TÜRKİYE CUMHURİYETİ
MARMARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

SAĞLIK YÖNETİMİNİN GELECEKTEKİ PAYDAŞLARINDAN BİLGİSAYAR MÜHENDİSLİĞİ ÖĞRENCİLERİNİN SAĞLIK BİLGİ SİSTEMLERİNİ BİLGİ GÜVENLİĞİ VE HASTA MAHREMİYETİ AÇISINDAN DEĞERLENDİRMESİ

ESRA SEVİMLİ

YÜKSEK LİSANS TEZİ

SAĞLIK YÖNETİMİ ANABİLİM DALI

DANIŞMAN

PROF. DR. GONCA MUMCU

2018 - İSTANBUL

TEZ ONAYI

Kurum : Marmara Üniversitesi Sağlık Bilimleri Enstitüsü

Programın seviyesi : Yüksek Lisans

Anabilim Dalı : Sağlık Yönetimi

Tez Sahibi : Esra SEVİMLİ

Tez Başlığı : Sağlık Yönetiminin Gelecekteki Paydaşlarından Bilgisayar Mühendisliği Öğrencilerinin Sağlık Bilgi Sistemlerini Bilgi Güvenliği ve Hasta Mahremiyeti Açısından Değerlendirmesi

Sınav Yeri : M.Ü. Sağlık Bilimleri Fakültesi, Sağlık Yönetimi Anabilim Dalı

Sınav Tarihi : 01.03.2018

Tez tarafımızdan okunmuş, kapsam ve kalite yönünden Yüksek Lisans Tezi olarak kabul edilmiştir.

Danışman (Unvan, Adı, Soyadı)	**Kurumu**	**İmza**
Prof. Dr. Gonca MUMCU	M.Ü. Sağlık Bilimleri Fakültesi, Sağlık Yönetimi Bölümü	
Sınav Jüri Üyeleri (Unvan, Adı, Soyadı)		
Prof. Dr. Mehveş TARIM	M.Ü. Sağlık Bilimleri Fakültesi, Sağlık Yönetimi Bölümü	
Doç. Dr. Gülfer BEKTAŞ	Acıbadem Üniv. Sağlık Bilimleri Fakültesi, Sağlık Yönetimi Bölümü	

Yukarıdaki jüri kararı Enstitü Yönetim Kurulu'nun 15/03/2018 tarih ve 35 sayılı kararı ile onaylanmıştır.

Prof. Dr. Göksel ŞENER

Sağlık Bilimleri Enstitüsü Müdürü

-Sınav evrakları 3 iş günü içinde ıslak imzalı tek kopya halinde Enstitüye teslim edilmelidir.
-Bu form bilgisayar ortamında doldurulacaktır.

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün safhalarda etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara kaynak gösterdiğimi ve bu kaynakları da kaynaklar listesine aldığımı, yine bu tezin çalışılması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığı beyan ederim.

Esra SEVİMLİ

TEŞEKKÜR

Tezimin konusunun belirlenmesi ve yürütülmesinde yardımlarını esirgemeyen, görüş ve önerileriyle beni sürekli destekleyen değerli danışmanım Sayın Prof. Dr. Gonca MUMCU'ya sonsuz teşekkürlerimi sunarım.

Ayrıca her zaman yanımda olan kıymetli aileme; tez süreci boyunca görüşlerinden yararlandığım değerli hocalarım Yrd. Doç. Dr. Leyla KÖKSAL'a, Yrd. Doç. Dr. Pınar KILIÇ AKSU'ya, Yrd. Doç. Dr. Nur ŞİŞMAN KİTAPÇI'ya, Dr. Okan Cem KİTAPÇI'ya ve istatistik bilgilerini benden esirgemeyen değerli dostum Aysun KÖRLÜ'ye sonsuz teşekkürlerimi sunarım.

Esra SEVİMLİ

İÇİNDEKİLER

Sayfa No

KISALTMALAR ve SİMGELER

AHBS	Aile Hekimliği Bilgi Sistemi
DDK	Devlet Denetleme Kurulu
ESK	Elektronik Sağlık Kaydı
HBYS	Hastane Bilgi Yönetim Sistemi
HIPAA	Health Insurance Portability and Accountability
MHRS	Merkezi Hastane Randevu Sistemi
MSVS	Minimum Sağlık Veri Setleri
SDP	Sağlıkta Dönüşüm Programı
SGK	Sosyal Güvenlik Kurumu
TSBS	Türkiye Sağlık Bilgi Sistemi
USVS	Ulusal Sağlık Veri Sözlüğü

TABLOLAR

SAĞLIK YÖNETİMİNİN GELECEKTEKİ PAYDAŞLARINDAN BİLGİSAYAR MÜHENDİSLİĞİ ÖĞRENCİLERİNİN SAĞLIK BİLGİ SİSTEMLERİNİ BİLGİ GÜVENLİĞİ VE HASTA MAHREMİYETİ AÇISINDAN DEĞERLENDİRMESİ

Esra SEVİMLİ

Danışman: Prof. Dr. Gonca MUMCU

Sağlık Yönetimi Anabilim Dalı

ÖZET

Amaç: Bu araştırmada; sağlık yönetiminin gelecekteki paydaşlarından olan Bilgisayar Mühendisliği öğrencilerinin, sağlık bilgi sistemlerinin bilgi güvenliğini ve hasta mahremiyetini değerlendirmesi amaçlanmıştır.

Gereç ve Yöntem: Bu kesitsel araştırmaya, Marmara Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği bölümü 3. ve 4. sınıf öğrencileri (n=163, K/E:71/92) ve Tıp Fakültesi 5. ve 6. sınıf öğrencileri (n=65, K/E:38/27) katılmıştır. Veriler anket formu ile toplanmıştır.

Bulgular: *"Doktordan başka bir sağlık çalışanının sağlık kayıtlarına erişiminden"* Bilgisayar Mühendisliği öğrencilerinin (%93,3); Tıp öğrencilerine (%78,5) göre daha fazla rahatsız olduğu belirlenmiştir (p=0.003). Benzer şekilde Bilgisayar Mühendisliği öğrencileri (%87,1); Tıp öğrencilerine göre (%66,2) *"Doktor ile elektronik ortamda daha fazla iletişim kurmayı"* istemektedir (p=0.001). Bilgisayar Mühendisliği (%40,5) ve Tıp öğrencileri (%35,4) elektronik sağlık kayıt sistemi üzerinden *''İletişim bilgilerinin''* erişiminin kısıtlanmasını istemektedir (p>0.05).

Sonuç: Bilgisayar Mühendisliği öğrencileri, sağlık yönetiminin multidisipliner yapısı içinde gelecekteki hem iç hem dış paydaşlardandır. Sağlık bilgi sistemlerinde güvenlik ve mahremiyet ile ilgili sorunların olabileceğini düşünmektedirler. Bilgisayar Mühendisliği öğrencilerinin sağlık hizmetleri ile mesleki eğitimleri arasındaki ilişki, sağlık yönetimi perspektifinden oldukça önemlidir.

Anahtar Kelimeler: Bilgi Güvenliği, Hasta Mahremiyeti, Sağlık Bilgi Sistemleri

THE EVALUATION OF INFORMATION SECURITY AND PATIENT PRIVACY OF HEALTH INFORMATION SYSTEMS IN COMPUTER ENGINEERING STUDENTS FROM FUTURE STAKEHOLDERS OF HEALTH MANAGEMENT

Esra SEVİMLİ
Consultant: Prof. Dr. Gonca MUMCU
Department of Health Management

SUMMARY

Aim: The aim of this study was to evaluate information security and patient privacy of health information systems in Computer Engineering (CE) students from future stakeholders of health management.

Materials and Method: In this cross-sectional study, Engineering Faculty, 3rd and 4th grade students of CE (n=163, F/M: 71/92) and 5th and 6th grade students of School of Medicine (n=65, F/M:38/27) in Marmara University were included. Data were collected by a questionnaire.

Results: CE students (93,3%) were more uncomfortable *"access to health records to other health workers than physicians"* compared to medical students (78,5%) (p=0.003). Similerly, they (87,1%) *''wanted to communicate more with the physicians via the electronic environment''* (87,1%) than medical students (66,2%) (p=0.001). CE (40,5%) and medical students (35,4%) wanted to restrict access to *''contact information''* in the health information system (p>0.05).

Conclusion: Computer Engineering students are future internal and external stakeholders within the multidisciplinary structure of health managemet. They thought that some security and privacy related problems could be present in health information system. In Computer Engineering students, the relationship between health services and their vocational training is very important for the perspective of health management.

Key Words: Information Security, Patient Privacy, Health Information Systems

GİRİŞ ve AMAÇ

Günümüzde tüm kurumlar gibi sağlık kurumları da verilerini elektronik ortamda bulundurmakta ve bu verileri bilgi sistemleri alt yapısı kullanarak işlemektedir. Bu açıdan sağlık bilgi sistemleri, sağlık alanında yer alan tüm kullanıcılar için önemli avantajlar sağlamaktadır. Ancak zamanla sağlık alanında derlenen veri miktarının artması ve verilere birçok kullanıcının kolaylıkla ulaşması, bilgi güvenliği ve mahremiyet ihlallerini de beraberinde getirmiştir.

Sağlık verileri, kişisel ve son derece hassas olduğu için sağlık bilgi sistemlerinde bilgi güvenliğinin sağlanması ve hasta mahremiyetinin korunması oldukça önemlidir.

Bilgisayar Mühendisliği öğrencileri, sağlık hizmetlerinin multidisipliner yapısı içinde gelecekteki hem iç hem dış paydaşlardandır. Bu grubun sağlık hizmetleri ile mesleki eğitimlerini ilişkilendirebilmeleri, sağlık yönetimi perspektifinden oldukça önemlidir.

Sağlık hizmetlerinin sunumundaki multidisipliner yaklaşım açısından, sağlık yöneticilerinin paydaşların görüş ve önerilerini dikkate almaları gerekmektedir. Bu araştırmada; sağlık yönetiminin gelecekteki paydaşlarından olan Bilgisayar Mühendisliği öğrencilerinin, sağlık bilgi sistemlerinin bilgi güvenliği ve hasta mahremiyeti hakkında görüşlerinin değerlendirilmesi amaçlanmıştır.

