Evaluation of Digital Health Services From a Legal Perspective

Servet Soygüder[1*], Murat Kızılırmak[2]
[1]Ankara Yıldırım Beyazıt University
ORCID No: http://orcid.org/0000-0002-8191-6891
[2]Ankara Yıldırım Beyazıt University,
ORCID No: http://orcid.org/0009-0008-2359-1866

Anahtar Kelimeler

Sağlık, Dijital Sağlık, Dijital Sağlık Uygulamaları, Hukuki Altyapı,

Öz

Günümüzde sağlık sektörü, teknolojik ilerlemelerle birlikte dijitalleşme sürecine hızla adapte olmaktadır. Bu dijital dönüşüm, sağlık hizmetlerini iyileştirmeyi ve etkinleştirmeyi amaçlayan birçok avantajı beraberinde getirirken, aynı zamanda ciddi hukuki zorlukları da beraberinde getirmektedir. Bu makale, dijital sağlık ve hukuk arasındaki kritik ilişkiyi ele alarak, dünya genelinde sağlık sektörünün dijitalleşme sürecini incelemeyi amaçlamaktadır. Aynı zamanda dünya çapında aktif olarak kullanılan dijital sağlık uygulamalarının hem web hem de mobil platformları kapsamlı bir şekilde incelenmiş ve irdelenmiştir. Yapılan araştırmalarda; bu uygulamaların temel işlevselliği, randevu sistemleri, ödeme sistemleri ve özellikle hukuki alt yapıları ele alınmıştır. Bu çalışmada dijital sağlık uygulamalarının sunduğu hizmetlerin detaylı analizini, kullanıcı deneyimlerini, veri güvenliğini ve hukuki uyumluluk açılarını kapsamlı bir bakış açısı sunmayı amaçlamaktadır. Dijital sağlık alanında faaliyet gösteren özel ve devlet kurumlarının ve sağlık profesyonellerinin, bu karmaşık düzenlemelere uyum sağlamak için benimsemeleri gereken en iyi uygulamaları anlamak, makalenin temel hedeflerindendir.

Evaluation of Digital Health Services From a Legal Perspective

Keywords

Health, Digital Health, Digital Health Applications, Legal Framework

Abstract

In today's world, the healthcare sector is rapidly adapting to the process of digitization with technological advancements. While this digital transformation brings numerous advantages aimed at improving and streamlining healthcare services, it also presents significant legal challenges. This article aims to examine the critical relationship between digital health and law, intending to explore the global digitization process in the healthcare sector. Additionally, it comprehensively investigates both web and mobile platforms of digital health applications actively used worldwide. In the conducted research, the fundamental functionality of these applications, appointment systems, payment systems, and especially their legal frameworks are addressed. This study aims to provide a comprehensive perspective on the detailed analysis of the services offered by digital health applications, user experiences, data security, and legal compliance aspects. Understanding the best practices that private and public institutions and healthcare professionals operating in the digital health field need to adopt to comply with these complex regulations is a fundamental goal of the article.

Araştırma Makalesi		Research Article	
Başvuru Tarihi	: 01.06.2024	Submission Date	: 01.06.2024
Kabul Tarihi	: 22.10.2024	Accepted Date	: 22.10.2024

1. INTRODUCTION

Developments in technology and decreasing costs have increased individuals' access to technological tools and applications. This easy access to technology has enabled people to carry out their activities in the digital environment with computers, smart mobile phones, tablets, and other systems and tools that help access necessary services without being physically present (Demirci, Ş. 2018). Digital technologies affect many issues such as the way people live, what they do in their spare time, how they work, their relationships with other people and the way they think.

