RESEARCH ARTICLE

THE EVALUATION OF THE EFFECT OF THE INFORMATION SECURITY AWARENESS LEVEL IN MEDICAL SECRETARIES ON THE SECURITY AND PRIVACY IMPLEMENTATIONS OF ELECTRONIC HEALTH RECORDS

Tülin FİLİK [*]
Demet ÜNALAN [**]

ABSTRACT

In this research, it is objected to "Evaluate the effect of the awareness level of information security in the medical secretaries on the security and privacy applications of electronic health records." The population of the research includes 258 medical secretaries working at Erciyes University, Health Research and Implementation Center. The study was conducted on 210 (80.7%) medical secretaries accepting to participate in the research voluntarily. The data in the research were collected using a questionnaire form for determining the descriptive characteristics of the medical secretaries together with "Information Security Awareness Scale (ISAS)" and "The Adjustment Scale of Electronic Health Records Security and Privacy Standards." In the presentation of the descriptive characteristics of the obtained results, mean, standard deviation, median, minimum and maximum values were indicated as well as number and percentage distributions. In intergroup comparisons, independent two samples t test and one-way analysis of variance were performed for quantitative variables. In multivariate analysis, structural equation modeling analysis was performed in order to confirm the relationship between ISAS and The Adjustment Scale of Electronic Health Records Security and Privacy Standards on a model. A positive and high level of statistically significant relation was found between the ISAS sub-scale scores and The Adjustment of Electronic Health Records Security and Privacy Standards sub-scale scores of the medical secretaries (p<0.01). In the structural equation modeling analysis performed in order to confirm the relationship between ISAS and The Adjustment Scale of Electronic Health Records Security and Privacy Standards on a model, it was revealed that the relationship between the two structures has a great and significant coefficient.

Keywords: *Medical Secretary, Information Security, Electronic Medical Records, Privacy*

ARTICLE INFO

[*] *Science Specialist, PhD Student, Kayseri University, Department of Healthcare Management, tulinfilik@hotmail.com*
https://orcid.org/0000-0003-3264-8226

[**] *Prof. Dr, Erciyes University, Halil Bayraktar Vocational Health College, Department of Medical Services and Techniques, unalandemet@gmail.com*
https://orcid.org/0000-0001-9854-437x

Recieved: 12.11.2020
Accepted: 16.02.2021

Cite This Paper:

Filik, T. & Ünalan, D. (2021). The Evaluation of The Effect of The Information Security Awareness Level in Medical Secretaries on The Security and Privacy Implementations of Electronic Health Records. Hacettepe Sağlık İdaresi Dergisi, 24(1), 183-202

ARAŞTIRMA MAKALESİ

TIBBİ SEKRETERLERDE BİLGİ GÜVENLİĞİ FARKINDALIK DÜZEYİNİN ELEKTRONİK SAĞLIK KAYITLARININ GÜVENLİK VE MAHREMİYET UYGULAMALARINA ETKİSİNİN DEĞERLENDİRİLMESİ

Tülin FİLİK [*]
Demet ÜNALAN [**]

ÖZ

Bu araştırmada, "Tıbbi sekreterlerde bilgi güvenliği farkındalık düzeyinin elektronik sağlık kayıtlarının güvenlik ve mahremiyet uygulamalarına etkisin değerlendirilmesi" amaçlanmıştır. Araştırmanın evrenini; Erciyes Üniversitesi Sağlık Uygulama ve Araştırma Merkezinde çalışan, 258 tıbbi sekreter oluşturmuştur. Araştırmaya katılmayı gönüllü olarak kabul eden 210 (%80.7) tıbbi sekreter ile çalışma gerçekleştirilmiştir. Araştırmada veriler tıbbi sekreterlerin tanımlayıcı özelliklerini belirlemeye yönelik anket formu ile "Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ)" ve "Elektronik Sağlık Kayıtları Güvenlik ve Mahremiyet Standartlarına Uyum Ölçeği" ile toplanmıştır. Elde edilen bulguların tanımlayıcı özellikleri sunumunda sayı ve yüzde dağılımları yanı sıra ortalama, standart sapma, ortanca, en küçük ve büyük değerler gösterilmiştir. Gruplar arası karşılaştırmalarda nicel değişkenler için bağımsız iki örneklem t testi ve tek yönlü varyans analizi uygulanmıştır. Çok değişkenli analizde BGFÖ ile Elektronik Sağlık Kayıtları Güvenlik Mahremiyeti Standartlarına Uyum ölçeği arasındaki ilişkinin bir model üzerinde doğrulanması amacıyla yapısal eşitlik modellemesi analizi yapılmıştır. Tıbbi Sekreterlerin BGFÖ alt boyut puanları ve Elektronik Sağlık Kayıtları Güvenlik Mahremiyeti Standartlarına Uyum ölçeği alt boyut puanları arasındaki arasında pozitif yönde orta ve yüksek düzeyde istatistiksel açıdan anlamlı ilişki bulunmuştur ($p<0.01$). BGFÖ ile Elektronik Sağlık Kayıtları Güvenlik Mahremiyeti Standartlarına Uyum ölçeği arasındaki ilişkinin bir model üzerinde doğrulanması amacıyla oluşturulan yapısal eşitlik modellemesi analizinde iki yapı arasındaki ilişkinin büyük ve anlamlı katsayıya sahip olduğu ortaya konulmuştur.

Anahtar Kelimeler: *Tıbbi Sekreter, Bilgi Güvenliği, Elektronik Sağlık Kayıtları, Mahremiyet*

MAKALE HAKKINDA

[*] *Dr. Öğrencisi, Kayseri Üniversitesi, tulinfilik@hotmail.com*
https://orcid.org/0000-0003-3264-8226

[**] *Prof. Dr., Erciyes Üniversitesi, unalandemet@gmail.com*
https://orcid.org/0000-0001-9854-437x

Gönderim Tarihi: 12.11.2020
Kabul Tarihi: 16.02.2021

Atıfta Bulunmak İçin::

Filik, T. & Ünalan, D. (2021). The Evaluation of The Effect of The Information Security Awareness Level in Medical Secretaries on The Security and Privacy Implementations of Electronic Health Records. Hacettepe Sağlık İdaresi Dergisi, 24(1), 183-202

I. INTRODUCTION

In order to increase the efficiency of an institution, it is aimed to accelerate the business processes, enhance the quality and facilitate the audit by using information technologies. The fact that information technology is used in every field and it has become indispensable, it has started to be used in many institutions and information is the most important competitive element has made it necessary to protect the produced information (Yılmaz, 2014).

Health care institutions of today having advanced technology aim at improving the quality of serving healthcare by using the advantages of the information and communication technologies. Information security is defined as the measures taken to protect information from misuse, access, disclosure, destruction, change of content or damage. Information security, playing an important role to provide the sustainability of organizations, ensures the important information of businesses in various environments, especially electronic records to be protected (Baykara et.al., 2013).

Electronic health record (EHR) can be defined as recording and storing the service records of those receiving healthcare services and any kind of administrative and medical data by using electronic systems, and as any kind of information transmitted, accessed, contacted and processed. EHR includes private and valuable information of people. In addition, it supports the work-flow of the healthcare professionals working at healthcare service delivery and reports the analysis of these records (Işık et.al., 2013). EHR system is a structuring providing data processing by ensuring data integrity and security.

