security Applications
22	Security policies and procedures are easily accessible and comprehendible in my organization.	0,710		
16	In my organization, there is a predefined agreed upon plan for security and privacy compliance efforts.	0,705		
20	In my organization, there are adequate internal controls (policies, procedures, training, encryption, access restrictions) to provide security and privacy of health records.	0,698		
18	Creating security awareness is an ongoing process in my organization.	0,686		
19	There is visible leadership about seriousness of security assurance efforts in my organization.	0,667		
21	Auditing is viewed as a necessary complimentary action to improve the security initiatives in my organization.	0,667		
17	There is a prevalent security culture where individuals look out for each other in my organization	0,659		
23	In my organization, there is an emphasis on establishing open communication channels about security issues without the fear of reprisal.	0,600		
38	I am aware of the password policy that I have to comply with, in my organization		0,826	
37	I am required to report any misuse of information (that I am in-charge of) or its inappropriate access		0,806	
32	In my organization, I understand what information I have access to and why?		0,739	
33	I am required to access health information only through approved devices and software in the organization.		0,643	
36	I am aware of the procedure about what to do when my system has malware in my organization		0,634	
39	I frequently receive communication about acceptable security behavior in my organization		0,596	
40	In my organization, there is an ongoing effort on training and education of employees about security issues.			0,723
27	Training about security measures is provided regularly to the staff/personnel in my organization			0,717
30	I am required to read the security policies frequently (Quarterly, bi-anually, annually) in my organization			0,710
31	In my organization, I have frequent communication about social engineering issues and am aware of how such tactics can create vulnerability for our system.			0,671
28	In my organization, security policies and procedures are periodically reviewed to assess if the policies meet the changing organizational needs			0,622
34	I am allowed to use removable storage media from outside on my machine in the organization.			0,454
	Variance (%)	21,669	18,035	17,226
	Croncbach's Alpha Values	0,879	0,871	0,804

ANOVA test. Kruskal Wallis test was used in non-normal distribution of data. Dr. Pınar KILIÇ AKSU provided support during the construction of the analyzes. SPSS v25 statistical program was used in the analysis of the study.

RESULTS

In this study, 68.3% (n=185) of the medical staff and 58.5% (n=103) of the administrative staff were women. 65,4% (n=151) of the medical staff and 34,6% (n=80) of the administrative staff are between 18-28 years of age. 37,6% (n=102) of the medical staff and 39,2% (n=69) of the administrative staff graduated from Bachelor's Degree/ Master's Degree programs (Table 2).

It was found that the general hospitals had significantly higher overall compared to the branch hospitals in terms of ***"work experience"*** (p=0.000), ***"period of employment within the organisation"*** (p=0.000), ***"experience using of EHR"*** (p=0.022), ***"ability of using computer"*** (p=0.000) and ***"ability using of EHR"*** (p=0.024). In addition, The self-reported scores of the general hospital (78,54±23,5) with regard to ***"Securtiy and Privacy of EHR in the Organization"*** were significantly higher compared to those of the branch hospital (68,49±26,8) (p= 0.002) (Table 3.)

"Experience Using of EHR" of administrative staff (69,41±48,20) is longer than that of medical staff (59,12±46,33) (p = 0.044). Additionally, "***Ability of***

Table 2. Socio-Demographic Characteristics of Medical and Administrative Staffs

		Medical Staff (n= 271)		Administrative Staff (n=176)		Total	
		n	%	n	%	n	%
Gender	Male	86	31,7	73	41,5	159	35,6
	Female	185	68,3	103	58,5	288	64,4
Age	18 - 28 years	151	65,4	80	34,6	231	51,7
	29 - 39 years	92	54,4	77	45,6	169	37,8
	40 - 50 years	23	62,2	14	37,8	37	8,3
	51 - 61 years	2	28,6	5	71,4	7	1,6
	62 years >	3	100	0	0	3	0,7
Education Level	High School	98	36,2	72	40,9	170	38
	Associate's Degree	71	26,2	35	19.9	106	23,7
	Bachelor's Degree/Master's Degree	102	37,6	69	39,2	171	38,3

Table 3. Working Conditions of General and Branch Hospitals and Electronic Health Record Usage