1

[1] Resp author; e-mail: servetsoyguder@gmail.com

Digital technologies, which affect many sectors in addition to their impact on humans, have a profound impact, especially on the healthcare sector (Dorn, 2015). Digital health technologies are defined as systems and tools that enable individuals to control their own health status, comply with treatment protocols, encourage preventive health activities, and strengthen communication between the individual and the healthcare professional. These technologies include applications such as the internet, mobile technologies, social networks, and e-mail. Digital health differs slightly from traditional healthcare settings and focuses on data management, mobile technologies and communication tools rather than complex equipment. These technologies include genetic mapping, digital medical imaging devices and various digital health applications aimed at improving human health. Digital technologies aim to create an integrated healthcare system between patients, healthcare professionals, stakeholders and companies by redefining the boundaries in the healthcare system. However, in this digitalization process, the role played by law is often overlooked. Digital transformation in the healthcare sector brings with it a number of complex legal issues such as data security, patient privacy, medical device regulations and telemedicine. Digital health law is constantly evolving to respond effectively and fairly to the challenges posed by technological advances in the healthcare industry. It has been determined in the literature that many studies have been carried out in this field. The article prepared by Özen aims to examine the impact and contributions of telemedicine and mobile health services, which are among the digital health applications and are becoming increasingly widespread in Turkey, to the United Nations' Sustainable Development Goals (Ozen, 2021). In their study, Yorulmaz, Odacı and Akkan emphasized the prevalence and importance of the e-pulse system in health services and aimed to determine the importance and usage of the e-pulse system in health services in Turkey by examining the awareness levels and e-pulse usage of citizens in Konya. (Yorulmaz, Odacı & Akkan, 2018). In his study, Toygar talked about the historical background and developments of E-health applications. (Toygar, 2018). In their studies, Avaner and Fedai focus on health information systems implemented in Turkey. Particularly, the duo touched upon the importance of digitalization in healthcare in terms of decision support processes. (Avaner & Fedai, 2018). In their work, Şimşir and Mete discuss the role of innovative digital technologies in medicine and what these technologies are to improve the quality of treatment. (Simsir & Mete, 2021). In their study, Akalın and Veranyurt emphasize the various advantages and disadvantages of artificial intelligence applications in the healthcare sector. The study also recommends that necessary legal regulations be made in the use of artificial intelligence applications. (Akalın & Veranyurt, 2021). In their studies, Uysal and Ulusinan examine the impact of concepts such as mobile health, artificial intelligence, digital hospital, which are included in the concept of e-health, on healthcare services and provide examples. (Uysal & Ulusinan, 2020). In his study, Küzeci evaluated the legal problems arising from the innovations brought by e-health applications. (KUzeci, 2018).

They discuss certain key legal structures that digital health companies and investors should consider and emerging legal trends affecting digital health practices in the United States (“US”), the European Union (“EU”), and the United Kingdom. (ICLG, 2023). In their study, Karaca,

Özsal and Duru examined the factors in the adoption of health care services offered using telehealth applications by healthcare personnel. (Karaca, Özsal & Duru, 2022).

Due to Covid-19, US President Donald Trump mentioned in his announcement on March 17, 2020 that he would expand telehealth services for patients with online applications to promote social distance. (Global News, 2020). While Mengi talks about making the internal control structures in health systems more reliable in his study, he also mentions that biometric systems should be switched to this system because they are more reliable than other systems. (Mengi, 2013). In their studies, Aladağ, Kurtarangil, and Bahtiyar talked about authentication methods that can be used to protect confidentiality due to security vulnerabilities in information systems. (Aladag, Kurta-Rangil & Bahtiyar, 2014). Tuckson, Edmunds and Hodgkins explained telehealth comprehensively in their studies. In their study, they talk about nine basic aspects of service delivery and also make suggestions as a result of implications for future research. (Tuckson, Edmunds & Hodgkins, 2017). Finally; In his study, Doğramacı talks about the meanings of the term telemedicine in different countries. While talking about the development of the concept of telemedicine in accordance with its chronological order in the world, he examined the history of telemedicine in Turkey separately. In addition, while talking about the areas where telemedicine is applied and the benefits it brings, he also examined its legal infrastructure. (Doğramacı, 2020).

2. DIGITAL HEALTH LAW

Digital health includes many areas such as the provision of health services, management of personal data and the use of health technologies. In parallel with the advancement of digital health technology, digital health law has also developed. Digital health law is a special field of law that emerged with the technological developments in the health sector and the spread of digital health applications. Digital health faces different legal challenges. The first of the most important issues is the privacy and security of personal data. The use, sharing and storage of digital health data created electronically should be well managed from a legal perspective. Another important legal issue is the consideration of digital health applications such as telemedicine. Telemedicine is a method that enables patients to receive services remotely from healthcare professionals, and this brings about legal regulations to determine the boundaries and legal standards of medical practices. Digital health law; It incorporates many regulations and standards such as medical device security, patient rights, data security standards, and aims to create a reliable framework in the sector by determining the compliance and responsibilities of healthcare providers and digital health technology providers.