II. BASIC CONCEPTS RELATED TO INFORMATION

2.1. The Concept of Information and Its Importance

Information, which has been thought hard by philosophers for centuries, is a concept that cannot be defined overall. Turkish Language Society defines information as "a whole of facts and principles that human mind is able to understand, information, knowledge. The fact, knowledge and experience obtained by learning, search or observation. Thoughts, knowledge and experience emerged by working of human intelligence. Basic thoughts that mind comprehend generally and at first feeling. The meaning that one attributes to the data by using rules."

In this century, information is evaluated as one of the most important factors of production. Thus, the most important property for institutions is the information they have. Institutional information refers to any kind of explicit and implicit information of an institution that is specific to the institution, based on written or oral experiences formed over the years or that the institution obtained from outside (Odabaş, 2003).

Information is a message including meaning in related issues. The objective of information is to help in making decisions and solving problems or when there is an opportunity. Information comes both from present (communication) and past (processed data or restructured description) sources. Thus, information is a concept formed in human mind as a result of the gathering together and evaluation of the experiences and information that an individual obtains during the interaction of his/her environment (Liew, 2013).

The purpose of information security is to ensure to protect the privacy of personal information by carrying out the infrastructure that will protect information integrity and provide its accessibility, and to improve the institutional reputation by protecting the confidentiality of customer and staff information. Information property's loss, damage, being stolen, being in danger and the interruption of institutions' activities is prevented by implementing security controls for the activities of information processing. Due to the conveniences and opportunities that information technologies provide, using information technologies has become an obligation for many organizations to perform their activities.

As the dependency on information technologies increases, the sensitivity for the measurements to be taken against security risks that can occur in these technologies also increases (Acılar, 2009).

2.2 Information Management

Information management is a process necessary for the businesses to increase and maintain their competitive capacities against existing and potential competitors of national and international economies. With this point of view, information management can be stated as the strategies or processes aiming at defining, obtaining and using information efficiently (Aras, 2018).

The outputs of the information in the institutions that realize information management are new products and applications, new technologies, systems, structures, operations, processes, relationships, contacts, services, markets and new information. Information is productive, and outputs obtained support the existence and the future of institutions (Alkan, 2003).

2.2.1. Information Security Management System

Even if one of the safety principles is violated or suffered, security is endangered. The main purpose of information security is to preserve information properties, to be accessible by authorized people or institutions and to protect privacy and confidentiality in order to ensure the continuity of the system (Baran, 2019).

With the establishment of information security management system, it is performed to apply a series of audit functions, to form processes in order facilities, environment and tools in which information is processed to be operated and managed relevantly and safely, to define responsibilities, to develop appropriate methods and to carry on security controls against malicious codes and applications in order to protect the integrity of the software and information; thus interruption of institutions' activities is prevented (Vural and Sağıroğlu, 2008).

2.2.2. National and International Standards in Information Security Management System

There are important concerns related to confidentiality and security due to the sensitivity of the healthcare data. It is required to be very careful to protect the health data and privacy of the patients. Concerns restrict healthcare service providers for accessing individual insurance data that can improve healthcare receivers' experiences related to their health and individualize the service and care they receive. The data is quite defenseless against attacks since most healthcare services have centralized. Security systems promising absolute control on the data that means that personal information cannot be sold or shared without express consent of consumers are needed. There are two policies and arrangement models in different countries in order to protect the data in healthcare services. Based on the basic confidentiality codes, among these, there is HIPAA in the USA, The Regulation of Health Information Privacy 2002 in Australia and Medical Confidentiality Code and Health Insurance Code. The other model is to accept personal health information as a part of personal information or sensitive information. Governments make law such as Data Protection Law in England and the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada (Hong, 2018).

In our country, some institutions have been imposed obligation to conform with the information security standard or to get certificate of conformity and some institutions have been imposed obligation to conform with the standard without getting the certificate of conformity with 27730 numbered “Notification of TS ISO/IEC 27001 Standard Operating within the Scope of Electronic Communication Security” related to information security management (Official Gazette, 2010).

Information security management system operated in health care institutions is at great importance for information security risk management. ISO 27001 information security management used for this purpose should be evaluated in the manner of including all processes in hospitals (Tavakoli et al., 2014).

The top international standard of Information Security Management System is ISO 27001 Information Security Management System standard.

Health information systems are created, protected and kept by using computer technology. The use of this technology creates new problems in protecting patients. Patients require health care organizations to develop comprehensive privacy and security programs. Health Insurance Portability and Accountability Act (HIPAA) Security Rule issued in 2003 highlights the need and importance of information and comprehensive security programs in protecting health (Wager et al., 2009).

Those participating in healthcare service delivery, accident and health insurance companies, companies delivering, selling and leasing medical stuff and service plans and other related organizations have to fulfill HIPAA standards obligations. The main purpose of HIPAA standards is to discourage institutions from open access applications to health records because health record histories of individuals may include more personal information than needed (Paksoy, 2019).

The National Health Information System (NHIS) is a system that the health information of those receiving healthcare from institutions and organizations delivering health care in Turkey and the information of manpower, movable and immovable properties and administrative and financial data related to these institutions and organizations gather under a central structure.

III. INFORMATION SYSTEMS

Information system can be defined as an information clusters system, which also included itself as a subsystem, necessary to gather, store, process, deliver, decide and transmit information clusters within a wider system having other subsystems. Every organization needs different quality of information depending on a different service field, a different way of working and the type of work performed. Information systems are classified in different features according to the management levels in organizations, functional fields and their way of supporting management (Ömürbek and Altın, 2009).

With the increase in the fields information technologies used have increased day by day, many implementations and services have been transferred to electronic environment. Applications and services such as e-state, e-health, e-commerce, e-municipality and e-school have become a part of daily life. Carrying out operations, storage and communication by using information technologies makes information security in digital media, accordingly information security important (Akgün and Topal, 2015).

3.1. Health Information Systems

In our age, information technologies are becoming increasingly widespread in health service delivery, healthcare services are becoming more technology dependent. Health information systems and decision support systems are developing immensely and technology performance is increasing incrementally. Computer use requires employees to have new qualifications such as, education, obtaining and implementing theoretical and analytical information, a different approach and the habit of continuous learning. Rapid advancements in information technologies have enabled significant innovations providing great achievements in healthcare field as they have in other disciplines (Işık and Akbolat, 2010).

With the use of current technology in healthcare sector remarkably, some risks of technology have been encountered. As well as all data in the electronic environment, it has become obligatory to take security measures for risks that also threaten personal health data. Since current technologies increase the risks of privacy, integrity and accessibility of personal health data, the security of health data are endangered. Due to the importance of the privacy of personal health data, it becomes essential to take measures and to determine and decrease the risks. In accordance with the importance of the security of information technologies, “Information Security Policies Guide” (The Ministry of Health, 2018) was issued by The General Directory of Health Information Systems.

3.2 Hospital Information System

Hospitals are service businesses that are affected greatly by technological improvements and work in knowledge intensive. Advancement of information technologies has made the use of information systems in also corporations delivering healthcare service essential as it has in all sectors. Healthcare corporations place great emphasis on the use of information systems, and in order to provide quality service delivery to patients and manage hospitals better, the demand of Hospital Information System (HIS) has emerged (Esatoğlu and Köksal, 2010).

Hospitals use information systems in many fields such as management services, identifying patients, supporting the decisions about patients to be made by doctors, guidance for the work of health professionals and laboratory services (Tengilimoğlu et al., 2017).

Two main factors are mentioned in today’s health information systems; electronic health records and individual health records. All health data a health system may need are in the electronic health records. Individual health records include the personal data and personal health records of patients. Although communication and access to information are made easy by these systems, it is required to provide accordance between the health system and patients (Tang and Lansky, 2005).