1. SAĞLIK HİZMETLERİ ve SAĞLIK YÖNETİMİ

1.1. Sağlık Kavramı ve Sağlık Hizmetleri

Sağlıklı olma ve sağlıklı bir çevrede yaşama hakkı, temel insan haklarının başında gelmektedir. Söz konusu bu temel insan hakkının, günümüzdeki içeriğinden farklı olsa da insanlık tarihi kadar eski bir geçmişi vardır. Bu konuda en iyi bilinen örnek Hammurabi Kanunlarıdır. M.Ö. 2000 yılında yaşayan Babil Kralı Hammurabi, kendi adıyla anılan kanunlarda, sağlık hizmetlerinin sunumunda hekimlerin alacağı sorumlulukları ve hizmet sonucunda elde edecekleri ödülleri belirlemiştir (Kavuncubaşı ve Yıldırım 2015, s.17).

Sağlık kavramı, geleneksel anlamda ‘‘hastalığın olmayışı’’ şeklinde tanımlanmıştır. Tanımın bu şekilde yapılması ‘‘hastalık’’ kavramını ön plana çıkarmış ve bu durum kişilerin ve toplumların sağlığının bu kavrama bağlı olarak değerlendirilmesi gerekliliğini doğurmuştur (Akdur 1999, s.4). Ancak hastalık kavramı kişiye, zamana ve topluma göre değişmektedir. Kendinde veya toplumunda hastalık bulunduğu halde, bunu hastalık olarak kabul etmeyen kişi ve toplumlar, kendilerini sağlıklı olarak değerlendirebilmektedir. Bu sebepten ötürü, ‘‘sağlığı’’, ‘‘hastalığın olmayışı’’ şeklinde tanımlamak yeterli olmamaktadır (Akdur 2006, s.17). Sağlığın farklı şekillerde birçok tanımı bulunmasına rağmen, bunlar arasında en çok kabul gören Dünya Sağlık Örgütü’nün (WHO) kuruluş yasasında yer alan tanımıdır. Bu tanıma göre, *‘‘Sağlık, sadece hastalık ve sakatlık halinin olmayışı değil, bedensel, ruhsal ve sosyal yönden tam iyilik hali’’* dir (http://www.who.int/en/, e.t:29.11.2016; Hayran 1998, s.3).

Sağlık çok boyutlu bir kavramdır ve birbiri ile ilişkili birçok faktörlerden etkilenmektedir. Sağlığı etkileyen unsurlar dört ana grupta toplanmaktadır. Bunlar; yaşam tarzı, çevre, kalıtım ve sağlık hizmetleri şeklinde sınıflandırılmaktadır (Somunoğlu 2012, s.6). Sağlığı etkileyen bu unsurlardan en önemli etken ‘‘çevre’’ dir. Bu durumu sırası ile ‘‘yaşam tarzı’’, ‘‘kalıtım’’ ve ‘‘sağlık hizmetleri’’ izlemektedir (Bekaroğlu 2011, s.164). Sağlığı etkileyen bu dört temel unsur; ekonomik, kültürel, politik, nüfus, tutum-davranış, doğal kaynaklar gibi faktörlerin

etkisi altında kalmaktadır. Örneğin sigara içme alışkanlığı, beslenme tarzı gibi davranışlar, içinde yaşanılan kültürel koşullardan etkilenmekte ve bu durum kişilerin sağlık statüsünde farklılıklar yaşamasına sebep olmaktadır (Somunoğlu 2012, s.6).

224 sayılı Sağlık Hizmetlerinin Sosyalleştirilmesi Hakkında Kanun'da sağlık hizmetleri; *''İnsan sağlığına zarar veren çeşitli faktörlerin yok edilmesi ve toplumun bu faktörlerin tesirinden korunması, hastaların tedavi edilmesi, bedeni ve ruhi kabiliyet ve melekeleri azalmış olanların işe alıştırılması (rehabilitasyon) için yapılan tıbbi faaliyetler''* şeklinde tanımlanmaktadır (T.C. Resmi Gazete, 12 Ocak 1961, Sayı:10705).

Ülkemizde, 1982 Anayasasının 56. Maddesinde sağlık hakkının talep edilebilme yönüne yer verilmiştir: *''Herkes sağlıklı ve dengeli bir çevrede yaşama hakkına sahiptir. Çevreyi geliştirmek, çevre sağlığını korumak ve çevre kirlenmesini önlemek Devletin ve vatandaşın görevidir. Devlet herkesin hayatını, beden ve ruh sağlığı içinde sürdürmesini sağlamak; insan ve madde gücünde tasarruf verimini arttırarak, işbirliğini gerçekleştirmek amacıyla sağlık kuruluşlarını tek elden planlayıp hizmet vermesini düzenler. Devlet, bu görevini kamu ve özel kesimlerdeki sağlık ve sosyal kurumlardan yararlanarak, onları denetleyerek yerine getirir. Sağlık hizmetlerinin yaygın bir şekilde yerine getirilebilmesi için kanunla genel sağlık sigortası kurulabilir''* (https://www.tbmm.gov.tr/anayasa/anayasa_2011.pdf, e.t:01.12.2016). Devletin bu alandaki çalışmaları ''sağlık hizmetlerini'' oluşturmaktadır (Sert 2007, s.41-42).

''Sağlık hakkı'' veya daha açık haliyle mümkün olan en yüksek bedensel ve ruhsal sağlık standardına sahip olma hakkı, uluslararası hukukla korunan temel bir insan hakkıdır (Zengin 2010, s.44). Kişinin temel hakları arasında yer alan ''yaşama hakkını'' tamamlayan en önemli haklardan biri olan ''sağlık hakkına'' uluslararası insan hakları belgelerinde önemle yer verilmiştir (Sert vd. 2011, s.489).

Sağlık hizmetleri en genel anlamıyla, hastalıkların teşhis, tedavi ve rehabilitasyonu yanında, hastalıkların önlenmesi, toplum ve bireyin sağlık düzeyinin geliştirilmesi ile ilgili faaliyetler bütünü anlamına gelmektedir. Toplum sağlığının korunması, geliştirilmesi, hastalıkların teşhis, tedavi ve rehabilitasyonu amacıyla sağlık kurumları ve sağlık çalışanları tarafından sunulan hizmetlerdir (Kavuncubaşı ve Yıldırım 2015, s.40). Bu hizmetler; ana-çocuk sağlığı ve aile planlaması, sağlığın

korunması ve geliştirilmesi, sağlıkla ilgili yaşam kalitesinin yükseltilmesi, çevre sağlığı hizmetleri gibi konuları kapsamaktadır (Somunoğlu 2012, s.8). Kişilerin sağlığının korunması ve yaşamlarına sağlıklı bir şekilde devam etmelerinin sağlanmasında, devlet birinci derecede rol oynamaktadır. Devlet bu bağlamda önlemler almak, gerekli kurum ve kuruluşları oluşturmak ve bunları denetlemek zorundadır Sert 2008, s.26).

1.2. Sağlık Hizmetlerinin Özellikleri

Sağlık hizmetleri, diğer mal ve hizmetlere göre birtakım farklı niteliklere ve özelliklere sahiptir. Sağlık hizmetlerinin kendine özgü bu özelliklerini aşağıdaki gibi sıralayabiliriz (Kavuncubaşı ve Yıldırım 2015, s.125-130):

- Sağlık hizmetlerinde üretim ve tüketim aynı anda gerçekleşmektedir. Yani hizmet üretildiği anda tüketilir,
- Diğer sektörlerin aksine, sağlık hizmetlerinde üretimin depolanması (stoklanması) olanaklı değildir,
- Sağlık hizmetlerinde arz ve talep eşitsizliği ve bilgi asimetrisi söz konusudur,
- Gelişmiş teknik donanım kullanmalarına rağmen sağlık hizmetleri emek yoğun bir özelliğe sahiptirler,
- Verilen hizmetler, hata ve belirsizliklere karşı oldukça duyarlıdır ve tolerans gösteremez,
- Sağlık hizmetlerinde gerçekleştirilen etkinliklerin büyük kısmı acil ve ertelenemez niteliktedir.

1.3. Sağlık Hizmetlerinin Sınıflandırılması

Sağlık hizmetleri bir bütün olmakla birlikte anlaşırlığını kolaylaştırmak amacıyla üç ana bölümde incelenmekte ve gruplandırılmaktadır (Akdur 2006, s.17-20; Hayran 1998, s.17-19; Kavuncubaşı ve Yıldırım 2015, s.40-45; Somunoğlu 2012, s.11-13). Son dönemlerde sağlığın geliştirilmesi hizmetleri de sağlık hizmetleri içinde incelenmektedir.

- **Koruyucu sağlık hizmetleri:** Koruyucu sağlık hizmetleri toplum temelli olduğu için dışsal faydası yüksek hizmetlerdir. Çevreye ve kişiye yönelik hizmetler olarak ikiye ayrılır. Kişiye yönelik olarak yapılan ilaçla ve serumla koruma, bağışıklama, aile planlaması, beslenmeyi düzenleme, kişisel hijyen, hastalıkların erken tanı ve tedavisi, ana çocuk sağlığı hizmetleri, sağlık eğitimi gibi işler ile biyolojik, fizik ve sosyal çevredeki olumsuz koşullardan kaynaklanan sağlık problemlerini önlemek amacıyla çevreye yönelik yapılan müdahaleler koruyucu hizmetlerdir. Koruyucu sağlık hizmeti sunan kurumlara örnek olarak sağlık ocağı, dispanserler, çevre sağlığı birimleri, işyeri reviri, ana-çocuk sağlığı ve aile planlaması merkezleri verilebilir (Kavuncubaşı ve Yıldırım 2015 s.41-43).
- **Tedavi edici sağlık hizmetleri:** Hastalık ve sakatlık halinin iyileştirilmesi ve hastalık etmenlerinin yok edilmesi amacına yönelik verilen hizmetlerdir. Bu hizmetler uzman hekim sorumluluğunda ve diğer sağlık çalışanlarının ekip halinde çalışmasıyla yürütülmektedir. Aynı zamanda ileri teknoloji kullanılması nedeniyle koruyucu hizmetlere göre daha maliyetlidir ve organizasyon gerektirmektedir. Tedavi edici sağlık hizmetleri; birinci basamak, ikinci basamak ve üçüncü basamak sağlık hizmetleri şeklinde sınıflandırılmakta ve hizmet sunumunda ayakta ve yatarak sağlık hizmeti sunan kurumlar yer almaktadır (Somunoğlu 2012, s.12).
- **Rehabilite edici sağlık hizmetleri:** Hastalık ve kaza sonucu oluşan kalıcı rahatsızlıklar ve sakatlıkların gündelik yaşamı etkilemesini engellemek veya oluşan bu etkiyi en aza indirgemek, bireylerin bedensel ve ruhsal yönden başkalarına bağımlı olmadan yaşamasını sağlamak amacıyla düzenlenen hizmetlerdir. Bu hizmetler, tıbbi ve sosyal rehabilitasyon olarak iki şekilde sunulmaktadır (Hayran 1998, s.19).
- **Sağlığın geliştirilmesi hizmetleri:** Sağlığın geliştirilmesi, birey ve toplumun bedensel ve zihinsel sağlık durumunun, yaşam süresinin ve yaşam kalitesinin yükseltilmesini amaçlar. Sağlığın geliştirilmesinde temel sorumluluk bireylere aittir (Kavuncubaşı ve Yıldırım 2015, s.45).