Keeping up with rapidly developing technology and updating the legal framework of these new technologies is a process that requires constantly staying up to date. Towards the end of the 1960s, with the introduction of computer technology into the health sector, digital health law began to lay its foundations. During this period, computers began to be used in administrative tasks such as hospital management and financial transactions. However, in these early applications, legal regulations were generally inadequate and specific legal standards regarding digital health had not yet been established. The 1980s and 1990s were a period when digital health law began to take shape. During this period, Electronic Health Records (EHR) and other

information systems began to become widespread. The healthcare industry has begun to take steps to create regulatory frameworks on issues such as hospital information systems and patient information security. In the 2000s, the rapid development of the internet and mobile technologies made digital health law even more important. Sharing personal health information in electronic environments has created the need to protect the privacy of patients and determine the responsibilities of healthcare providers. During this period, legal regulations for digitalization in the healthcare sector began to increase around the world. Regulations in the field of law aim to ensure that both healthcare professionals and patients feel safe in the digital health environment. Digital health law in Turkey includes practices and legal orders regulating the use of technology, data security, and patient rights. Some important digital health law regulations in Turkey are as follows;

Electronic Health Services: Here, electronic health records, digital storage of patient data, digital prescription applications, etc. Includes topics.

Access to Information: Includes the right to obtain information regarding access to and sharing of health data.

Processing and Privacy of Personal Health Data: It determines the rules regarding the processing, storage and sharing of personal health data. Protection of personal data is important.

Electronic Signature: Includes the importance of electronic signature to ensure authentication and security in digital health services.

Collection of Personal Data: It includes obtaining the necessary information to ensure correct service delivery.

3. COLLECTED PERSONAL DATA AND COLLECTION METHODS

Personal data can be collected from the service application in various ways. Personal data is not collected unless voluntarily provided directly by the customer or through authorized representatives.

If the personal data collected needs to be divided into 2 stages, it may be in the table below;

3.1. How is Personal Information Collected?

- If a comment is published,
- Automatically (such as from cookies) when you visit sites or use services
- Such as when you participate in telehealth services and/or interact with in-app messaging services.
- From third parties (when payment is made using the payment processor)
- Can be collected by the customer verbally or through applications and forms.
- Identity information, e-mail address, financial information and relevant information required to complete the health record in order to benefit from its services.

- Create and maintain a record of care and services received. This may include electronic medical records, if available, audio and/or video files of consultations, and test results.
- From programs such as Microsoft HealthVault or Google Health,
- Information provided from smart devices,
- Location from GPS-enabled devices,
- Automatically over time and from our own and third-party websites, through tracking technologies such as cookies,
- The Websites may use Google Analytics to collect and store information about you.

3.2. Cookies

Cookies are small pieces of information created when you visit a website. These are used to collect and store certain information about your interactions with the website, which we can later use to make your journey better. We can remove cookies from our computer at any time, and we also have the opportunity to choose to disable cookies from the settings of our internet browser.

Session cookies are temporary cookies that exist only for the duration of using the Website. Session cookies help the Website remember what was selected on the previous page, eliminating the need to re-enter information.

Persistent cookies are a type of cookies that are saved on the device after visiting the Website. For example, when you log in to the GPS System, a permanent cookie is created to remember the preferences so that the system remembers the selection the next time you log in.

Advertising Cookies: Used to personalize advertisements. They share information by remembering the sites you visit.

Performance Cookies: These cookies help understand site access, browsing habits and usage. This data does not contain personal information that could reveal individual identity.

4. USE AND PURPOSE OF PERSONAL INFORMATION

Uses personal information for service delivery, personalization, security and legal requirements.

4.1. Offering Our Services

- To manage your account, provide and personalize our services and process payments
- Providing customer support
- Providing information about services to the customer

4.2. Personalizing Your Experience

- To improve users' experiences, both in terms of content and ease of use

- To adjust ads to attract customer's attention

4.3. Marketing

Where you have given your express consent, we may use your personal information to inform you about services, including products, promotional offers and events.