3.3 Basic Components Constituting Hospital Information Management Systems

Systems for supporting healthcare service providers and healthcare management are used to carry out many operations starting from patient admission and registration procedures to the invoicing the charges received from patients. As well as steadily continuing activities, support is provided for the management also in analysis and reporting. Systems to support the management can be sorted as following: Patient admission, consultation, appointment and record information system, patient payment and invoice information system (Wager et al., 2009).

During the development of HIMS, the needs of the stakeholders who will use this system come to the fore as the main determinants. At this point, it is seen that healthcare employees, executives, suppliers, decision makers and patients are the stakeholders. In this context, information systems to be used for healthcare services’ delivery are usually divided into three classes (Tengilimoğlu et al., 2017).

Information intensity of healthcare services has been increasing rapidly. With the use of information systems, remarkable improvements have experienced in the management of chronic diseases. A decrease is observed in medical mistakes such as inappropriate use of antibiotics, faulty prescriptions and unexpected side effects. Healthcare professionals can access medical information of patients faster and easily. In addition, saving is provided by avoiding unnecessary tests and workups. Important amount of time is saved in the service delivery provided for patients. Health data can be archived more appropriately, healthcare staff can have better communication with patients and devote more time for them. It is reported that productivity, efficiency and cost effectiveness is ensured (Raymond and Dold, 2002).

IV. ELECTRONIC HEALTH RECORDS AND THEIR IMPORTANCE

4.1. Medical Documentation: Definition and Importance

In “The Regulation on the Procedures and Principles to be Adopted in Official Correspondences,” ‘document’ is defined as “any kind of information or document received or prepared by the management to carry out an individual transaction, organizational function or organizational transaction, preserving the chain of concern by constituting evidence for the related function or transaction with its content, relation and form, and autographed or signed by electronic signature and recorded in EDMS or institutional document record system.”

Documentation is defined as a process consisting of many activities; refers the method created to determine and obtain the information needed, the recording of the information and the storage of the recorded information in appropriate environments, or the collection, arrangement and presentation of the already existing documents containing the required information to the users who need it or refers a part of the process (Guzman and Verstappen, 2003).

Medical documentation; medical document is defined as the documents created by regularly sorting out the data obtained from the actions performed for human health, and medical documentation refers to all processes regarding archiving these document appropriately with scientific and legal rules and presenting them to institutions or patients when required (Esatoğlu and Artukoğlu, 2000).

Medical documentation is at great importance for hospitals, patients receiving healthcare service, healthcare professionals, forensic medicine, public health and health professionals who conduct medical researches (as data source for their researches) (Tengilimoğlu and Çıtak, 2003).

4.2. Electronic Health Record System

In developed countries, Electronic Health Records have distinct advantages providing a wider acceptability than paper records. These include the opportunity of improving the quality in patient care and security in health care institutions, the opportunity of cost reduction and increase in the productivity of organizations, access to medical records from remote locations, improved speed and the convenience of recording and reducing the occurrences of prescription errors by eliminating hand written prescriptions (Attah, 2017).

EU countries have both adopted EHRs and confirmed the commitments for patient privacy principles. The USA system is lack of a strong framework of the privacy of healthcare services and this will affect the application of EHRs. If the USA applies EHRs efficiently, technical and politic aspects of the privacy should be in the center of the discussion (Hiller et al., 2011).

4.3. Duties and Responsibilities of Medical Secretaries

In English, the word ‘secretary’ is derived from ‘secret’, which means confidential, and secretary means the one keeping secret. In the dictionary of Turkish Language Society, secretary is defined as “a person providing communication and being able to exchange correspondence to help a certain office or person in private and state institutions; clerk.”

Medical secretaryship is different from other types of secretaryships in terms of the specialty. Medical secretaries should know the processes and characteristics of health care institutions and medical terminology very well. They perform duties of vital importance such as recording in the service areas such as clinics, polyclinics, laboratories, operating theatres and intensive care units in hospitals. In healthcare service delivery, recording the data in an orderly way, accessing them easily and the analysis of the information is related to a good operation of medical secretaryship services. Highly educated medical secretaries and well planned secretaryship services are required in improving the quality of healthcare service delivery and delivering fast and economic service to patients, relatives and other related institutions (Tengilimoğlu and Çıtak, 2003).

V. THE PROTECTION OF PERSONAL DATA

Personal data refers to any kind of information about an identified or identifiable natural person. To be able to mention personal data, the data should belong to a natural person.

Personal data is defined as “Any kind of information belonging to an identified or identifiable natural person” in the 24.03.2016 dated and 6698 numbered code issued in the 04.04.2016 dated and 29677 numbered Official Gazette. It is defined as “All information about an identified or identifiable natural person” in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series, No. 108 (Council of Europe, 1981). Data protection principles were determined in the Guidelines issued by OECD in 1980.

5.1. The Concept of Personal Health Information

Countries should establish a comprehensive legal and political framework throughout the country including privacy and privacy rights, which are among human rights, for privacy and security. The framework should contain administrative and technical policies, procedures, instructions and standards in order to provide the utility, integrity, privacy and physical security of health information, to balance high utility advantages for planning and operations of public health and to ensure researches by protecting personal rights. Such a comprehensive framework will help to provide the consistency and integrity in electronic health record application, thus will reduce the risk of undesired result. While all frameworks should be adapted to local needs, contexts, priorities and values, a clearly defined framework is definitely preferred over an implicit one. Even if overall frameworks have advantages, it is important for each setting to adopt a bespoke approach handling local contexts and problems (WHO, 2017).

Personal health data are in the sensitive data category. Therefore, more strict measures of protection are stipulated compared to other types of data. Accordingly, in the cases that explicit consent is not required, these data can be processed only by the people having the responsibility of keeping secrets or authorized institutions and organizations. There is no such a limitation for other data types included in the category of sensitive data (Akgül, 2013).

In the Law of Personal Data Protection, medical information of patients is in the definition of special quality personal data. Special quality personal data is defined as individuals’ races, ethnic origins, political opinions, philosophical beliefs, religions, sects and other beliefs, appearances, memberships of society, foundation or union, health, sexual lives, criminal convictions and the data related to security measurements and biometric and genetic data (Law of Personal Data Protection, 2016).

5.2. The Importance of Personal Health Data in Healthcare Services

Privacy is a human right, and citizens’ control of their health data should be supported by the policy of privacy and security of the national electronic health records. The policy should contain necessary procedures for those who might be suffered from violations. These policies can ensure protection against social or economic discrimination and establish trust to healthcare system. In addition, care should be taken to ensure that critical health data remains accessible at the point of healthcare, and systems should exist to manage privacy protection in the context of infectious diseases and/or environmental hazards. Appropriate software and control infrastructure is required for patients’ control of their data and to monitor who has viewed a record or who a record has been transferred to. The infrastructure of monitoring privacy violations requires establishing special teams (WHO, 2017).

VI. METHOD

This cross-sectional study was conducted on 280 participants working at Erciye University Health Implementation Center (HIRC) as medical secretaries between the dates of October – December 2019. Sample was not selected in the research, and it was aimed to reach the whole population. The study was conducted with 210 (80.7%) medical secretaries who accepted to participate in the research voluntarily.