1.4. Sağlık Yönetimi Kavramı

Sağlık yönetimi; sağlık hizmetlerinin planlanması, örgütlenmesi, yönetilmesi, koordinasyonu ve hizmetlerin sonuçlarının verimliliğini kontrol etmek ve tekrar planlama yapmak üzere gerçekleştirilen faaliyetler bütünüdür (Çamcı 2007, s.42). Sağlık yönetiminde eğitim önemli bir yer tutmaktadır. Sağlık hizmetleri yönetimi, insan sağlığı konusunda olduğu kadar, psikoloji, iletişim, insan kaynakları, işletme, muhasebe, hukuk, ekonomi, bilişim hizmetleri yönetimi gibi alanlarda da bilgi ve beceri sahibi olmayı gerektirmektedir (Çimen 2010, s.137). Günümüzde sağlık hizmetleri yönetimi, disiplinler arası bir alan olup, tıbbi ve idari hizmetler ile birlikte bilişim hizmetleri yönetimi, bilgisayar mühendisliği, biyomedikal mühendisliği gibi alanları da birleştirmektedir (http://www.cahiim.org/him/him.html, e.t:28.11.2017).

2. SAĞLIK BİLGİ SİSTEMLERİ ve UYGULAMA ALANLARI

2.1. Bilgi Kavramı ve Bilgi Sistemleri

Geleneksel üretim faktörleri; toprak, emek ve sermayedir. Günümüz dünyasında ise dikkatler daha az somut olan dördüncü bir faktör olan bilgiye yönelmiştir. Bilginin daha önemli bir kaynak haline gelmesi, küresel ekonominin odak noktası olmuştur. Bundan dolayı organizasyonların ve bireylerin başarısı için bilginin ne anlama geldiğini anlamak ve onu yönetmek zorunlu hale gelmiştir (Baraz 2015, s.113).

Bilgi; sistemli bir şekilde belli bir yöntemle başkalarına aktarılan, olgu veya fikirlerle ilgili düzenli ve sistemli ifadelerdir (Koçdar 2016, s. 4). Bilgi sistemi; bilgilerin toplanması, saklanması, işlenmesi, erişimi ve dağıtımı gibi işlemlerin yerine getirilmesi için gerekli olan bilgisayar, uzman işgücü, iletişim, bilgisayar ağları, sistem modelleri ve sistemde bulunan bilgilerin tümüdür. Organizasyonun hedeflerini gerçekleştirebilmesi amacıyla, gündelik işlemlerini yerine getirebilmek ve uzun dönemli planlar yapabilmek için gerekli olan bilgileri elde etmek üzere bilgi sistemleri geliştirilir (Işık 2014, s.6).

Bilgi sistemin üç temel bileşeni bulunmaktadır. Bunlar (Kavuncubaşı ve Yıldırım 2015, s.426);

- **Bilgisayar ve iletişim teknolojisi**: Bilgi sisteminin en önemli bileşenidir. Bilgisayar ve iletişim teknolojisi, kişisel bilgisayarlardan, büyük bellekli ve işlem kapasiteli farklı türde araç ve cihazları kapsamaktadır. Bilgisayar ve iletişim teknolojileri, diğer bilgi sistemi bileşenlerinin kurulması ve işletilmesi için temel fonksiyondur. Yani bilgisayar ve iletişim teknolojisi bulunmadıkça bilgi sisteminden söz edilemez.
- **Veri tabanı yönetimi**: Veri tabanı yönetimi, verilerin depolanmasını, organize edilmesini ve işlenmeye hazır tutulmasını sağlayan araç ve programları içermektedir.
- **Model yönetimi:** Veri tabanında depolanan verileri işleyen ve bilgi üreten kişi ve programları içermektedir.

Veriden bilgiye geçiş aşamaları düşünüldüğünde; veri özümlenmemiş ve yorumlanmamış gözlemler, gerçekler olarak ifade edilirken; bilgi düzenlenmiş veri olarak tanımlanmaktadır (Mumcu 2011, s.2). Verinin tek başına bilgilendirici özelliği bulunmamaktadır. Bilgi; belirli bir amaç ya da görev için, biçim ve içeriği uygun olan veridir (Kavuncubaşı ve Yıldırım 2015, s.425).

Bilgi sistemlerinde bilgi oluşturma süreci; girdi, işlem, çıktı, depolama ve dağıtım olmak üzere beş basamaktan oluşmaktadır. Girdi aşamasında, organizasyondan ya da çevresinden ham veriler toplanır. Süreç ya da işleme aşamasında, toplanan bu ham veriler anlamlı bir biçime dönüştürülür. Çıktı aşamasında ise anlamlı hale getirilen bu veriler bilginin kullanıcılarına transfer edilir. Çıktılar sisteme dahil olan üyeler tarafından değerlendirilmek ve doğrulanmak amacıyla geri bildirimlerde bulunur ve girdi olarak tekrar döngünün başına döner. Sonrasında tekrar bir dizi işlemden geçirilerek kullanıcılara veya organizasyona çıktı olarak sunulur (Işık 2014, s.7).

Bilgiyi yaratmak, paylaşmak, elde tutmak ve uygun iş sürecini gerçekleştirmek olarak tanımlanan bilgi yönetimi; bilginin organizasyon içinde hızla dağılmasını ve paylaşılmasını sağlar, verimsizlik ve zaman kaybını önler, bilginin işletme stratejileriyle ilişkilendirilmesini, yönetilmesini ve aynı zamanda işbirliği koşullarının belirlenmesini hedefler (Mumcu 2011, s.2).

2.2. Sağlıkta Bilişim Teknolojileri ve Gelişim Süreci

Sağlıkta bilişim teknolojileri; bilgisayar, iletişim ve bilgi teknolojilerinin/ sistemlerinin tıbbi uygulamalara, sağlık hizmetlerine, eğitime ve araştırmalara uyumlandırılması olarak tanımlanır. Sağlıkta tıbbi uygulamalar ile teknoloji işbirliğinin sağlandığı dinamik bir bilimsel çalışma alanı olarak da ifade edilir. Küreselleşen dünyamızda iletişim gereksiniminin artması ve aynı zamanda bilgisayar teknolojisinin gelişimi, disiplinler arası iletişim ortamını sağlayan sağlıkta bilişim teknolojilerinin gelişiminde önemli rol oynamıştır (Mumcu 2011, s.1).

Sağlık hizmetleri alanına giren yazılım şirketlerinin sayısındaki artış ve donanım ürünlerinin daha da gelişmesi, bilgisayarın hem klinik hem de idari işlevlerde kullanılabilir olmasını sağlamıştır. Böylelikle finansal amaçlı kullanılan bilgisayar

sistemleri yanında, klinik bilgi sistemlerini içeren entegre hasta kayıt sistemleri, dijital görüntüleme sistemleri tüm sağlık çalışanları tarafından kullanılmaya başlanmıştır. Sonrasında ise tıbbi kayıtlarda gizlilik, verinin bütünlüğü ve çok amaçlı kullanımı, kullanıcı kabulü, verinin güvenliği, internet, bilgisayar tabanlı hasta kayıt sistemlerinin oluşturulması tıpta dönüm noktasını oluşturmuştur. Günümüzde, elektronik sağlık kayıt sistemleri ve E-sağlık uygulamaları, sağlık sektörünün temel uygulamaları arasında yer almaktadır (Işık 2014, s.11).

Sağlıkta bilişim teknolojileri, verinin ve bilginin uygun bir şekilde işlenmesini sağlar. Sağlık hizmetlerinin planlanmasında, klinik uygulamalarda, epidemiyolojik çalışmalarda ve stratejik bilgi yönetiminde etkin rol oynar. Sağlıkta bilişim teknolojileri kalite ve etkili hasta bakımı için gerekli desteği sağlar. Teknolojik yenilikler, ağ ve veri tabanı uygulamaları, taşınabilir elektronik araçlar, elektronik tıbbi kayıtlar ve bilgisayar yazılım programları sayesinde, sağlık hizmetlerinin birçok alanına sağlık bilişim teknolojilerinin uyarlanması sağlanmıştır (Mumcu 2011, s.3).

2.3. Sağlık Hizmetlerinde Bilgi Sistemlerinin Kullanımı ve İşlevleri

Günümüzde sağlık hizmetlerinde kliniklerin, hastanelerin, eczanelerin ve hastaların, yönetsel maliyetlerin azaltılması ve sağlık bakım kalitesinin geliştirilmesi amacıyla bilgiyi paylaşıp, bilgi tabanlı bir topluluk haline gelmeye başladığı görülmektedir (Özata ve Güleş 2005, s.88). Sağlık hizmetleri bilgi tabanlıdır ve klinik uygulamaların birçoğu bilginin toplanmasını, birleştirilmesini ve işlenmesini gerektirir. Bundan dolayı bilgi yönetimi sağlık hizmetlerinin temel yapıtaşı haline gelmiştir. Hizmet sunumu, bilgi teknolojilerinden/sistemlerinden önemli derecede etkilenmektedir (Saluvan ve Şahin 2014, s.45).

Sağlık bilgi sistemleri; koruyucu ve tedavi edici sağlık hizmetlerinin yönetimi ve sunumu için gerekli olan her türlü bilginin üretilmesi, iletimi ve etkin biçimde kullanımı için kurulan donanım, yazılım, yöntem ve yönergeler bütünüdür (Işık 2014, s.8). Bilgi ve iletişim teknolojileri, birçok alanda olduğu gibi sağlık alanında da bilgiye erişimin en önemli kaynaklarından biri haline gelmiştir (Ekiz 2017, s.6). İyi organize olmuş bir sağlık sisteminin oluşturulmasında bilgi sistemlerinin önemi büyüktür. Sağlık sektöründe yer alan kurumlar, karar verme aşamasında verileri daha

etkili şekilde kullanarak değerlendirmek, hizmet yelpazesini genişletmek, verimliliği artırarak maliyetleri düşürmek, hasta hizmetlerini iyileştirmek ve kaynakların daha iyi yönetilmesini sağlamak amacıyla bilgi teknolojilerinden ve sağlık bilgi sistemlerinden faydalanmaktadır (Ömürbek ve Altın 2009, s.211).