4.4. Other Situations

- Track and monitor user interaction
- Ensuring the security of services
- To fulfill legal obligations
- To detect, prevent or investigate security violations,
- Payment information to carry out insurance and credit card transactions,
- Authentication,
- Creating de-identified information (e.g. statistics, market research)
- To convey health information to the customer (himself),

5. USE AND DISCLOSURE OF PERSONAL DATA

They have the right to notify employers, insurers and healthcare providers regarding medical care requests. Unauthorized use is not possible except where required by law. Consent is obtained before personal data is collected and used without permission.
They may collect, use and disclose personal data without permission, based on the 'legitimate interests' exception under the KVKK, in order to detect and prevent fraud and misuse of services. In such cases, relevant explanations will be made to the insurer or employer (DoctorAnywhere,).

5.1.Sharing Your Personal Information

Personal Information is not licensed or disclosed to unaffiliated third parties except in cases of sale, legal requirements, transfer or merger of the company.
We may share Personal Information with third parties, including service providers, in certain situations or for certain purposes, including:

- It must be shared with general practitioners and medical team in order to provide the service.
- The e-mail, date of birth and contact information provided during website registration can be shared with professional consultants such as analysis advertising services and law firms.
- Personal Information may be shared with third parties upon request.
- May share personal information with affiliates in the corporate group.
- May share to comply with laws or obligations under these laws.
- Personal Information may be shared in connection with an asset sale, merger, bankruptcy or other business transaction.
- For advertising (as described in the cookies section)

- Additionally, de-identified information may be disclosed in order to perform analysis activities.
- With police, fire, ambulance and rescue services
- Public health institutions responsible for controlling infectious diseases,
- In processes within the scope of insurance
- If services are received through the ministry, information can also be shared with other institutions under the responsibility of the ministry.
- Applications that provide prescription services can be shared with pharmacies.

5.2.Purposes of Use of Shared Data

- Sharing requested information with the Ministry of Health and other public institutions and organizations,
- Fulfilling legal requirements,
- Sharing the requested information with private insurance companies within the scope of eligibility inquiry,
- Information about the appointment,
- Planning and managing the operation of the institution,
- In order to improve health services,
- Invoicing for our services,
- Confirming the relationship with contracted institutions,
- Answering questions and complaints regarding health services,
- Taking precautions within the scope of data security,
- Providing campaign information
- Measuring patient satisfaction,

6. The Storage of Personal Data

Personal information is generally stored on the secure servers of the applications. Information is stored for a certain period of time depending on the application's regulations. This period is determined by each application's own regulation. In general, data stored indefinitely in case of legal necessity is deleted automatically or upon customer request if it no longer serves its purpose.

7. Security Method and Data Protection

Each country has its own Personal Data Protection Law. To ensure the security of Personal Information, precautions are taken against accidental, illegal or unauthorized access. However, they do not fully guarantee the security of information transmitted over the internet, and the responsibility of keeping the password transmitted to the customer confidential is left entirely to the customer.

In addition, some applications in the world, such as the Neyim Var application used in Turkey, have security measures taken by the Ministry of Health of the relevant countries. Although the same methods are not applied in every application, if we talk about general precautions against duplication of disclosure;

Table 1. Security methods

Use of Firewalls, Anti-Virus Software and Data Loss Prevention	Virus Software and Data Loss Prevention
Network Security and Application Security Risks have been identified and precautions have been taken.	Risks have been identified and precautions have been taken.
Key Management Application Service providers are regularly audited.	Service providers are regularly audited.
Closed System Network Usage Personal data is reduced as much as possible.	Personal data is reduced as much as possible.
Information Technologies System Security Secure software development procedures are implemented.	Secure software development procedures are implemented.
Keeping Log Records Physical environments are secured against external risks.	Physical environments are secured against external risks.
Cloud Security The security of environments containing personal data is ensured.	The security of environments containing personal data is ensured.
Data Masking Regular training and awareness activities are carried out for employees.	Data Masking Regular training and awareness activities are carried out for employees. Regular training and awareness activities are carried out for employees.
Secure Transmission of Special Data. Commitments are made to ensure the confidentiality of the data.	Commitments are made to ensure the confidentiality of the data.
Intrusion Detection and Prevention Systems Secure Encryption/Use of Cryptographic Keys (SSL Technology)	Use of Secure Encryption/Cryptographic Keys (SSL Technology)
Cyber Security Measures Encrypted Backup	Encrypted Backup
Portable Media Encryption Account requires two-step authentication.	The account requires two-step authentication.
Keeping Access Logs	

8. ACCURACY OF PERSONAL INFORMATION

Since it is not possible to verify the information provided by customers who register on the site, application owners rely on the customer by taking the information provided by the customer as a reference. Some applications pull data from the Ministry of Health application used by countries. However, these applications generally assign responsibilities for data accuracy to the institutions and organizations that send data, healthcare personnel who enter data, people who add their own data to the system, and drug information service providers.