The data in the research were collected by a questionnaire form for determining the descriptive characteristics of the medical secretaries, “Information Security Awareness Scale” and “The Adjustment Scale of Electronic Health Records Security and Privacy Standards.” As descriptive characteristics, secretaries answered the questionnaire for “Knowledge, Attitudes and Behaviors Related to Information Security and Electronic Health Records Privacy."

a) Questionnaire Form

A questionnaire form with two parts was used in the study. In the first part of the questionnaire form, which was prepared in the light of similar previous studies (Öztürk, 2014; Özata, 2016; Paksoy, 2019), Patient Right Regulation and literature, 11 questions were asked related to gender, age, marital status, education status, the department they work at, the unit they work in the institution, the state of working suitable for the professional education, overall working period in the profession, the state of receiving training about electronic health records, working period in the institution and the experience period of electronic health record use. The second part included 10 questions asked to evaluate medical secretaries’ Knowledge, Attitudes and Behavior patterns of Electronic Health Records’ Privacy.

The questionnaires in the study were conducted by the researcher by using face to face interview technique.

b) Information Security Awareness Scale

Information Security Awareness Scale, developed by Keser and Güldüren (2015) was used in the research. The questions were prepared in 5 point likert scale. The participants were asked to score the items as “Strongly Disagree (1),” “Disagree (2),” “Undecided (3),” “Agree (4)” and “Strongly Agree (5)” (Appendix 1).

The scale includes 34 items, and two subscales as “attacks and threats” and “protection of personal data.” The first 16 items in the scale are the questions for determining the awareness for attacks and threats, and the items from 17 to 34 are for specifying the awareness for personal data protection. Keser and Güldüren found the overall Cronbach alpha reliability coefficient of the scale as 0.97, for “attacks and threats” subscale as 0.97 and for “personal data protection” subscale as 0.94. In the research, findings are interpreted by using the original factor structure of Keser and Güldüren’s (Keser and Güldüren, 2015).

c) The Adjustment Scale of Electronic Health Records Security and Privacy

The Adjustment Scale of Electronic Health Records Security and Privacy, which was developed by Paksoy by being based on the Health Insurance Portability and Accountability Act (HIPAA) standards was used in the research. The questions were prepared in accordance with the 5-point likert scale. In the grading, the participants were asked to score the items as “Strongly Disagree (1),” “Disagree (2),” “Undecided (3),” “Agree (4)” and “Strongly Agree (5)” (Appendix 2).

As a result of the factor analysis, 24th, 25th, 26th, 29th and 35th questions were omitted from the scale since they were the items resulting high factor load value in more than one factor. The scale with 20 questions including 3 factors explains 56.93% of the total variance with its final form (Brown, 2015). The scale, obtained with factor analysis, evaluated in the subscales of Security and Privacy Policies, Organizational Security and Training and Security by considering the literature. Security and Privacy Policies includes the 22nd, 16th, 20th, 18th, 19th, 21st, 17th and 23rd questions, Organizational Security includes the 38th, 37th, 32nd, 33rd, 36th and 39th questions and Training and Security Applications includes the 40th, 27th, 30th, 31st, 28th and 34th questions. The reliability of the scale was evaluated by Cronbach Alpha reliability coefficient. For all items indicating internal consistency, Cronbach Alpha reliability coefficient was determined as 0,879 for Security and Privacy

Policies, as 0,871 for Organizational Security and as 0, 804 for Training and Security Applications, and it was observed that there was internal consistency (Erbil, 2009; Field, 2009).

Statistical Evaluation

In the statistical analysis, SPSS 25 and Stata 14.0 statistics software were used. Number and percentage distributions, mean, standard deviation, median and minimum and maximum values were revealed in the presentation of the descriptive characteristics of the obtained data. The compliance test for normal distribution was performed in order to decide to use whether parametric or nonparametric tests in the statistical analysis for Information Security Awareness Scale and the Adjustment Scale of Electronic Health Records Security and Privacy Standards. Parametric tests were decided to be used in the analysis to be performed for the scales. In the between-group comparisons, independent two-sample independent t-test and one-way analysis of variance were used for quantitative variables. Tukey (post-hoc test) method was used as the multiple comparison analysis. The significance level was accepted as $p< 0.05$ in the evaluations. Correlation analysis was performed to test the relation between the total and subscale scores of the Adjustment Scale of the Electronic Health Records Security and Privacy Standards and total and subscale scores of ISAS. Multivariate linear regression analysis was performed to determine the effect of ISAS subscales on the EHR total score in the multivariate analysis. The obtained results were presented in the form of standardized beta and significance level and the effect size of each variable.

Ethics Committee Approval (committee name, date and number): This study was approved by Kayseri University Ethics Committee (26.09.2019 dated and 26 numbered).

VII. RESULTS

60.2% of the medical secretaries were at the age range of 34-43, 32.7% were at the age range of 24-33, 69.7% of them were female, 81.5% were married, 53.3% had associate degree and 34% had bachelor’s degree.

31.8% of the medical secretaries worked at polyclinics, 30.4% at clinics, 19.9% at laboratories and 18.0% at administrative units.

55.2% of the medical secretaries worked at the departments suitable for their professional education, the overall working periods of the 47.4% were at the range of 0-11 years and the working period at the institution of the 47.4% was 11-20 years.

41.2% of the medical secretaries stated that “recording and sharing health records on the computer environment affected information security and privacy negatively,” 96.7% stated they “believed the importance of privacy, which is the essential right of patients, and personal information privacy,” 96.2% stated they “followed the rules preventing patients to be affected by their diseases,” 97.6% stated they “protected the privacy/personal information privacy of the patients incapable for protecting themselves,” 97.2% stated “the confidentiality of the private lives/personal information of the patients was ensured unless there was a legal obstacle” and 91.0% stated that "the private and personal information of the patient was never shared with others without the patient's consent / approval."

68.2% of the medical secretaries stated the reason for possible information security / privacy violations in hospitals as carelessness, 62.6% of them as busyness and 54.0% as unawareness.

While 90.5% of the medical secretaries stated that hospitals are responsible for ensuring the security of the health records, 82.0% stated that healthcare professionals are responsible.

82.9% of the medical secretaries state the primary privacy area of the patients as their private life and personal information, 72.0% of them as their health state and 63% as the bodies of the patients.

Table 1. Subscale Averages of Information Security Awareness Scale and the Adjustment Scale of Electronic Health Records Security and Privacy Standards of the Individuals Included in the Research Group

Subscales	Mean	Standard Deviation
Information Security Awareness Scale		
Awareness for attacks and threats	3.1	1.1
Personal Data Protection	4.0	0.7
Information Security Awareness General	3.6	0.8
The Adjustment Scale of Electronic Health Records Security and Privacy Standards		
Security and Privacy Strategies	3.8	0.8
Organizational Security	4.0	0.7
Training and Security Policies	3.5	0.8

Among Information Security Scale (ISAS) subscales, the level of “Personal Data Protection” was determined as high (4.0±0.7), the level of “the Awareness for Attacks and Threats” was as moderate (3.1±1.1) and the level of “Information Security Awareness General” as (3.6±0.8).

It was determined that, among the Adjustment Scale of Electronic Health Records Security and Privacy Standards subscales, medical secretaries received the highest score from “Organizational Security” (4.0±0.7) and the lowest score from “Training and Security Policies” (3.5±0.8) **(**Table 1).

When the ISAS subscale scores of the medical secretaries were analyzed in terms of their demographic and socio-cultural characteristics, the difference between the groups in terms of gender was found statistically significant. Female secretaries’ score averages of the Awareness for Attacks and Threats subscale, Personal Data Protection subscale and Information Security Awareness General subscale were found significantly higher when compared to the male secretaries ($p<0.05$).