Sağlık bilgi sistemlerinin temel özellikleri

Sağlık bilgi sistemlerinin belirlenen amaçlara ulaşabilmesi için şu özellikleri taşıması beklenir (Işık 2014, s.8);

- Doğru, güvenilir, yararlı, eksiksiz ve kapsamlı verileri zamanında, hızlı ve ekonomik olarak derleyebilmeli,
- Derlediği verileri yetkili kişiler kullanabilmeli ve bilgiye dönüştürebilmeli,
- Üretilen bilgi bir havuzda biriktirilebilmeli,
- Gelişmelere uyarlanabilecek esnekliğe sahip olmalı, ülke içinde kurumlar arası, ülke dışında ülkeler arası bilgi alışverişine bulunabilecek standartlara sahip olmalı,
- Gizliliğe özen gösterilmeli,
- Sağlık personelinin tümünün etkin ve verimli bir şekilde katıldığı, motive olduğu ve kullanabildiği bir sistem olmalı,
- Gerektiğinde sistemin tümü ya da bir kısmı hızlı ve kolayca güncellenebilmeli.

Elektronik sağlık kaydı sistemi

Günümüzde tıbbi kayıtlar; hastalar, sağlık çalışanları, hastaneler, tedarikçiler, özel sigorta şirketleri, sosyal güvenlik kurumu, yöneticiler, adli birimler ve eczacılar gibi pek çok profesyonel kişi, kurum ve politika yapıcılar tarafından kullanılmaktadır. Tüm bu kişi ve kurumların ihtiyaçlarına zamanında cevap verebilmek için nitelikli bir sağlık bilgi sisteminin kurulması ve çalıştırılması bir zorunluluktur. Tüm bu sorunların çözümü için insanların yaşamları boyunca sağlık durumları ile ilgili bilgilerini kayıt altına alan ‘‘elektronik sağlık kaydı sistemi’’ oluşturulmuştur (Işık 2014, s.14).

Sağlık hizmetlerinde elde edilen verilerin temeli, kişiye ait özel verilerden oluşmaktadır. Bunlar; sosyo-ekonomik veriler, finansal veriler, hasta kimlik verileri ve klinik verilerdir (Tekin 2016, s.6).

- **Sosyo-ekonomik veriler:** Hastayı tanımlayan verilerdir. Bunlar; isim, adres, doğum tarihi, aile, ırk, eğitim, gelir kaynağı, cinsiyet, meslek, evlilik durumu gibi verilerden oluşmaktadır.
- **Finansal veriler:** Sunulan sağlık hizmetinin maliyeti ve fiyatlandırılması ile ilgili veriler için kullanılan bir terimdir. Geri ödemeler, sigorta ödemeleri, cepten ödemeler ve kamu bütçesinden gelen pay gibi işlemleri izlemek için kullanılır.
- **Hasta kimlik verileri:** Hastanın sağlık kuruluşuna başvurduğunda hastaya verilen kişisel kimlik numarasını (provizyon numarası) içerir. Bu numara hastayı diğer hastalardan ayırmak için kullanılır.
- **Klinik veriler:** Hastanın tedavisi ile ilgili bilgileri içerir. Bu veriler hasta kaydı olarak düzenlenir ve doktorlar, diğer sağlık çalışanları ve yasal olarak hasta ile ilgilenen kişiler tarafından kullanılan verilerdir. Bu veriler; hastanın öyküsü (anamnez ve fiziksel muayene), izlem notları, şikayetleri, hemşire bakım planı, acil servis raporları, patoloji raporları, ameliyat raporları, doktor istekleri (laboratuar ile görüntüleme istekleri) ve konsültasyon gibi diğer değerlendirme raporlarıdır.

Elektronik Sağlık Kaydı (ESK); dijital ortamda hasta veri havuzunun oluştuğu, verinin saklandığı, güvenli koşullarda değişimin sağlandığı ve farklı kullanıcıların sisteme ulaşabildiği bir yapılanmadır. Anamnez, fizik muayene sonuçları, konsültasyonlar, laboratuvar ve görüntüleme istekleri ile bunların sonuçları, tedavi protokolleri ve ilaç uygulamalarına ait tüm bilgiler bu sistemin içinde yer alırlar. ESK'da her hasta için kullanılan ilaçların listesi, dozları, tedavi süresince kesilen ilaçlar, yeni başlananlar, ek reçete sayılarına ait bilgilere ulaşmak mümkündür. Ayrıca acil durumlarda tıbbi kayıtların ve hastanın kullandığı ilaçların tanımlanmasında da önemli yer tutar (Mumcu 2011, s.61).

Sağlık hizmetlerinde elektronik sağlık kaydına gereksinim duyulma nedenleri

ESK sisteminin sağlık hizmetlerinin sunumundaki önemi aşağıdaki gibi sınıflanabilir (Mumcu 2011, s.62-63):

- Hizmetin kalitesi ve hasta güvenliğini artırma,
- Etkinlik ve üretimin geliştirilmesindeki gereksinimler,
- Kâğıda dayalı formlardaki sorunlar,
- Toplumsal beklentiler,
- Politika yapıcıların beklentileri,
- Teknolojik avantajlar,
- Finansal tasarruf.

Elektronik sağlık kayıtlarının saklanması ile ilgili özellikler

- **Süreklilik:** Sağlık kayıtları her nerede olursa olsun kalıcı ve korunmalı bir şekilde gebelikten doğuma, doğumdan ölüme kadar saklanmalıdır.
- **Devamlı bakım:** Sürekliliğin sağlanması için kayıtların devamlılığı gereklidir. Sistem yazılımının korunması, donanımın uygun bakımı ve onarımı önemlidir. Sistemin alımında yapılan anlaşmalarda güvenirlik ve onarım garantisi yer almalıdır.
- **Güvenlik tedbirleri:** Devamlı bakım sağlamak, güvenlik önlemleri almak ve herhangi bir saldırı durumunda hızlı ve kararlı eylemde bulunma işlevidir.
- **Sistemi güncelleştirmek:** ESK sistemleri yeni bilgi tipleri, yeni özellikler ve yeni işlemler kolayca eklenebilecek şekilde tasarlanmalıdır.
- **Yedekleme ve kurtarma:** Sistemdeki verilerin zarar görmesi ya da sistem yetmezliği durumunda kaybolan verilerin yeniden kurtarılmasını içerir (Işık 2014, s.13).

ESK; bireyin geniş kapsamlı kayıtlarından oluşmaktadır ve hastanın yalnızca rahatsızlıkları ya da şikâyetlerini değil, sağlıklı olma halindeki bilgilerini de içerir. Aynı zamanda hekimlerin ve diğer sağlık çalışanlarının iş akışını düzenler ve bu kayıtlar çıktıların raporlanmasını da sağlar (Işık 2014, s.18).

Sonuç olarak; ESK sisteminde kişisel sağlık kayıtlarının oluşturulması, standart ve kodların uygun şekilde seçimi ve entegrasyonunun sağlanması, veri güvenliğinin oluşturulması ve bilgi yönetiminin sağlanması kritik noktalardır (Mumcu 2011, s.68).

Hastane bilgi yönetim sistemi

Hastane bilgi yönetim sistemi (HBYS); sağlıkta bilgi sistemleri kullanımının bir örneğidir ve yüksek kalitede etkili hasta bakımını sağlamayı amaçlar. Hastane otomasyon bilgilerini toplayan ve disiplinler arası bilgiye ulaşılabilirliği arttıran HBYS; yönetimsel, tıbbi ve finansal olarak üç farklı disiplinde değerlendirilir. Sonuç olarak; HBYS farklı disiplinlerden gelen bilginin sisteme uyumunu sağlayan hasta merkezli bir yaklaşım olarak da düşünülebilir (Mumcu 2011, s.4).

Başarılı bir HBYS takım çalışmasını gerekli kılar ki bu takım bir hastane ya da sağlık kuruluşunda yer alan bilgi teknolojileri bölümü (IT), hemşireler, idareciler, doktorlar, klinisyenler, cerrahlar, muhasebeciler, tedarikçiler, depolayanlar, eczacılar, biyomedikal uzmanları, büro çalışanları gibi bütün disiplinlerden oluşur (Tekin 2016, s.15).

HBYS; hastanenin bilgi işleme faaliyetleri ile ilgili bütün insan, araç ve eylemleri kapsayan hasta bilgilerini, tanı ve tedavi yöntemlerini, hastane mali sistemlerini ve yönetim sistemlerini, laboratuvar bulgularını kapsayan yazı formatındaki veri tabanlarından oluşmaktadır (Özata ve Güleş 2005, s.120).

Türkiye'de hastane bilgi yönetim sistemleri ile ilgili Sağlık Bakanlığının ilk çalışması ''Sağlık Enformasyon Sistemleri Projesi'' ile başlamıştır. Hastane bilgi yönetim sistemi unsurları; yazılım, donanım, network (ağ), izleme komitesi ve insan gücünden oluşmaktadır (Tekin 2016, s.15-16).

Hastanelerde bilgi sistemlerinin kullanım amaçları

Hastanelerde bilgi sistemlerinin kullanım amaçlarını aşağıdaki gibi sıralamak mümkündür (Akbolat 2014, s.115):

- Hastanın tıbbi özgeçmişi ve hastalığına ait tüm bilgiler bilgisayara anında kaydedilir ve istenildiğinde bu bilgilere erişilebilir,

- Hastanın tıbbi özgeçmişine ve daha önceki bilgilerine hızla erişilmesini sağlayacak çağdaş bir arşivleme sisteminin kurulması, hastalığın teşhisinde hızlı ve güvenilir sonuçların alınmasını sağlayacaktır,
- Hastane yönetimi ile ilgili tüm bilgiler bilgisayar sisteminde takip edilmekte ve bu bilgilere kolay ve hızlı bir şekilde ulaşılabilmektedir. Böylece hastanede tüm idari işlemleri daha sağlıklı ve düzgün şekilde yürütmek mümkündür,
- Hastanelerde faturalama ve resmi evrak hazırlama işlemleri hızlı ve güvenilir bir şekilde yerine getirilerek gelirlerin artırılması gerçekleştirilebilir,
- Hastanelerdeki tüm satın alma ve malzeme dağıtım işlemleri bilgisayarlar aracılığı ile yürütülür, stok miktarları takip edilir, alınan malzemelerin adet ve alım fiyatları incelenebilir.