	General Hospital			Branch Hospital			
	n	Mean	Standart Deviation	n	Mean	Standart Deviation	p*
Work Experience (month)	368	94,56	83,61	68	59,16	53,31	0.000
Period of Employment Within The Organisation (month)	376	63,73	54,23	68	37,78	34,49	0.000
Experience Using of EHR (month)	303	65,24	46,48	52	51,75	50,73	0.022
Training to about EHR	223	14,74	25,01	14	15,43	24,25	0.575
Ability of Using Computer (0-100 point)	378	78,80	20,31	69	68,12	21,28	0.000
Ability of Using EHR (0-100 point)	378	74,20	23,80	69	65,94	27,73	0.024
Securtiy and Privacy of EHR in the Organization (0-100 point)**	378	78,54	23,53	69	68,49	26,81	0.002

* Mann-Whitney U test was used
** 0 point = Very Poor - 100 point = Very Good

Using EHR" of administrative staff (75,99±22,5) is longer than that of medical staff (70,93±25,72)) (p = 0.033). There were no significant differences between groups with regard to ***"work experience"***, ***"period of employment within the organisation"***, ***"ability of using computer"***, ***"ability using of EHR"***, ***"Securtiy and Privacy of EHR in the Organization"*** (p > 0.05) (Table 4).

When examining the status of receiving "***training use of electronic health records"***; it was determined that 69.8% (n = 264) of the staff in general hospitals and 34.8% (n = 24) of the staff in branch hospitals were trained (p = 0.000).

The mean score of **"Organizational Security"** sub-dimension was significantly higher in general hospitals (3,89 ± 0,74) than that of branch hospitals (3,69 ± 0,64) (p = 0.042). The **"Education and Security Practices"** sub-dimension (3,47 ± 0,76) is significantly higher than the branch hospitals (2,99 ± 1,96) (p = 0.000). No significant difference was found in the **"Security and Privacy Policies"** sub-dimension (p> 0,05).

The mean score of **"Organizational Security"** sub-dimension was found significantly higher in general hospitals (3,89 ± 0,74) than that of branch hospitals (3,69 ± 0,64) (p = 0.042). Similarly, The mean score of **"Education and Safety Practices"** sub-dimension is significantly higher in general hospitals (3,47 ± 0,76) than that of branch hospitals (2,99 ± 1,96) (p = 0.000). There is no significant difference in **"Security and Privacy Policies"** sub-dimension (p>0.05) (Table 5).

Table 4. Working Conditions of Medical and Administrative Staff and Electronic Health Record Usage

	Medical Staff			Administrative Staff			
	n	Mean	Standart Deviation	n	Mean	Standart Deviation	p*
Work Experience (month)	267	88,79	85,38	169	89,43	72,72	0.936
Period of Employment Within The Organisation (month)	271	56,54	49,72	173	64,81	56,36	0.105
Experience Using of EHR (month)	212	59,12	46,33	143	69,41	48,20	0.044
Training to about EHR	137	11,45	18,64	100	19,35	31,08	0.158
Ability of Using Computer (0-100 point)	271	75,77	21,32	176	79,27	19,85	0.083
Ability of Using EHR (0-100 point)	271	70,93	25,72	176	75,99	22,50	0.033
Securtiy and Privacy of EHR in the Organization (0-100 point)**	271	75,26	25,76	176	79,66	21,67	0.062

* Independent-Samples T test was used
** Mann-Whitney U test was used
*** 0 point = Very Poor - 100 point = Very Good

Table 5. The Relationship Between The Security and Privacy of Electronic Health Records Sub-Dimensions and General-Branch Hospitals, Medical-Administrative Staff, Manager-Staff

		Security and Privacy Policy	Organisational Security	Education and Security Applications
Genaral Hospital (n=378)	Mean	3,65	3,89	3,47
	Standart Deviation	0,77	0,74	0,76
Branch Hospital (n=69)	Mean	3,52	3,69	2,99
	Standart Deviation	0,66	0,64	0,89
	p*	0.190	0.042	0.000
Medical Staff (n=271)	Mean	3,56	3,82	3,34
	Standart Deviation	0,77	0,75	0,79
Administrative Staff (n=176)	Mean	3,75	3,92	3,49
	Standart Deviation	0,72	0,70	0,82
	p*	0.009	0.147	0.050
Manager (n=31)	Mean	3,70	3,69	3,39
	Standart Deviation	0,66	0,69	0,78
Staff (n=431)	Mean	3,63	3,87	3,40
	Standart Deviation	0,77	0,73	0,81
	p*	0.859	0.182	0.960

* Independent-Samples T test was used
Likert Scale 1-5 (1: Strongly Disagree - 5: Strongly Agree)

When sub-dimensions are evaluated in terms of medical and administrative staff, the mean score of **"Security and Privacy Policies"** sub-dimension was significantly higher in administrative units (3.75 ± 0.72) than that of medical staff (3.56 ± 0.77) (p = 0.009). The average score of **"Education and Safety Practices"** is significantly higher in administrative staff (3,49 ± 0,82) than that of medical staff (3,34 ± 0,79) (p= 0.050). There is no significant difference in organizational security dimension (p> 0.05) (Table 5).