When the distribution of the subscale scores of the Adjustment Scale of Electronic Health Records Security and Privacy Standards of the medical secretaries were analyzed in terms of demographic and socio-cultural characteristics, the difference between the groups in terms of gender in Organizational Security subscale was found significant. Male medical secretaries’ organizational security subscale scores were found significantly higher than the female secretaries’ ($p<0.05$).

When the distribution of the subscale scores of ISAS of the medical secretaries were analyzed in term of the unit they work, a statistically significant difference was found in Personal Data Protection and Information Security Awareness General subscales between the groups. Personal Data Protection and Information Security Awareness General subscale score averages of those working at polyclinics was found significantly higher than the other groups’ ($p<0.05$).

When the ISAS subscale scores of the medical secretaries in terms of the overall working period, the difference in the Awareness for Attacks and Threats, Personal Information Security and Information Security Awareness General subscales between the groups was found significant. The subscale scores averages of the medical secretaries working at the range of 1-10 years was found significantly higher than the others’ ($p<0.05$).

When the ISAS subscale score distributions of the individuals included in the research group was analyzed in terms of the working period in the institution, a statistically significant difference was found in the Personal Data Protection and Security Information Awareness General subscales between the groups. The subscale score averages of the medical secretaries working at the institution at the range of 1-10 years determined as significantly higher than the others’ ($p<0.05$).

When the ISAS subscale score distributions of the medical secretaries were analyzed in terms of using Electronic Health Records, a statistically significant difference was determined in the subscales of the Awareness for Attacks and Threats, Personal Data Protection and Information Security Awareness General between the groups. The subscale score averages of the medical secretaries using Electronic Health Records at the range of 1-10 years were found significantly higher than the others' (p<0.05).

When the subscale score distributions of the Adjustment Scale of Electronic Health Records Security and Privacy Standards were analyzed in terms of the state of working at the suitable department for professional education, the difference between the groups in the Training and Security Policies scores and the Adjustment Scale of Electronic Health Records Security and Privacy Standards total scores was found statistically significant. The scores of the medical secretaries working at the suitable departments for their professional education were significantly higher than those stated they did not work at the suitable departments for their professional education (p<0.05).

When the distributions of the ISAS subscale scores of the individuals included in the research group in terms of knowledge, attitudes and behaviors related to information security and privacy were analyzed, the subscale scores of the Awareness for Attacks and Threats of the medical secretaries stating they always protected "the privacy / personal information privacy of the patients incapable to protect themselves" were found significantly higher than those stating sometimes they provided it (p<0.05).

The distributions of the Adjustment Scale of Electronic Health Records Security and Privacy Standards subscale scores of the medical secretaries in terms of the Knowledge, Attitudes and Behaviors Related to Electronic Health Records Privacy were analyzed. As a result, Security and Privacy Strategies scores and the Adjustment Scale of Electronic Health Records Security and Privacy Standards total scores of the medical secretaries stating they always followed the "the rules preventing patients to be affected by their diseases" were found significantly higher than those stating they sometimes followed the rules (p<0.05).

The Organizational Security subscale scores of the medical secretaries stating they always followed "the rules preventing patients to be affected by their diseases" were found significantly higher than those stating they sometimes followed the rules (p<0.05).

Table 2. The correlation between Information Security Awareness Scale, the Adjustment Scale of Electronic Health Records Security and Privacy Standards, subscale scores and some variables

Subscales	**Age**	**Overall Working Period**	**Working Period at the Institution**	**EHRs use experience**
Information Security Scale				
Attacks and threats	r= -0.151*	r= -0.162*	r= -0.164*	r= -0.152*
Personal Data Protection	r= -0.208**	r= -0.239**	r= -0.235**	r= -0.194**
ISAS total score	r= -0.191**	r= -0.212**	r= -0.212**	r= -0.185**
The Adjustment Scale of Electronic Health Records Security and Privacy Standards				
Security and privacy strategies	r= -0.087	r= -0.084	r= -0.125	r= -0.047
Organizational security	r= 0.038	r= -0.014	r= 0.008	r= 0.011
Training and security policies	r= 0.027	r= 0.004	r= -0.037	r= -0.001
Total score	r= -0.019	r= -0.042	r= -0.068	r= -0.019

***p<0.05, **p<0.01**

When the correlation between the scores of ISAS, the Adjustment Scale of Electronic Health Records Security and Privacy Standards and subscale scores and some variables was analyzed, a statistically significant, negative, very weak and weak correlation was found between age, overall working period, working period at the institution and EHRs use experience period and ISAS and subscale scores (p<0.01) **(**Table 2**).**

Table 3. **The correlation between Information Security Awareness Scale and the Adjustment Scale of Electronic Health Records Security and Privacy Standards subscale scores of the medical secretaries**

Information Security Awareness Scale subscales	**The Adjustment Scale of Electronic Health Records Security and Privacy Standards**			
	Security and Privacy Strategies	**Organizational Security**	**Training and Security Policies**	**Scale Total Score**
Awareness for Attacks and Threats	r= 0.517 p<0.01	r= 0.494 p<0.01	r= 0.550 p<0.01	r= 0.584 p<0.01
Personal Data Protection	r= 0.556 p<0.01	r= 0.586 p<0.01	r= 0.520 p<0.01	r= 0.620 p<0.01
Information Security Awareness General	r= 0.581 p<0.01	r= 0.580 p<0.01	r= 0.583 p<0.01	r= 0.651 p<0.01

When the correlation between the Adjustment Scale of Electronic Health Records Security and Privacy Standards and Information Security Awareness Scale subscales scores of the individuals included in the research group was analyzed, statistically significant, positive, moderate and high correlation was found between the scales and the subscales (p<0.01) (Table 3).

Table 4. The effect of the Information Security Awareness Scale subscales on the Adjustment Scale of Electronic Health Records Security and Privacy Standards total score, the result of the multivariate linear regression analysis

	Coef.	**S.Beta**	**t**	**Sig.**	**η^2**
ISAS Attacks and threats subscale	0.186	0.299	4.132	0.000	0.076
ISAS Personal Data Protection subscale	0.379	0.413	5.708	0.000	0.135
Invariant	1.671		8.400	0.000	

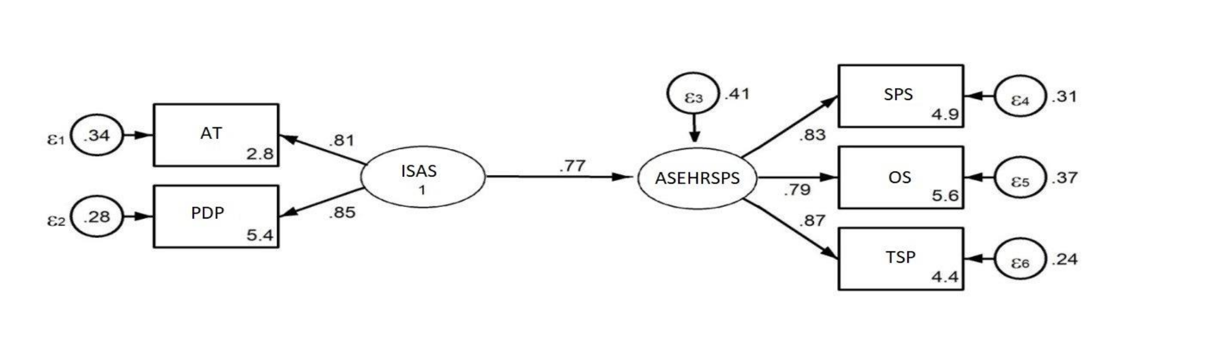
R^2=0.431 Coef.: Regression coefficient, S.Beta: standardized regression (beta) coefficient,

η^2: Eta Squared-effect size (0.01-0.04 low, 0.06-0.13 moderate, 0.14-0.20 high)

As a result of the multivariate regression analysis, it was determined that ISAS attacks and threats and personal data protection subscales separately affected the Adjustment Scale of Electronic Health Records Security and Privacy Standards scores of the medical secretaries that they obtained over the total score. Accordingly, while the standardized beta value of the personal data protection was at the level of 0.413, a value of 0.299 was observed in the attacks and threats subscale (p<0.001).