Hastane bilgi yönetim sistemleri

- **Eczane bilgi sistemi:** İlaçların satın alınması, depolanması, stok durumlarının kontrolü, hasta ve servislere dağıtımı amacıyla eczane bilgi sistemi geliştirilmiştir. Aynı zamanda tedavi hizmetlerini de desteklemektedir. Hastalara verilen ilaçları takip etme, hasta reçetelerini inceleme, ilaçların yan etkileri ve dozu hakkında sağlık çalışanına bilgi veren sistemdir (Kavuncubaşı ve Yıldırım 2015, s.447).
- **Radyoloji bilgi sistemi:** Tıbbi görüntülerin raporlaması, radyoloji istatistik raporlaması, hasta tıbbi bilgi girişi, hastadan istenen tıbbi görüntüleme yöntemi, döküm alımı ve raporlamayı kapsayan sistemdir (Mumcu 2011,s.7).
- **Laboratuvar bilgi sistemi:** Hastalara ait tetkikleri ilgili poliklinik, ameliyathane, yoğun bakım, acil servis gibi birimlerin bilgisayar terminallerinden isteyen ve sonuçları ilgili terminallere gönderen sistemdir (Odacıoğlu 2016, s.55).
- **Hemşirelik bilgi sistemi:** Hastanın izlenmesi, değerlendirilmesi, bakım planlarının hazırlanması, elde edilen bilginin diğer sağlık personeliyle ve kurumları arasında paylaşılmasını sağlayan sistemdir (Özata ve Güleş 2005, s.103).

3. SAĞLIKTA DÖNÜŞÜM PROGRAMI ve E-SAĞLIK UYGULAMALARI

3.1. Türkiye Sağlık Bilgi Sistemi (TSBS)

E-sağlık; sağlık hizmetlerinin etkin ve verimli sunulabilmesi, vatandaşın hizmetlere hızlı erişiminin sağlanması, sağlık sektöründe yer alan tüm paydaşlar ile veri paylaşımının sürdürülebilir olması, yükselen hasta beklentilerinin karşılanması için bilgi ve iletişim teknolojilerinin sağlık alanında kullanılmasıdır (Akca 2014, s.159).

Sağlık Bakanlığı'nın Sağlıkta Dönüşüm Programı'ndaki 11 bileşeninden birisi; ''Karar Sürecindeki Etkin Bilgiye Erişim: Sağlık Bilgi Sistemi'' dir. E-sağlık uygulamalarının temelini de Sağlık Bilgi Sistemi oluşturmaktadır. Sektörler arası iş birliği ile Türkiye Sağlık Bilgi Sistemi (TSBS) alt yapısını oluşturmak için Sağlık Bakanlığı Koordinatörlüğü ile kamu, sivil toplum kuruluşları, üniversiteler ve özel sektörün katılımı ile Türkiye Sağlık Bilgi Sistemi çalışmaları başlatılmıştır. Bu çalışmalar, E-dönüşüm Türkiye Projesi ile birlikte koordinasyon içerisinde yürütülmektedir (Sağlık Bakanlığı 2004, s.7).

Sağlık Bakanlığı koordinasyonuyla hazırlanan ''Türkiye Sağlık Bilgi Sistemi Eylem Planı'' aşağıdaki hedefleri içermektedir (Sağlık Bakanlığı 2004, s.43-54):

- Sağlık enformasyonu konusunda ulusal ve uluslararası entegrasyonu sağlamak amacıyla, ''Veri Sözlüğü ve Standartları'' nın belirlenmesi,
- Sağlık kayıtlarının doğum ile başlayıp yaşam boyu elektronik ortamda tutulmasının sağlanması için tek numaraya dayanan ''Kişisel Sağlık Tanımlayıcısı'' nın oluşturulması,
- Sağlık sektörünün ihtiyaçları doğrultusunda, sağlık olayları, bağışıklama, tanı ve tedavi prosedürleri, ulusal kanser kayıtları, ruh sağlığı kayıtları ve kişisel sağlık verilerini toplamak amacıyla, birinci, ikinci ve üçüncü basamak sağlık hizmetleri için öncelikli ''Sağlık Veri Modeli ve Minimum Sağlık Veri Setleri'' nin oluşturulması,

- Tanı ve tedavi alanında tıp teknolojilerindeki ilerlemeler ve bunun sonuncunda elektronik kişisel sağlık kayıtlarının ciddi oranda artması sebebiyle kâğıt üzerinde veya elektronik ortamda tutulan sağlıkla ilgili ‘‘Kişisel Verilerin Mahremiyet ve Güvenliği’’ nin sağlanmasına yönelik yasal ve teknolojik tedbirlerin alınması,
- Sağlık tehditlerinin zamanında belirlenmesi amacıyla, bulaşıcı hastalıklar ağı gibi ülke düzeyinde uluslararası sistemler ile entegre ‘‘Erken Uyarı Sistemleri’’ oluşturmak,
- Sağlık sektöründe yer alan kuruluşların sağlıkla ilgili verileri ortak kullanabilmeleri, iletişim altyapısının ve organizasyonun sürekliliği için ulusal düzeyde güvenli ‘‘Sağlık Özel Ağı’’ nın oluşturulması,
- Araştırma, yönetim, eğitim gibi alanlarda ve yerinde sağlık bakımı gerektiren durumlarda, sağlık hizmetlerine erişimde sorun yaşanan yerlerde bilgi ve iletişim teknolojilerinin mesleki alanda kullanılması için ‘‘Tele-tıp’’ uygulamalarının yaygınlaştırılması,
- Mezuniyet öncesi ve sonrası sağlık eğitiminde bilgi teknolojileri alanına yer verilmesi ve müfredat programlarında gerekli düzenlemelerin yapılması için ‘‘Sağlık Bilişimi’’ alanında nitelikli insan kaynağının yetiştirilmesi hedeflenmektedir.

Sağlık Bakanlığı’nın E-sağlık vizyonu; Ülke genelinde sağlık sektöründe görev alan ve sağlık verileri için erişim hakları tanımlanmış tüm paydaşların (sağlık hizmeti alan, sunan, tedarik eden, finanse eden, kamu kuruluşları, üniversiteler, özel sektör, sivil toplum kuruluşları vb.) katkısıyla ulaşılabilir, tüm vatandaşları kapsayan, her bireyin kendi bilgilerine ulaşabildiği, doğum ile başlayıp tüm yaşam süresince sağlıkla ilgili verilerden oluşan, uluslararası standartlarla uyumlu, karar destek sistemleri ile desteklenen işlevsel bir veri tabanının; yüksek bant genişlikli ve tüm ülkeyi kapsayan bir iletişim ağında paylaşılması ve tele-tıp uygulamalarına varan teknolojilerin mesleki pratikte kullanılmasını temel alan ‘‘Ulusal Sağlık Bilgi Sistemi’’ nin kurulmasıdır (Sağlık Bakanlığı 2004, s.5).

Ulusal Sağlık Bilgi Sistemi (USBS), sağlık hizmeti sunan tüm kurum ve kuruluşların insan gücü, taşınır, taşınmaz, idari ve mali verilerini de kayıt altına

alacak şekilde tasarlanmıştır. E-sağlık projeleri ile sağlık hizmeti veren kurumlarda hizmet kalitesini artırmak hedeflenmektedir. E-sağlık projelerinin temel amaçları şu şekilde özetlenebilir (Akdağ 2012, s.233):

- Sağlık veri standardizasyonunun sağlanması,
- Veri analiz desteği ve karar destek sistemleri oluşturulması,
- Elektronik kişisel sağlık kayıtlarının oluşturulması,
- Kaynak tasarrufunun sağlanması ve verimliliğinin artırılması,
- Bilimsel çalışmalara destek verilmesi,
- E-sağlık kavramının ulusal anlamda benimsenmesinin hızlandırılması.

3.2. Sağlık-Net Portalı

Sağlıkta dönüşüm programının tüm bileşenleri arasında uyumun sağlanabilmesi için bütünleşik bir sağlık bilgi sistemine ihtiyaç duyulmuştur. Bundan dolayı Sağlık Bakanlığı bir E-sağlık uygulaması olan Sağlık–Net'i tasarlamıştır. Vatandaşların elektronik sağlık kayıtlarının sağlık kuruluşları arasında paylaşılabilirliğinin temeli de Sağlık-Net ile atılmıştır. Eskiden yalnızca istatistikî ve matbu form olarak toplanan veriler, Sağlık-Net ile bireylerin doğumundan ölümüne kadar olan süreçte bütün sağlık bilgilerini kapsayacak şekilde toplanmaya başlanmıştır (Akca 2014, s.172).

Sağlık-Net, tüm vatandaşların kişisel sağlık verilerinin merkezi bir yerde kayıt altına alındığı bir sağlık veri bankacılığı modelidir. Sağlık kuruluşlarında elektronik ortamda üretilen verileri standartlara uygun şekilde toplayan, güvenli, hızlı, entegre bir bilgi ve iletişim platformudur ve sağlık hizmetlerinde verim ve kaliteyi arttırmayı amaçlamaktadır (Akdağ 2012, s.233).

Sağlık-Net altyapısının temel özellikleri şunlardır (Akdağ 2012, s.234):

- Sağlık kurumlarındaki farklı yazılımlardan standart veri transferi yapabilir,
- Hukuka uygun olarak uluslararası veri değişimi sağlar,
- Bilgiye hızla erişir,
- Uluslararası kurumlarla (DSÖ, OECD) paylaşılan göstergeleri takip eder,
- Karar mekanizmasında rol alabilen, hastalık yüküne ve sağlık harcamalarına, demografik analizlere yönelik gerekli ve yeterli bilgiye ulaşmayı sağlar.

Sağlık-Net uygulamasında verilerin değiştirilmesi, depolanması, bilginin organizasyon içerisinde ve organizasyonlar arasında paylaşılmasını ve farklı sistemlerin birlikte çalışmasını sağlayabilmek için verilerin belirlenmiş standartlar doğrultusunda toplanması gerekmektedir. Bunun için standartlar altyapısı oluşturulmuştur (Akca 2014, s.172).