9. CORRECTION OF PERSONAL DATA

Generally, requests for correction of personal data are made in writing or via e-mail to the Data Protection Officers in the applications. Although this request varies on each site, the application determines an average response time of 2 weeks. This request may be paid or free of charge, depending on the application from which the service is received.

10. CHİLDREN'S PERSONAL INFORMATION AND SERVICES

In general, services are not provided to children under the age of 13. In some applications, this age goes up to 17. However, services may be provided at the discretion of the HCP (Health Care Professional).
If the child receiving the service is under the age of 18, he/she must have the permission of his/her parent or legal heir to benefit from the service.
Legal infrastructure such as the information received from individuals who have reached the age of majority, its use and sharing is valid for children as well.

11. PRESCRIPTION

The patient has a responsibility to ensure that their information is accurate and complete, and this means that the patient, knowingly or unknowingly, may influence the advice received and medications prescribed, which could lead to serious consequences. In this case, neither the system nor any doctor assumes responsibility. The patient can consult qualified doctors through online assessment surveys or secure video chat and then receive their treatments from pharmacies registered with the service. Doctors can provide documents such as prescriptions, referral letters, and notes whenever they see fit.

Due to the service of obtaining prescriptions from local pharmacies, patients have to choose e-health applications that serve in their own country, even if the applications serve in different countries.

12. EXAMINATION AND APPOINTMENT

Applications generally provide health services over the internet. As a result of the interviews, doctors state the patient's complaints and make the relevant diagnosis. Using e-health applications, especially in order to avoid wasting time, provides an advantage in this respect. Generally, these e-health services are not suitable for medical emergencies or any diagnosis or treatment that requires a physical examination.

Inspections are carried out by downloading the applications of the company to be serviced from the App Store for those who receive service from products with an iOS-based operating system, and from Google Play applications for those who receive service from products with an Android-based operating system. These services can be in the form of voice chat, video chat and messaging. At the same time, while some sites can receive service through their own sites, they also provide this service by using applications such as WhatsApp, Zoom, etc. One of the most important issues that should be taken into consideration here is that the services provided must be recorded or the legal infrastructure must be thoroughly learned. If you want to take legal action in the future in case of a misdiagnosis, your probability of being right without any evidence is almost zero. According to the information we received from WhatsApp, Audio and video calls on WhatsApp are end-to-end encrypted. Thus, whether you make calls from your phone or your computer, "WhatsApp cannot listen to or see these calls." is an indication that we cannot claim rights.

13. CONCLUSION AND DISCUSSION

Data regarding the collection of personal data is conveyed above under the title "Collected Personal Data and Collection Methods". The conclusion to be drawn here is that data is collected by different methods and it is possible to partially block these methods. It is envisaged that this can be prevented by restricting the cookies section, but blocking or restricting personal information also restricts the service received. Because customer data is needed for the service.

The user cannot do much about sharing personal data; any security weakness means that the information will be used by a third person or institution. In today's age, especially services received over the internet, applications with weak cyber security measures cause data to be shared with a third party. Therefore, it brings with it the obligation to thoroughly research the data security policy of the application to be serviced and the methods applied for data protection. Although data is protected by law, it should not be forgotten that it can also be shared through illegal means. The accuracy of personal data is parallel to the accuracy of the service received. Therefore, users who will provide health services via the internet or mobile should add this data to the system carefully and accurately. As mentioned above, the information entered mostly holds the user responsible, not the application owner. Although it is possible to correct incorrectly entered information, this may cause loss of both time and money.

If the user accepts a service over the internet, he/she should especially read the terms of acceptance carefully. While some practices do not offer prescription services, some do. The most important part here is "Please note that Evital does not and will not give any medical advice through the Platform, does not aim to give medical advice, and does not provide guidance or recommendations regarding any diagnosis, prognosis or treatment", which I encountered while researching different applications (Evital, 2023). This article is an example of how careful we should be in this regard. Choosing companies that carry out the necessary procedures and provide approved digital health services in accordance with the regulations published in the official gazette in Turkey will increase the quality of the service received. By carelessly accepting this and similar articles before receiving service, while you think you are

being treated, you are actually admitting that you are not legally receiving a service in exchange for money. The use of e-health applications has increased significantly today, especially due to expensive healthcare expenses in other countries. In addition to providing financial profit, these applications also provide significant benefits in terms of time. The examination, which will be carried out online, allows patients to receive service regardless of where or when they are.