When the effect size of the variables in the model on the Adjustment Scale of Electronic Health Records Security and Privacy Standards was analyzed, it was found that the effect size was at moderate level with 0.076 in ISAS attacks and threats subscale, and with 0.135 in ISAS personal data protection subscale. The coefficient of determination of the model is R^2=0.431. The obtained result indicates that information security level has a very important role in conforming to Electronic Health Records Security and Privacy Standards **(**Table 4).

Figure 1. The structural equation modeling between ISAS and the Adjustment Scare of Electronic Health Records Security and Privacy Standards



ISAS: Information Security Awareness Scale, **AT:** Attacks and Threats, **PDP:** Personal Data Protection, **ASEHRSPS:** the Adjustment Scare of Electronic Health Records Security and Privacy Standards, **SPS:** Security and Privacy Strategies, **OS:** Organizational Security, **TSP:** Training and Security Policies

Table 5. Testing the correlation between Information Security Awareness Scale and the Adjustment Scale of Electronic Health Records Security and Privacy Standards via structural equation modeling

Variables	**Coef. (%95CI)**	**Z**	**p**
Structure model			
The Adjustment Scale of Electronic Health Records Security and Privacy Standards ←ISAS	0.77 (0.68-0.85)	17.82	0.000
Measurement model			
Awareness for Attacks and Threats ←ISAS	0.81 (0.74-0.88)	21.92	0.000
Personal Data Protection ←ISAS	0.84(0.77-0.91)	23.73	0.000
Security and Privacy Strategies ← The Adjustment Scale of Electronic Health Records Security and Privacy Standards	0.83(0.77-0.88)	29.36	0.000
Organizational Security ← The Adjustment Scale of Electronic Health Records Security and Privacy Standards	0.79(0.73-0.85)	24.96	0.000
Training and Security Policies ← The Adjustment Scale of Electronic Health Records Security and Privacy Standards	0.87(0.82-0.92)	34.67	0.000

Chi-square=14.17, sad=4, p=0.006, RMSEA=0.110, CFI=0.982, SRMR (Standardized Root Mean Square Residual) =0.020

As a result of the structural equation modeling created to confirm the correlation between Information Security Awareness Scale and the Adjustment Scale of Electronic Health Records Security and Privacy Standards, the correlation between the two structure is observed to have a large and significant coefficient [0.77 ($p<0.001$)]. CFI (Comparative Fit Index) that shows the goodness of fit of the created model is at the good level with the value 0.98. Chi-square/degrees of freedom is about 4, and RMSEA (Root Mean Square Error of Approximation) is slightly above the limit with the value of 0.11. Standardized RMR (Root Mean Square Residuals) value is at good level with 0.02. It is observed that this significant model created reveals an adequate structure (Table 5).

VIII. DISCUSSION AND CONCLUSION

In our study, it was determined that medical secretaries obtained the highest score from the ISAS "Personal Data Protection" subscale, and the lowest score from "Information Security Awareness General" subscale. In the study conducted by Çelik-Çöp (2017) on Quality Directors, the level of Personal Data Protection of the directors was determined as high, and the levels of the Awareness for Attacks and Threats and Information Security Awareness General were determined as moderate. In the study conducted by Taner (2019), the level of Information Security Awareness were reported as generally low. Our study results reveal that the awareness level of "Personal Data Protection" of the medical secretaries is high rather than the operation of the process, and this result is important.

It was determined that medical secretaries obtained the highest score from "Organizational Security", the subscale of the Adjustment Scale of Electronic Health Records Security and Privacy Standards scale, and the lowest score from "Training and Security Policies." When the average scores of the subscales of Electronic Health Records Security and Privacy were evaluated in the study by Paksoy (2019), it was reported that highest score was in "Organizational Security," and the lowest score was in "Training and Security Applications." Our study findings are similar to the findings in the study by Paksoy (2019).

In our study, the score averages of ISAS subscales "Awareness for Attacks and Threats," "Personal Data Protection" and "Information Security Awareness" of female participants were found significantly higher than males ($p<0.05$). It might be thought that the high level of the Awareness for Attacks and Threats of females is related to that they did not feel secure about attacks and threats as much as males and they feel incompetent in protecting themselves. The fact that female secretaries had high levels of Personal Data Protection and Information Security Awareness might be an indication that they are more sensitive when compared to males.

In the research conducted by Öztezcan (2017) in order to reveal the information security level awareness of the administrative and academic staff working at Marmara University, it was observed that female staff had less awareness for the matters related to attacks and threats and personal data protection. Our study findings do not correspond with the results of some other similar studies. It is believed that one of the reasons of this difference is a result of that sample groups are different.

In our study, subscale scores of organizational security of the Adjustment Scale of Electronic Health Records Security and Privacy Standards of male medical strategies were found significantly higher than the female secretaries' ($p<0.05$). Yılmaz et al. (2016) conducted a study on teachers working at private and state schools in Balıkesir province titled "Digital Data Security Awareness of Teachers," and revealed that digital data security awareness of female teachers was lower than male teachers'. On the other hand, in the study conducted to evaluate the knowledge and attitudes of nurses in the context of electronic health records and information applications, it was reported that attitude score averages of the nurses for information technologies applications did not differ significantly in terms of the gender variable (Çakırlar, 2016). Based on all these results, studies to be conducted with the same and well-attended sample groups are needed to make definite judgments related to the issue.

In our study, the score averages of ISAS Personal Data Protection and Information Security Awareness General of the medical secretaries working at policlinics were found significantly higher than those working at other units ($p<0.05$). With the study by Terlemez (2014), it was revealed the thoughts of the medical secretaries and administrative staff working at Namık Kemal University Health Implementation and Research Center about information and archive systems, and most of the participants reported that they believed electronic environment should be used and the measures for document security and protection should be improved. In our study, it was determined that the awareness levels of Personal Data Protection and Information Security the medical secretaries working at polyclinics were high, and this result might be related to that since patient circulation is high in polyclinics and it might be easier to get patient information, the staff feels the requirement of being more careful and deliberate.

In our study, it was determined that the medical secretaries having overall working period and working period at the institution at the range of 1-10 years obtained significantly higher subscale score averages of ISAS Awareness of Attacks and Threats, Personal Data Protection and Information Security Awareness General when compared to other secretaries having other working periods ($p<0.05$). These results can be explained by the fact that secretaries at the beginning of their working life embrace their jobs more enthusiastically, they have the expectation of promotion and their occupational knowledge and equipped is new. In other words, it might be thought that as the working period in the profession increases, factors such as decrease in the enthusiasm and idealism in the beginning, becoming of secondary importance of promotion expectation and development of tiredness might be effective. In our study, the was found that medical secretaries using Electronic Health Record at the range of 1-10 years had significantly higher subscale score averages of the Awareness for Attacks and Threats, Personal Data Protection and Information Security Awareness when compared to those using electronic health records other ranges of time periods, and this finding supports the above mentioned discussions.