3.3. Ulusal Sağlık Veri Sözlüğü ve Minimum Sağlık Veri Setleri

E-sağlık uygulamalarında Ulusal Sağlık Veri Sözlüğü (USVS) ve Minimum Sağlık Veri Setleri (MSVS) önemli bileşenlerdir. USVS; Türkiye'deki sağlık kuruluşlarında kullanılmakta olan sağlık bilgi sistemlerinin referans olarak kullanacağı bir sözlük çalışmasıdır. Sözlük, farklı kategorilerde veri kümelerinin olduğu terimlerden ve bu terimler arası ilişkilerden oluşmaktadır. Veri sözlüğünün temel amacı, sağlık alanındaki tüm aktörlerin aynı kavramdan aynı içeriği anlamalarını sağlayacak bir terminoloji birliği oluşturmaktır. Veri sözlüğü, sağlık kurumlarından verilerin belirlenmiş standartlar doğrultusunda toplanmasını, analizini ve değerlendirmesini sağlayacaktır. Aynı zamanda sahadan sağlık verisi toplama konusunda verimi artıracak, tekrarlanan ve hatalı verileri azaltacak ve toplanan verilerin amacına uygun bir şekilde kullanılmasına olanak tanıyacaktır (Sağlık Bakanlığı 2007, s.15).

Minimum Sağlık Veri Setleri ise; ülke çapında sağlık kuruluşlarından veri toplama konusunda ulusal standart haline gelebilecek setlerden oluşan veri kümeleridir. Yani Sağlık Bakanlığı'nın kurumlardan toplayacağı minimum içeriğe sahip veri gruplarını ifade etmektedir. MSVS ile şimdiye kadar kâğıt ortamda toplanan veriler, bilgi ve iletişim teknolojileri sayesinde daha hızlı ve doğru bir şekilde, doğrudan verinin üretildiği bilgi sisteminden elektronik ortamda Sağlık Bakanlığına iletilecektir. Hastane bilgi sistemleri, veri setleri içinde yer alan veri elemanlarına göre veri tabanlarını güncelleyecek ve Sağlık Bakanlığı veri tabanı ile haberleşebilecek bir yapıya ulaşacaktır (Sağlık Bakanlığı 2007, s.8).

MSVS içerisinde yer alan verilerin tamamı, Ulusal Sağlık Veri Sözlüğü içinde tanımlanmaktadır. Örneğin intihar girişimi ve kriz izlemden obeziteye, kronik hastalıklardan HIV tespitine, kadına yönelik şiddetten gebe izleme, 15-49 yaş kadın

izlemden hasta özlük bilgilerine kadar onlarca veri seti tanımlanmıştır. Her veri seti için hedef ve amaç ayrı ayrı belirtilmiştir. Örneğin, hasta özlük bilgileri için oluşturulan veri setinde; kişisel sağlık kayıtlarının oluşturulmasında, kişiye ait yaşam tarzı, öğrenim durumu, sosyo kültürel durum vb. karakteristikler oldukça önemli bilgiler içermektedir. Bundan dolayı bu veri seti ile toplanan bilgilerin demografik analizlerde, epidemiyolojik çalışmalarda ve sağlık hizmetlerinin planlanmasında kullanılması hedeflenmektedir (http://www.kisiselsaglikverileri.org/hakkinda.php?id=32, Türk Tabipleri Birliği, Kişisel Sağlık Verileri Çalışma Grubu, Sağlık Hizmetlerinde Kişisel Veri Toplanması, Korunması ve Değerlendirilmesi, e.t:17.10.2016).

3.4. Aile Hekimliği Bilgi Sistemi (AHBS)

Birinci basamak sağlık hizmetlerinin temelini oluşturan AHBS ile aile hekimlerinin hastalarını hastanelere sevk ederken, randevu alabilmesi ve hastanın hastanede muayene olacağı doktorunu seçebilmesi için internet tabanlı randevu sistemi geliştirilmiştir. AHBS uygulaması, her bireyi doğumdan önce takibe alır ve sağlığı ile ilgili bilgileri depolar. Bireyin anne karnındaki gelişimi ve doğumu ile ilgili bütün bilgiler AHBS aracılığıyla kaydedilir ve aile hekiminin sorumluluğu altındaki bilgi bankasında kişinin ömür boyu sağlık kaydının ilk bilgi parçaları olarak yer alır. Kişinin hayatı boyunca, sağlık kayıtları da onunla birlikte büyür. AHBS sayesinde aile hekimleri, bireylere ait sağlık verilerini, elektronik ortamda doğrudan Bakanlığa gönderebilmektedirler. Böylelikle her vatandaşın elektronik sağlık dosyası oluşturularak, bu dosyalardan üretilen istatistikler sayesinde karar süreçlerinde kullanılmaktadır (Akca 2014, s.173-174).

3.5. E-nabız Kişisel Sağlık Kaydı Sistemi

E-sağlık uygulamalarının en yenisi E-nabız Kişisel Sağlık Sistemidir. E-nabız sistemi ile vatandaşların sağlık verileri tek veri tabanı sisteminde depolanmaktadır. E-nabız, güvenlik sistemiyle sağlık verilerinin hasta ve hastanın istediği kişilerle paylaşılmasına olanak vermektedir. Vatandaşlar E-nabız'a ilk girişlerini E-devlet

üzerinden ya da Aile Hekimleri aracılığıyla yapabilmektedir (Sağlık Bakanlığı 2016, s.1-3).

E-nabız; muayene, tetkik ve tedavilerin nerede ve kim tarafından yapıldığına bakılmaksızın, tüm sağlık bilgilerin çevrimiçi ortamda yönetilebildiği ve kişilerin tıbbi özgeçmişine tek bir yerden ulaşılabildiği bir kişisel sağlık kaydı sistemidir (https://enabiz.gov.tr/Giris.aspx, T.C. Sağlık Bakanlığı, E-nabız Kişisel Sağlık Sistemi, e.t:26.10.2016). 2016/6 sayılı Sağlık Bakanlığı genelgesinde de ifade edildiği üzere; *''Kişisel sağlık verilerinin gizlilik, güvenlik, bütünlük ve mahremiyeti korunarak Sağlık.Net Online Sistemi ve bu sisteme bağlı çalışan, ilgili kişilerin kendilerinin veya yetki verdikleri üçüncü kişilerin sağlık verilerine erişimini sağlayan Kişisel Sağlık Kaydı Sistemi (E-nabız) geliştirilmiştir. Bu sistemler sayesinde kişiler kendi sağlık durumları ile ilgili doğrudan bilgi sahibi olacaktır''* (http://www.saglik.gov.tr/TR/dosya/1-103259/h/genelge20166.pdf, T.C. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü, 2016/6 Sayılı Genelge, e.t:17.10.2016).

Sistemin özellikleri aşağıdaki gibi sıralanabilir (https://enabiz.gov.tr/Giris.aspx, T.C. Sağlık Bakanlığı, E-nabız Kişisel Sağlık Sistemi, e.t:26.10.2016):

- **Giyilebilir sağlık teknolojileri:** Adım, nabız, kalori, oksijen dağılımı gibi verileri ölçen akıllı bileklikler, bluetooth özellikli tansiyon, şeker ölçüm cihazları ve tüm GSM operatörlerinin sağlıkla ilgili uygulama ve cihazları E-nabız profiline entegre edilebilmektedir. Böylelikle bireye ait sağlık bilgileri tek bir yerde kayıt altında tutulabilmektedir.
- **Sağlık geçmişini görüntüleyebilme:** E-nabız kapsamında kayıt altında tutulan her türlü sağlık bilgisine internetin bulunduğu her ortamda erişmek mümkündür. Özellikle mobil uygulamalar sayesinde bu erişim kolaylığı giderek daha da artmıştır. E-nabız sistemi ile sağlık kurumlarında hangi branşlara ne zaman gidildiği gibi detaylı bilgilere, muayene bilgilerine, hastalara yazılmış reçetelere, reçeteleri yazan hekimin adına, ilaç bilgilerine ulaşılabilmektedir. Ayrıca laboratuarda yaptırılan tahlillerin sonuçlarına, alınan raporların bilgilerine, tıbbi görüntülere ve bunlara ait raporlara kolayca erişim sağlanabilmektedir. Böylelikle gidilen her sağlık kurumunda tekrar aynı türden tetkikleri yaptırma zorunluluğu ortadan kalkmaktadır.

- **Merkezi Hastane Randevu Sistemi (MHRS):** MHRS ile çalışan E-nabız sisteminde sağlık kurumu randevuları da alınabilmektedir.
- **Mobil uygulamalar:** Web sitesi üzerinden görülebilmekte olan ‘‘sağlık geçmişim, hastalıklarım, reçetelerim, tahlillerim, görüntülerim, acil durum notlarım ve raporlarım’’ bölümlerine ulaşılabilmektedir.
- **Güvenlik:** E-nabız sisteminde tüm verilerin kontrolü vatandaşların elindedir. E-devlet şifresiyle sisteme girip, E-nabız profili dondurulabilir ya da tamamen kapatılabilir. E-nabız'da paylaşılan bilgiler, kişinin onayı dışında veya yargı kararı/yasal bir yükümlülük bulunmadığı sürece herhangi bir üçüncü şahıs, kurum ve kuruluş ile hiçbir nedenden ötürü paylaşılmayacaktır. E-nabız sisteminde eksik veya hatalı olduğu düşünülen sağlık verilerinin (muayene, rapor, reçete vb.) olması durumunda kişi ilgili hastanenin ‘‘hasta hakları’’ birimine başvurmalıdır.

E-nabız sistemi Sağlık Bakanlığı içinden ve dışından birçok sistemden veri alış-verişi yapmaktadır. Bu sistemler aşağıdaki gibidir (Sağlık Bakanlığı 2016, s.60-63):

- Merkezi Hastane Randevu Sistemi (MHRS),
- Merkezi Nüfus İdare Sistemi (MERNİS),
- Aile Hekimliği Bilgi Sistemi (AHBS),
- Tele-tıp ve Tele-radyoloji,
- İlaç Bilgi Sistemi,
- E-devlet.

3.6. Hasta Doğrulama Sistemleri

Sistem, hastaların bazı değiştirilemeyen kişisel özellikleriyle (parmak izi, damar izi, retina vs.) kayıt altına alınmaları ve bu verilerin sağlık kurumlarına başvuru yaptıklarında sorgulanması esasına dayanmaktadır. Özellikle günümüzde ‘‘damar izi’’ taraması yaygın olarak kullanılan bir yöntemdir. Fakat hasta bilgilerinin güvenli koşullarda saklanması konusundaki belirsizlikler ve hasta mahremiyeti açısından sistemin işleyişine karşı çıkılmıştır. Yine de özel sağlık kurumlarında zorunlu olarak kullanımına devam edilmektedir (Dursun 2016, s.152).