There were no significant differences in all sub-dimensions that the security and privacy of electronic health records between the managers and other employees (p> 0.05) (Table 5).

When the relationship between sub-dimensions

Table 6. The Relationship Between The Security and Privacy of Electronic Health Records Sub-Dimensions and Training to About EHR

Training to About EHR		Security and Privacy Policy	Organisational Security	Education and Security Applications
Training (+) (n=288)	Mean	3,69	3,94	3,51
	Standart Deviation	0,79	0,72	0,81
Training (-) (n=138)	Mean	3,50	3,68	3,14
	Standart Deviation	0,69	0,75	0,77
	p*	0.018	0.000	0.000

* Independent-Samples T test was used.
Likert Scale 1-5 (1: Strongly Disagree - 5: Strongly Agree)

that the security and privacy of electronic health records and the age of the research group is evaluated; significant differences were identified in the sub-dimensions of **"Security and Privacy Policies"** (p=0.016), **"Organizational Security"** (p=0.050) and **"Education and Safety Practices"** (p=0.010). This difference was between 18-28 years and 40-50 years in all sub-dimensions.

Furthermore, it was found that the average score of **"Organizational Security"** sub-dimension of female employees (3.91 ± 0.68) was significantly higher than male employees (3.76 ± 0.80) (p=0.042). When evaluated in terms of education levels, there was no significant difference (p>0.05).

It was determined that the mean of the educated individuals in all sub-dimensions was significantly higher. **"Security and Privacy Policies"** (p=0.018), **"Organizational Security"** (p=0.000) and **"Education and Safety Practices"** (p=0.000) (Table 6).

DISCUSSION

It is stated that the health information systems are more likely to be exposed to the threat such as viruses compared to traditional IT departments (Forcepoint, 2015). Therefore, the necessary applications for the safety and privacy of electronic health records should be considered as a whole. (Pham, 2016). HIPAA standards which contain multiple factors offer highly effective solutions and sanctions to ensure the safety and privacy of digital data (Liginlal et al., 2012). For his reason, in this study, the safety and privacy of electronic health records in Turkey is evaluated within the scope of HIPAA standards.

It is seen that the "score of the safety and confidentiality of the institution's electronic health records" in general hospitals was higher than the branch hospitals. More effective involvement of IT departments in general hospitals and staff training are an important factor. Software companies may not offer software to suit the needs of branch hospitals. Additionally, the preferred technology may not be appropriate for the organizational structure (Çınaroğlu and Avcı, 2015).

According to the study, administrative staff have higher point of electronic health record skill. Because administrative staff use information technologies more intensively. Medical staff give priority to the health services. The resistance may develop against the information system by the medical staff due to some reasons such as loss of time, lack of computer usage, increased workload and problems of trust in the system. In this respect, the softwares must support the needs of the medical staff (Ajami and Bagari-Tadi, 2013).

It was determined that 69.8% (n = 264) of staffs in the general hospitals were trained and 34.8% (n = 24) of the branch hospitals were trained. Training practices are very important in order to benefit from the opportunities provided by electronic health records and to ensure data security (McGinn et al., 2011). In this context, HIPAA standards are given importance to the training of employees as administrative measures (www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index).

It is seen that the average of "Organizational Communication" and "Education and Security Policies" dimensions are higher in general hospitals compared to in branch hospitals. There is no difference in determining strategies among institutions, but there are deficiencies in branch hospitals in the implementation phase. In a study, it was determined that there was an adaptation problem in the use of electronic health records in small health enterprises. (Simon et al., 2007). The reason for this is the lack of financial capacity for the establishment of the system and the incompatibility of the system and work flows. In addition, the lack of financial resources and the lack of IT expert in the staff of the small capacity health institutions is defined as the obstacle to compliance with HIPAA standards (Chen and Benusa, 2017).

The average of the "Security and Privacy Strategies" and "Education and Security Policies" dimensions were

higher in the administrative units compared to the medical units. The medical staffs consider their priority as health care. Other applications are seen as extra workload. For this reason, less importance is given to the safety of the electronic health record system. Similarly, in a study on data privacy confidentiality, it was determined that health workers give higher priority to their professional responsibilities and do not give enough importance to data privacy (Lapke and at al., 2016).