In our study, the scores of Training and Security Policies subscale of the Adjustment Scale of Electronic Health Records Security and Privacy Standards and the Adjustment Scale of Electronic Health Records Security and Privacy Standards total scores of the medical secretaries working at the suitable department for their professional education found significantly higher than those stating they did not work at the suitable department for their professional education ($p<0.05$). This result can be explained by the fact that being employed at the departments suitable for their professional education increases medical secretaries' enthusiasm since their professional knowledge and equipment is high and also they work at their occupational field. In the compilation study by Ay (2008), the importance of the arrangement of curriculums in health education and including the subject of information technologies before and after graduation is emphasized in order electronic health record systems to be used and maintained efficiently.

In our study, the subscale scores of ISAS Awareness for Attacks and Threats, Personal Data Protection and Information Security General of the medical secretaries who stated they always protected “the confidentiality of the privacy / personal information of the patients incapable to protect themselves” were found significantly higher than those stating they sometimes provided protection ($p<0.05$). In the study by Adeyato-Odepidan (2016) it is stated that healthcare service providers should provide adequate protection for the health information and privacy of the patients, and institutions should inform their employees about privacy policy and introduce the passwords. It is an expected result that Medical Secretaries who stated in our study that they always protected “the confidentiality of the privacy / personal information of the patients incapable to protect themselves” will demonstrate these successful practices in other fields.

In our study, Security and Privacy Strategies and the Adjustment Scale of Electronic Health Records Security and Privacy Standards total scores of the medical secretaries who stated they always followed “the rules preventing patients to be affected by their diseases” were found significantly higher than those stating they sometimes followed the mentioned rules ($p<0.05$). In the study titled “The Evaluation of Patient Confidentiality Implementations in Hospitals in the Context of Quality Standards in Healthcare: The Case of Konya” by Özata (2016), it was revealed that the hospitals in the context of the study generally exercised due care of the patient privacy protection and they made necessary arrangements. The fact that medical secretaries stating they always followed the rules preventing patients to be affected by their diseases had high scores of Security and Privacy Strategies and high total scores of the Adjustment Scale of Electronic Health Records Security and Privacy Standards conforms with the approach that a success in a field is observed in other fields. Similarly, Organizational Security subscale scores of the medical secretaries stating they always followed the rules preventing patients to be affected by their diseases were found significantly higher than those stating they sometimes followed the rules in question ($p<0.05$).

In our study, a negative, very weak and weak statistically significant correlation was found between the ages, overall working periods, working periods in the institution and EHRs use experience of the medical secretaries and their ISAS and its subscale scores ($p<0.01$). In the study conducted by Karakaya (2018) to search for the Importance of Medical Documentation for Health Care Institutions, it was found that as the age averages of the participants decreased, their perception level of electronic medical record system increased, and as the age increased, the perception decreased.

It can be foreseen that ISAS the Awareness for Attacks and Threats, Personal Data Protection and Information Security Awareness General subscale scores might decrease in relation to the reasons such as the decrease in the enthusiasm for working and promotion and not their knowledge being updated as the ages, overall working periods, working periods in the institution and EHR use experiences of the medical secretaries increased. In the study conducted by Karakaya (2018), it was determined that the perception levels of the participants in the Form Medical Record subscale did not affected by the increase or decrease in the working periods. However, a significant correlation was found between the perception of Medical Record System in terms of Electronic Record System and Quality Accreditation and working periods. With the increase in the participants' working periods in the institution, their perception levels of Medical Record System in terms of EHRs and Quality Accreditation decreased, but with the decrease in the working periods perception levels increased.

When the correlation between the ISAS subscale scores and the Adjustment Scale of Electronic Health Records Security and Privacy Standards subscale scores was examined, a positive, moderate and high level of statistically significant correlation was found between the scales and subscales ($p<0.01$). In the analysis of structural equation modeling, which was created to confirm the correlation between Information Security Awareness Scale and the Adjustment Scale of Electronic Health Records Security and Privacy Standards on a model, it was revealed that the correlation between the two structures had a large and significant coefficient ($p<0.001$). This result means that as the medical secretaries have Information Security Awareness, the Adjustment of Electronic Health Records Security Privacy Standards will increase, and the opposite is also true. In another word, this situation is a cause and effect relation. In Paksoy's research result, it is emphasized that the practice of the standards determined for the security and privacy of electronic health records and regular training delivery is quite important in adopting the culture of information security and privacy.

Consequently, the effect of the Information Security Awareness levels of the medical secretaries on the Adjustment of Electronic Health Records Security and Privacy Standards was searched in this study, and it was revealed that as a result of the analysis of structural equation modeling created to confirm the correlation between Information Security Awareness Scale and the Adjustment Scale of Electronic Health Records Security and Privacy Standards, the correlation between the two structures had a large and significant coefficient.

Limitations and Recommendations

The research findings are limited with the data obtained from those working at Erciyes University Health Implementation and Research Center (HIRC) as medical secretaries.

The awareness levels of the medical secretaries in our study is high, and since the security and privacy of the information of those receiving healthcare service delivery is evaluated as one of the fundamental human rights, and against the possibility of being obtained of these data by individuals or organizations that will use them for their personal interests, hospital directors should take the measures related to software, encoding and protection that are necessary especially for electronic medical record systems.

REFERENCES

Acılar, A., (2009). İşletmelerde bilgi güvenliği ve örgüt kültürü. *Organizasyon ve Yönetim Bilimleri Dergisi*, 1(1), 30.

Adeyato-Odepidan, M., (2016). *Electronic health record systems - A study of privacy in the region kronoberg of Sweden*. (Master's Thesis). Linaeus University, Sweden.

Akgül, A., (2013). *Kişisel verilerin korunmasi açisindan idarenin hukuki sorumluluğu ve yargisal denetimi*. (Doktora Tezi). Kocaeli Üniversitesi, Kocaeli.

Akgün, Ö. E., & Topal, M., *(2015).* Eğitim fakültesi son sinif öğrencilerinin bilişim güvenliği farkındalıkları: Sakarya Üniversitesi eğitim fakültesi örneği. *Sakarya University Journal of Education*, 5(2), 98-121.

Alkan, N. (2003). Tıp ve sağlik kuruluşlarında bilgi yönetimi. *Bilgi Dünyası*, 4(2), 122-145.

Aras, M. (2018). İşletmelerde bilgi koruma stratejileri. *Ordu Üniversitesi Sosyal Bilimler Araştırmaları Dergisi,* 8(3), 613-621.

Ay, F. (2008). Elektronik hasta kayıtları: Güvenlik, etik ve yasal sorunlar. *Bilim ve Teknoloji Dergisi,* 9(2), 65-175.

Baran, S., & Şener, E. (2019). Hastanelerde bilgi güvenliği yönetimi: Nitel bir araştirma. *Süleyman Demirel Üniversitesi Vizyoner Dergisi*, 10(23), 108-125.

Baykara, M., Daş, R., & Karadoğan, İ. (2013). Bilgi güvenliği sistemlerinde kullanılan çalışması. *Dokuz Eylül Üniversitesi Hemşirelik Fakültesi Elektronik Dergisi,* 12(1), 21-30.

Brown, T. A. (2015). *Confirmatory Factor Analysis for Applied Research*. Guilford publications, New York.