14. CONFLICT OF INTEREST

The authors declared that there is no conflict of interest.

REFERENCES

Akalin, B., & Veranyurt, U. (2021). Saglik Hizmetleri ve Yonetiminde Yapay Zeka. Acta Infologica, 5(1), 231-240.

Aladag CE, Kurtarangil E, Bahtiyar S. (2014). Medikal bilgi sistemlerinde güvenlik, mahremiyet ve kimlik dogrulama. XVI. Akademik Bilisim Konferansı Bildirileri, 313-317.

Avaner, T., & Fedai, R. (2017). Saglik Hizmetlerinde Dijitallesme: Saglik Yönetiminde Bilgi Sistemlerinin Kullanilmasi. Suleyman Demirel universitesi Iktisadi Ve Idari Bilimler Fakultesi Dergisi, 22(Kayfor 15 Ozel Sayisi), 1533-1542.

Demirci, S. (2018). Sagligin Dijitallesmesi, Mehmet Akif Ersoy Universitesi Sosyal Bilimler Enstitusu Dergisi, 10, 710-721.

DoctorAnywhere "Gizlilik Ve Veri Koruma Politikası ("Gizlilik Politikası")". (2023). DoctorAnywhere - Gizlilik Politikası

Dogramacı YG. (2020). Teletip, Saglık Turizmi ve Uzaktan Saglik Hizmetleri: Mesafeli Sozlesmeler. İstanbul Hukuk Dergisi, 78(2), 657-710

Dorn, S. D. (2015). Digital Health: Hope, Hype, and Amara's Law. Gastroenterology, 149(3), 516-520.

Evital "Evital - Danışan Odaklı E-Saglık Platformu Ve Web/Mobil Uygulamaları Platformu Kullanım Hukum Ve Kosulları". (2023). (Evital - Kullanıcı Hüküm ve Koşulları

Global News, "A Division of Corus Entertaintment Inc. Coronavirus outbreak: Trump announces expansion of medicare telehealth services amid pandemic."., Global News

ICLG "Dijital Saglik Yasaları ve Duzenlemeleri Kuresel Dijital Saglik Duzenlemesinde Ortaya Cikan Egilimler 2023-2024"., ICLG - Dijital Saglik Yasaları

Karaca A, Orsal O, Duru P. (2022). Facilitators and barriers to healthcare professionals' adoption of tele-health interventions. J Nursology. 25(3), 168-176.

Kuzeci, E. (2018). Saglik Bilisim Teknolojileri Ve Yeni Hukuksal Soru(N)Lar. Inonu Universitesi Hukuk Fakultesi Dergisi, 9(1), 477-506.

Mengi, B. T. (2013). Saglık Hizmetlerinde Meydana Gelebilecek Hileleri Onlemeye Yonelik Bir Uygulama Olarak Biyometrik Kimlik Dogrulama Sistemlerinin Kullanımı. Muhasebe Ve Finansman Dergisi, (60), 39-50.

Özen, H. (2021). Dunya Saglik Hizmetlerinin Surdurulebilir Kalkınma Hedefleri Acısından Degerlendirilmesi. OPUS–Uluslararası Toplum Arastırmaları Dergisi, 17(38), 5440-5472.

Simsir,I., Ve B. Mete, "The Future of Healthcare Services: Digital Health Technologies", Journal of Innovative Healthcare Practices, c. 2, sy. 1, ss. 33–39, 2021.

Uysal, B., & Ulusinan, E. (2020). Guncel Dijital Saglik Uygulamalarının Incelenmesi. Selcuk Saglik Dergisi, 1(1), 46-60.

Toygar, Ş. A. (2018). E-Saglık uygulamalari. Yasama Dergisi (37), 101-123

Tuckson RV, Edmunds M, Hodgkins ML. (2017). Telehealth. N Engl J Med, 377(16),1585-1592.

Yorulmaz M & Odaci Ş. & Akkan M. (2018). Dijital Saglık Ve E-Nabiz Farkindalik Duzeyi Belirleme Calismasi. Selcuk Universitesi Sosyal ve Teknik Arastirmalar Dergisi, 16, 1-11