3.7. Mobil Sağlık Uygulamaları (M-sağlık)

M-sağlık; akıllı telefonlar, tabletler ve kablosuz taşınabilir cihazlardaki uygulamalar kullanılarak, sağlığın korunması ve sağlıkla ilgili veri aktarılmasıdır. Hastaların cep telefonu üzerinden tansiyon ve şeker düzeylerini belirleyerek ilgili verilerini sağlık kuruluşuna iletmesi, akıllı telefon yazılımı ile tanı, teşhis ve tedavi sunulması M-sağlık konusunun kapsamına girmektedir (Kılıç 2016, s.105).

Türkiye'de M-sağlık alanında birçok farklı uygulamalar geliştirilmiştir. Örneğin; bir GSM operatörü, kronik hastalardan tansiyon, nabız vb. verileri alıp kablosuz olarak telefona, oradan da ilgili sağlık kuruluşuna aktarabilmektedir. Başka bir GSM operatörü de kadın sağlığı, gebelik, diyet, stresle başa çıkma gibi konularda mobil sağlık uygulamalarını geliştirmiştir (Kılıç 2016, s.115).

3.8. Tele-tıp

Tele-tıp; uzak merkezler arasında, bilgisayar ve iletişim teknolojilerini kullanarak, tanı, tedavi ve hasta izlemine yönelik sağlık hizmeti sunumu olarak tanımlanmaktadır (Gürgan 2011, s.35).

Tele-tıp projesinin amaçları aşağıdaki gibidir (Akdağ 2012, s.236):

- Sadece ilgili hekimlerin incelemesi ve raporlaması için güvenli ve hızlı bir elektronik ortamın oluşturulması,
- Hizmet kalitesinin artırılması,
- İşlemlerin dijital ortama taşınarak dijital hastane oluşturulması,
- Uzaktan sağlık bakım hizmeti sunumunda bilgi ve iletişim teknolojilerinden faydalanılması,
- Konsültasyon yapılabilmesi,
- Doğru ve hızlı tanı konulması,
- Hasta memnuniyetinin artırılması,
- Hastayla ilgili tıbbi görüntülerin ve bilgilerin ortak bir elektronik ortamda toplanması,
- Hekimler arasında bilgi ve deneyim paylaşımının yapılması.

4. BİLGİ GÜVENLİĞİ ve HASTA MAHREMİYETİ

4.1. Bilgi Güvenliği

Bilgi güvenliği; bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak, her türlü ortamda istenmeyen kişiler tarafından elde edilmesini önleme çabalarının tümüdür (https://bilgiguvenligi.saglik.gov.tr/, T.C. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü, Bilgi Güvenliği, e.t:26.10.2016**).**

Bilgi güvenliğinin sözlük anlamı; bilgiyi izinsiz erişimlerden, yok edilmesinden, ifşa edilmesinden, değiştirilmesinden veya hasar verilmesinden koruma işlemidir (https://tr.wikipedia.org/wiki/Bilgi_güvenliği; e.t:26.10.2016).

Bilgi güvenliğinin temel amacı (Kılıç Aksu vd. 2015, s.55-56);

- Mahremiyet ve gizliliğin sağlanması,
- Sistemin daima çalışabilirliğinin sağlanması,
- Veri bütünlüğünün korunması,
- İzinsiz erişimin engellenmesidir.

Bilgi güvenliğinin sağlanabilmesi bilginin gizliliğinin, bütünlüğünün ve erişebilirliğinin yeterli düzeyde sağlanabilmesi ile mümkündür. Bu üç temel güvenlik unsurundan herhangi biri zarar görürse güvenlik zafiyeti oluşur.

Gizlilik: Bilginin depolanması, işlenmesi, iletilmesi veya herhangi bir işlem sırasında, sahibi tarafından yetkilendirilmemiş kurum ya da kişiler tarafından ulaşılmasının engellenmesi anlamına gelmektedir (Aslandağ 2010, s.18). Başka bir deyişle gizlilik, bilginin yalnızca yetkilendirilmiş kurum veya kişilerce ulaşılmasıdır.

Bütünlük: Bilginin yetkisiz kişilerce değiştirilmesi, silinmesi veya herhangi bir şekilde zarar verilmesi tehditlerine karşı içeriğinin korunmasıdır (Yılmaz 2013, s.15). Bütünlük bilginin tam, eksiksiz, tutarlı ve doğru olmasını nitelendirmektedir (Ganbat 2013, S.4).

Kullanılabilirlik: Bilginin, yetkisi olan kurumlar ve kişiler tarafından her ihtiyaç duyulduğunda kullanıma hazır durumda olması demektir. Herhangi bir sorun veya

problem çıkması durumunda bile bilginin erişilebilir olması, kullanılabilirlik özelliğinin bir gereğidir (Önel ve Dinçkan 2007, s.6).

4.1.1. Bilgi Güvenliğini Etkileyen Faktörler

Bir kuruma yönelik bilgi güvenliği saldırıları, hem kurum içinden hem de kurum dışından kaynaklanabilmektedir. Bu sebeple, bilgi güvenliği tehditleri, içsel (dahili) ve dışsal (harici) olarak gruplandırılabilmektedir.

İçsel (dahili) tehditler

Bilgi güvenliği tehditleri arasında, kurum bünyesinde çalışan kişilerin oluşturabileceği bilinçli veya bilinçsiz tehditler olarak tanımlanabilen iç tehditler, oldukça önemlidir. Bilinçli tehditler iki şekilde oluşabilir. Birincisi, kurumda çalışan kötü niyetli bir kişinin kendisine verilen erişim haklarını kötüye kullanmasını içerir. İkincisi ise, bir kişinin başka birine ait erişim bilgilerini elde ederek, gerçekte erişmemesi gereken bilgilere erişerek kötü niyetli bir davranış gerçekleştirmesini kapsar. Veritabanı yöneticisinin, eriştiği verileri çıkar amacıyla başka bir firmaya satması ilk gruba verilecek örnektir. Veritabanı yöneticisi olmayan ve normalde veritabanına erişim hakkı bulunmayan bir kişinin, erişim bilgilerini bir şekilde elde ederek verilere ulaşması ve bunu çıkarı için kullanması ikinci gruba örnektir (http://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/bilisim-sistemleri-guvenligi-arastirmalarinin-yonu.html, Kara M, Bahşi H. Bilgi Sistemleri Güvenliği Araştırmalarının Yönü, e.t:02.12.2016).

Kurum çalışanlarının yanı sıra kurumda geçici olarak çalışanlar, iş ortakları, danışmanlar, taşeronlar ve tedarikçiler de iç tehdit unsuru yaratan gruplar arasında sayılabilir. Yapılan birçok araştırma, bilgi güvenliği sorunlarının çoğunlukla içsel kaynaklı olduğunu ortaya koymaktadır. Örneğin; yapılan bir araştırmaya göre güvenlik ihlallerinin yaklaşık yarısının yetkili kullanıcılar tarafından gerçekleştirildiği görülmüştür (Baraz 2015, s.146). Başka bir araştırmada, mevcut ve eski çalışanlarının ciddi tehlike oluşturduğu da bildirilmiştir (Yıldız 2009, s.18).

Dışsal (harici) tehditler

Dışarıdan gelen saldırılar çeşitlidir. Örneğin bilgisayar korsanları müşteri listelerine veya kurum için önemli olan projelere ulaşıp rakiplere satmaya çalışabilir (Baraz 2015, s.146).

Güvenlik olayları genel olarak aşağıdaki gibi 6 kategoride ele alınmaktadır (Vardal 2009, s.23-24):

- **Çalışan sahtekârlığı:** Çalışanlar tarafından sahtekârlığa yönelik aktiviteleri içeren olaylar.
- **Kayıp:** Fiziksel medyaların örneğin disklerin, donanımların veya basılı materyallerin, sistemde yer alan bilgilerin, tahrip edilmesini veya kaybolmasını içeren olaylar.
- **Taklit:** Bir kişinin farklı bir kişi ya da kurum gibi kendini tanıtarak gerçekleştirilen olaylar.
- **Hırsızlık:** Fiziksel medyaların örneğin; disklerin, ekipmanların veya basılı materyallerin çalınmasını içeren olaylar.
- **Yetkisiz açıklama (ifşa):** Bilinmeyen veya yetkisiz kişilere bilginin gösterilmesini içeren olaylar.
- **Sızma/Nüfuz etme:** Bilgisayar yazılımına, sistemine veya ağına sızma olayları.

4.1.2. Bilgi Güvenliğine Yönelik Önlemler

Bilgi güvenliğinde alınması gereken önlemler aşağıdaki şekilde sıralanabilir (Baraz 2015, s.147):

- **Yedekleme:** Bilgi kaybını önlemenin en kolay yoludur. Kayıpları önlemek için önemli bilgileri içeren dosyaların sistemli bir şekilde çoğaltılmasını sağlar.
- **Anti-virüs programları:** Bilgisayarları, virüslere, solucanlara ve truva atları gibi kötü amaçlı yazılımlara karşı korumaya yardımcı olur.

- **Güvenlik duvarı:** Bilgisayar ile internet arasında veya bilgi işlem sistemi ile internet arasında sanal bir duvar oluşturarak her iki tarafa aktarılan verileri denetler. İzinsiz giriş denemelerini önler.
- **Fiziksel güvenlik:** Fiziksel önlemler ile (güvenli alan, kartlı geçiş, güvenlik kameraları vb.) güvenliğin sağlanmasıdır.
- **Erişim denetimi:** Şifreleme, E-imza, akıllı kart, tek kullanımlık parola gibi erişimin denetlenmesini sağlayan araçların kullanılmasıdır.
- **Yönetsel önlemler:** Kuruma ait bilgi güvenliği politikalarının oluşturulması, standartlar ve prosedürlerin belirlenmesi ve çalışanlarda farkındalık yaratılarak bilgi güvenliğinin sağlanmasıdır.

4.1.3. Bilgi Güvenliği Yönetimi ve Standartlar

Bilgi güvenliği yönetimi, kurumun hassas bilgilerini yönetebilmek için benimsenen sistematik bir yaklaşımdır. Bu sistemin temel amacı, hassas bilginin korunmasıdır. Bu sistem çalışanları, iş süreçlerini ve bilgi teknolojileri sistemlerini kapsar (Sağlık Bakanlığı 2014, s.11).

Bilgilerin gizliliğini korumak ve güvenliğini sağlamak için kuruluşlara, bilgi güvenliği yönetim sistemi kurma ve işletme konusunda yol gösterici olmak üzere önemli standartlar ve yasal düzenlemeler oluşturulmuştur (Baraz 2015, s. 158).