Çakırlar, A. (2016). *Hemşirelerin elektronik sağlık kaydı ve bilişim uygulamalari kapsamındaki bilgi ve tutumlarının değerlendirilmesi*. (Yüksek Lisans Tezi). Bilim Üniversitesi, İstanbul.

Çelik-Çöp, Ç. (2017). *Kalite yönetim direktörlerinin bilgi güvenliği farkındalığı: İstanbul İli örneği.* (Yüksek Lisans Tezi). Okan Üniversitesi, İstanbul.

Erbil, N. (2009). Hasta hakları kullanma tutumu ölçeğinin geliştirilmesi. *Uluslararası İnsan Bilimleri Dergisi*, 6(1), 826-838.

Esatoğlu, A. E., & Artukoğlu, A. (2000). Tıbbi dokümantasyon tarihi ve tıbbi dokümantasyon ile ilgili meslekleşmenin gelişimi. *Ankara Üniversitesi Dikimevi Sağlık Hizmetleri Meslek Yüksekokulu Yıllığı*, 1(1), 13.

Esatoğlu, A. E., & Köksal, A. (2010). *Sağlık Hizmetlerinde Bilgi Yönetimi.* Ankara Üniversitesi Uzaktan Eğitim Yayınları, Ankara.

Field, A. (2009). *Discovering Statistics Using SPSS.* (2th Edition), SAGE Publications, London.

Guzman, M., & Verstappen, B. (2003). Human rights information and documentation systems. *Cenevre, İnsan Hakları İzleme ve Dökümantasyon Dizisi*, 2, 5-9.

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): U.S. and EU Compared.* Virginia: Sci. & Tech.

Hong, L., Luo, M., Wang, R., Lu, P., Lu, W., & Lu L. (2018). Big data in health care: Applications and challenges. *Data and Information Management*, 2(3), 175-197.

Işık, O., & Akbolat, M. (2010). Bilgi teknolojileri ve hastane bilgi sistemleri kullanimi: Sağlık çalışanları üzerine bir araştırma. *Bilgi Dünyası,* 11(2), 365-389.

Işık, O. (2013). Sağlık bilgi sistemlerinin gelişimi. Yılmaz A. (editör), *Sağlık Kurumlarında Bilgi Sistemleri* (ss.2-23). Eskişehir: Anadolu Üniversitesi Açıköğretim Fakültesi Yayınları.

Karakaya, İ. (2018). *Tıbbi dokümantasyonun sağlık kurumlari açısından önemi ve bir uygulama: Kamu ve özel hastane çalışanlarının tıbbi kayıt sistemine yönelik tutumları.* (Yüksek Lisans Tezi). Arel Üniversitesi, İstanbul.

Keser, H., & Güldüren. C. (2015). Bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *K. Ü. Kastamonu Eğitim Dergisi*, 23(3), 1167-1184.

Liew, A. (2013). DIKIW: Data, information, knowledge, intelligence, wisdom and their inte relationships. *Business Management Dynamics*, 2(10), 49- 62.

Odabaş, H. (2003). Kurumsal bilgi yönetimi. *Türk Kütüphaneciliği*, 17(4), 357-386.

Attah, A. O. (2017). *Implementing the electronic health record in a Nigerian secondary healthcare facility: Prospects and challenges*. (Master's Thesis). The Arctic University of Norway, Norway.

Ömürbek, N., & Altın, F. (2009). Sağlık bilişim sistemlerinin uygulanmasına ilişkin bir araştırma: İzmir örneği. *Süleyman Demirel Üniversitesi, Fen Edebiyat Fakültesi Sosyal Bilimler Dergi*si, 19, 211-232.

Özata, M., & Özer, K. (2016). Hastanelerde hasta mahremiyetine yönelik uygulamalarının sağlıkta kalite standartları bağlamında değerlendirilmesi: Konya örneği. *The Journal of Academic Social Science Studies*, 45, 11-33.

Öztezcan, B. A. (2017). *Bilgi güvenliği farkındalığı üzerine bir araştırma: Marmara Üniversitesi örneği.* (Yüksek Lisans Tezi). Marmara Üniversitesi, İstanbul.

Öztürk, H., Özçelik, S. K., & Bahçecik, N. (2014). Hemşirelerin hasta mahremiyetine özen gösterme durumu. *Ege Üniversitesi Hemşirelik Fakültesi Dergisi*, 30(3), 19-31.

Paksoy, V. M. (2019). *Elektronik sağlık kayıtlarının güvenlik ve mahremiyet uygulamalarının özel hastanelerde değerlendirilmesi: Kayseri İli örneği*. (Doktora Tezi). Marmara Üniversitesi, İstanbul.

Raymond, B., & Dold, C. (2002). *Clinical Information Systems: Achieving The Vision*. Oakland: Kaiser Permanente.

Resmi Gazete (2010). *Elektronik Haberleşme Güvenliği Kapsamında TS ISO/IEC 27001 Standardı Uygulanmasına İlişkin Tebliğ*, sayı: 27730 mükerrer.

Resmî Gazete (2016). *Kişisel Verilerin Korunması Kanunu*, sayı: 29677 mükerrer.

Sağlık Bakanlığı. (2018). *Tam Donanımlı Dijital Hastane Kılavuzu*. Ankara: Sağlık Bakanlığı yayınları.

Taner, E. (2019). *Güvenlik güçlerinin bilgi güvenliği farkindaliğina yönelik bir betimleme*. (Yüksek Lisans Tezi). Kocatepe Üniversitesi, Afyon.

Tang, P. C, & Lansky, D. (2005). The missing link: Bridging the patient-provider health information gap. *Health Affairs*, 24(5), 1290-1295.

Tavakoli, N., Ehteshami, A., Hassanzadeh, A., & Amini, F. (2014). Information security management in Isfahan University of Medical Sciences Academic Hospitals in 2014. *Int Journal Health System Disaster Management*, 2(3), 175-179.

Tengilimoğlu, D., & Çıtak N. (2003). *Yönetici ve Tıp Sekreterliği.* Ankara: Seçkin Yayıncılık.

Tengilimoğlu, D., Işık, O., & Akbolat M. (2017). *Sağlık İşletmeleri Yönetimi*. (8.Basım), Nobel Yayıncılık, Ankara.

Terlemez, B., Şahin D., & Dilek, F. (2014). Namık Kemal Üniversitesi Sağlık Uygulama ve Araştırma Merkezindeki tıbbi sekreterler ve idari personelin bilgi ve arşiv sistemleri hakkındaki düşünceleri. *Electronic Journal of Vocational Colleges,* Bürokon Özel Sayısı, 376.

The World Health Organization (WHO) and the Pan American Health Organization. (2017). *Handbook for Electronic Health Records Implementation*. Geneva: WHO Publishing.

Vural, Y., & Sağıroğlu, Ş. (2008). Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 23(2), 507-522.

Wager, A., Lee, F., & Glaser, J. (2009). Healthcare information systems. *Jossey-Bass*, 28(29), 251-277.

Yılmaz, E., Şahin, Y. L., & Akbulut, Y. (2016). Öğretmenlerin dijital veri güvenliği farkındalığı. *Sakarya University Journal of Education*, 6(2), 26-45.

Yılmaz, H. (2014-15). TS ISO/IEC 27001 bilgi güvenliği yönetimi standardı kapsamında bilgi güvenliği yönetim sisteminin kurulması ve bilgi güvenliği risk analizi. *Denetişim*, 15, 45-59.