It is observed that the sub-dimension scores are better in the groups with high average age. In the studies conducted, it is seen that the adaptation of the young health workers to the use of electronic health record is better (Singh, 2016). Further, it is determined that the individuals who are educated about the use of electronic health records have higher averages in all dimensions.

CONCLUSION

The existence of information and communication technologies in compliance with international standards is important for ensuring the security and privacy of electronic health records in health institutions. In the process of establishment of health technology systems, technical personnel should be present in the field. The impact of employees on processes should not be ignored as much as the existence of a secure system. For the privacy of electronic health records, employees should be trained about system use and safety awareness, and must be repeated periodically.

Today, patients are aware of digital data security and are concerned about this issue. Therefore, institutions must meet the expectations of patients. The determination of strategies and policies at international standards is also important in terms of corporate image and competitive advantage. In the process of ensuring data security, the differences between general-branch hospitals and medical-administrative unit should be considered.

REFERENCES

1. Ajami S, Bagheri-Tadi T. Barriers for Adopting Electronic Health Records (EHRs) by Physicians, Acta Informatica Medica, 2013, 21(2): 129-134
2. Aksu Kılıç P, Kitapçı Şişman N, Çatar R. Ö, 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
3. Aldosari B. Causes of EHR Projects Stalling or Failing: A Study of EHR Projects in Saudi Arabia, Computers in Biology and Medicine, 2017, 91: 372-381.
4. Bohu Y, Klouche S, Lefevre N, Webster K, Herman S. Translation, Cross-Cultural Adaptation and Validation of the French Version of The Anterior Cruciate Ligament-Return to Sport After Injury Scale, Knee Surg. Sports Traumatol Arthrosc., 2015, 23: 1192-1196.
5. Chen Q, Benusa A. HIPAA Security Compliance Challenges: The Case for Small Healthcare Providers, International Journal of Healthcare Management, 2017, 10 (2): 135-146
6. Cronbach L. Coefficient Alpha and The Internal Structure of Test, Psychometrika, 1951, 16(3): 297-334.
7. Çınaroğlu S, Avcı K. Comparison of Asessments of Medical and Surgical Nurses About Usage of Electronic Health Records, TAF Preventive Medicine Bulletin, 2015, 14 (3): 257-264.
8. Forcepoint, Industry Drill-Down Report Healthcare, 2015. www.insight.com/content/dam/insight-web/en_US/article-images/ebooks/Partner/2015-industry-drill-down-report-healthcare.pdf
9. Hartley C, Jones E. EHR Implementation: A Step-by-Step Guide for the Medical Practice, American Medical Association, 2th Edition, Chicago, 2012.
10. Kohli R, Tan S. Electronıc Health Records: How Can Is Researchers Contrıbute To Transformıng Healthcare?, MIS Quarterly, 2016, 40(3): 553-573.
11. Lapke M, Garcia C, Henderson D. The Disconnect Between Healthcare Provider Tasks and Privacy Requirements, Health Policy and Technology, 2016, 1-8.
12. Mishra S, Leone G, Caputo D, Calabrisi R. Securıty Awareness For Health Care Informatıon Systems: A HIPAA Compliance Perspective, Issues in Information Systems, 2011, 12(1):224-236.
13. Liginlal D, Sim I, Khansa L, Fearn P. HIPAA Privacy Rule Compliance: An Interpretive Study Using Norman's Action Theory, Computers & Security, 2012, 31: 206-220.
14. Lukaschyk J, Brockmann-Bauser M, Beushausen U, Transcultural Adaptation and Validation of the German Version of the Vocal Tract Discomfort Scale, Journal of Voice, 2017, 31 (2): 261-268.
15. Pham T. The Current State of Healthcare Endpoint Security, Industry News, 2016.
16. Shahmoradi L, Darrudi A, Arji G, Nejad A. Electronic Health Record Implementation: A SWOT Analysis, Acta Medica Iranica, 2017, 55 (10): 642-649.
17. Simon S, Kaushal R, Cleary P, Jenter C, Volk L, Poon E, Orav J, Lo H, Willıams D, Bates D,. Correlates of Electronic Health Record Adoption in Office Practices: A Statewide Survey, Journal of the American Medical Informatics Association, 2007, 14 (1): 110-117.
18. Singh B. Nurse's Attitude Towards Computerization in Private Hospitals of Tamil Nadu, India, Research J. Pharm. and Tech., 2016, 9 (12): 1451-1456.
19. Vignola R, Tucci A. Adaptation And Validation of The Depression, Anxiety and Stress Scale to Brazilian Portuguese, Journal of Affective Disorders, 2014, 155: 104-109.