Standartların kullanım nedenleri

Kurumların bilgi güvenliğinin sağlanmasında karşılaştıkları zorluklar aşağıdaki gibi sıralanabilir (http://bilgiguvenligi.gov.tr/bt-guv.-standartlari/bilgi-guvenligi-standartlari.html, Poşul A. Bilgi Güvenliği Standartları, e.t:16.12.2016):

- İşletmelerin düşük maliyetli ve yüksek verimli sistemlere duydukları ihtiyaç,
- Hızla değişen teknoloji ile temellendirilmiş bilgisayarların, uygulamaların ve ağ yapılarının yüksek tehdit altında bulunmaları,
- İşletmelerin beceri, kaynak ve uzmanlık bakımından bilgi güvenliğini sağlamadaki yetersizlikleri,

- Teknolojik sistemlerin, sürekli saldırıya maruz kalmaları ve açıklıklarının keşfedilmeleri.

Yürürlükteki standartlar

Health Insurance Portability and Accountability (HIPAA): Sağlık sektöründeki bilgi güvenliğini sağlamak için uygulanmaya başlanan HIPAA'ya göre bireylerin korunmuş sağlık bilgilerini aktaran kurumlar, internet uygulamaları veya elektronik sistemler vasıtasıyla HIPAA standartlarının yükümlülüklerini yerine getirmek zorundadırlar. Bu kurumlar, sağlık sigortaları, eczaneler, tıbbi cihaz satan ve kiralayan şirketler, muayenehaneler, hastaneler vb. gibi kurumlar olabilir. HIPAA, bireylerin sağlık bilgilerini korumak için mahremiyete ve güvenliğe uygun olarak geliştirilen bir takım idari, fiziksel ve teknik önlemler ile ilgili standartlardır (http://bilgiguvenligi.gov.tr/bt-guv.-standartlari/bilgi-guvenligi-standartlari.html, Poşul A. Bilgi Güvenliği Standartları, e.t:16.12.2016).

- **İdari önlemler:** Birimlerin denetlenmesi ve gerekli prosedürlerin yazılması için bir yöneticinin atanması, korunması gereken sağlık bilgilerine kimlerin ulaşıp kimlerin ulaşmayacağının belirlenmesi, organizasyon ile beraber çalışan diğer kurumların da bu standartlara uyacağına dair anlaşmaların yapılması ve veri üzerinde zarar tespiti yapabilmeleridir.
- **Fiziksel önlemler:** Cihazların ağ çalışma gruplarına katılırken ya da gruplardan çıkarılırken gereken önlemlerin alınması, sağlık bilgilerini içeren cihazlara ulaşımın dikkatlice kontrol edilmesi, izlenmesi ve bu cihazlara ulaşımın yetkilendirilmiş kişiler tarafından sağlanmasıdır.
- **Teknik önlemler:** Sağlık bilgilerini içeren cihazların, siber saldırılara karşı korunması, bu bilgilerin ağ üzerinden akması halinde, şifreleme yöntemlerinin kullanılması, her birimin sağlık verilerinin değişmeyeceği veya hareket ettirilmeyeceğine dair güvence vermesi, risk yönetiminin ve analizlerinin belgelendirilmesidir.

4.2. Mahremiyet Kavramı

Mahremiyet kavramı; bireyin yalnız bırakılma hakkı (Akgül 2014, s.71) ya da bireyin herkesle paylaşamayacağı veya herhangi bir kimse ile paylaşmama hakkının bulunduğu olay ve inançlarının, ancak isteği üzerine o kişiyle paylaşılması olarak tanımlanabilir (Küzeci 2010, s.14). Mahremiyet kendi başına önemli ve değerlidir. Mahremiyet; bireyin beden ve zihinsel bütünlüğüne erişilmesine bir sınır koyması anlamına da gelmektedir. Mahremiyet hakkı ise, kişilerin korumak, kontrol etmek ve saklamak istediği düşünceleri, duyguları ve beden bütünlüğüyle ilgili bir haktır (Bahçecik 2011, s.139).

Bireyin kendi durumu ile ilgili maddi ve manevi varlıklara, yine kendisiyle ilgili bütün bilgilere, diğer bireylerin erişimine sınır koyduğu alanlarda mahremiyet başlamaktadır. Mahremiyet kavramının ‘‘gizlilik’’ ve ‘‘sır’’ kavramları ile yakından ilgisi vardır (Çobanoğlu 2010, s.512).

Bilgi ve iletişim teknolojilerinin gelişmesiyle birlikte veri toplama ve bunları otomatik olarak işleme kapasitelerindeki artış, kişilerin mahremiyet alanının (özel hayat) savunmasız hale gelmesine sebep olmaktadır. Özellikle bilişim teknolojilerindeki gelişmeler sonucunda, verilere erişim, paylaşım ve transferinin çok kolaylaştığı bir ortamda kişisel verilerin meta haline gelmesi ve kişisel verileri hedef alan ya da bunları kullanmak suretiyle işlenen suç olaylarının artması kişilerin mahremiyet alanını ciddi derecede daraltmış ve kişisel verilerin korunması ihtiyacını doğurmuştur (http://www.tccb.gov.tr/ddk/ddk56.pdf, Devlet Denetleme Kurulu 2013, s.778-779, e.t:04.12.2016).

4.3. Kişisel Verilerin Korunması

Kişisel verilerin korunması, günümüz bilgi ve iletişim teknolojileri karşısında kişisel bilgileri sınırsız bir şekilde toplanan, kullanılan, devredilen bireyin korunmasını amaçlamaktadır. Bu bağlamda kişisel verilerin korunması hakkı, genellikle ‘‘özel yaşamın gizliliği hakkı’’ kapsamında değerlendirilmektedir (Küzeci 2015, s.43).

Bir temel hak olarak bireyin kişisel verilerinin korunması hakkı, ilgilinin rızası olmadan kişisel verilerine yapılan saldırılar karşısında bireyin korunmasını amaçlamaktadır (Akgül 2013, s.25). Kişisel verilerin korunmasının altında ‘‘mahremiyet’’ anlayışı bulunduğu için, özel yaşamın korunmasına ilişkin düzenlemelerin aynı zamanda kişisel veriler üzerinde de etkisi olduğu görülmektedir (Dülger 2015, s.47).

Kişisel verilerin işlenmesine ilişkin ilkeler aşağıdaki gibi sıralanabilir (Küzeci 2015, s.40):

- Hukuka ve dürüstlük kurallarına uygun işleme,
- Doğru ve gerektiğinde güncel olarak tutulma,
- Amacın gerektirdiğinden daha uzun süre tutulmama,
- Toplanma ve işlenme amaçlarına uygun, ilgili olma, aşırı olmama.

Kişinin özel yaşamının korunması, bir uluslararası anlaşmada ilk kez ‘‘Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi’’ nde düzenlenmiştir (Keser vd. 2014, s.39). Beyannamenin 12. Maddesi; *‘‘Hiç kimsenin özel yaşamına, ailesine, evine ya da yazışmasına keyfi olarak karışılamaz, onuruna ve adına saldırılamaz. Herkesin, bu gibi müdahale ya da saldırılara karşı yasa tarafından korunma hakkı vardır’’* hükmü getirmektedir (https://www.tbmm.gov.tr/komisyon/insanhaklari/pdf01/203-208.pdf, e.t:01.12.2016). Avrupa Konseyi de ‘‘Avrupa İnsan Hakları Sözleşmesi’’ ni (AİHS) hazırlayarak kişisel verileri koruma altına almıştır (Keser vd. 2014, s.39; http://www.danistay.gov.tr/upload/avrupainsanhaklarisozlesmesi.pdf e.t:01.12.2016).

Bilgi ve iletişim teknolojilerindeki artışla beraber, kişisel verilerin korunmasına yönelik daha kapsamlı uluslararası düzenlemelere ihtiyaç duyulmuş ve ülkemizin de üyesi olduğu Avrupa Konseyi tarafından ‘‘108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunmasına Dair Sözleşme’’ hazırlanmıştır. Sözleşme bu alanda bağlayıcılığı olan ilk düzenleme olup, bu alandaki kuralların üretiminde temel oluşturmaktadır (Dülger 2016, s.105; http://www2.tbmm.gov.tr/d24/1/1-0966.pdf, e.t:01.12.2016).

Türkiye’de kişisel verilerin korunması, 2010 yılından itibaren açıkça anayasal bir hak olarak düzenlenmiştir. Anayasanın 20. Maddesine eklenen son fıkra şöyledir; *‘‘Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu*

hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir" (Küzeci 2015, s.52; https://www.tbmm.gov.tr/anayasa/anayasa_2011.pdf, e.t:01.12.2016). Madde, kişisel verilerin ancak kanuna dayalı düzenlemelerle işlenebileceğini ve kişisel verilerin mutlak korunmasını öngörmektedir. Aynı zamanda kişisel verilerin ancak bireyin açık rızası (onam) ile işlenebileceğini ifade etmektedir.

4.4. Hassas Veri Olarak Kişisel Sağlık Verileri

Kişisel Veri

Belirli ya da belirlenebilir nitelikteki bir kişiye ilişkin her türlü bilgiyi ifade eden kişisel veri, ulusal ve uluslararası birçok hukuki düzenlemede benzer şekilde ele alınmıştır (Akgül 2013, s.23). Türkiye'de 24 Mart 2016 yılında kabul edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3(d) Maddesinde de kişisel veri; *''Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi''* olarak tanımlanmıştır (T.C. Resmi Gazete, 07 Nisan 2016, Sayı:29677).

Bireyin kişisel verileri, özünde bireyin kimliğini ortaya çıkartan, bir kişiyi belirli kılan ve onu karakterize eden verilerdir. Örneğin; kişinin adı, adresi, doğum tarihi, medeni hali, mesleği, e-posta adresi, banka bilgileri, emeklilik, kurum sicili ve vergi numarası, parmak izi, eğitim bilgileri, sağlık verileri, sosyal güvenlik numarası, genetik bilgileri, telefon mesajları, sosyal paylaşım sitelerinde yazdığı veya paylaştığı yazı, fotoğraf, ses veya görüntü kayıtları kişisel veri kapsamında ele alınmaktadır (Akgül 2014, s.8-9). Bu nedenle bireyin bu veriler üzerindeki denetim yetkisini kaybetmesi bireyin özgürlüğünün, özerkliğinin, mahremiyetinin kısaca ''ben'' olma özelliğinin kaybedilmesine sebep olur (İzgi 2014, s.29).

Veri belirli ya da kimliği belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek ya da kaynağı belirlenemeyecek duruma geldiğinde ona, ''anonim veri'' adı verilmektedir. Araştırma, istatistik, planlama vb. amaçlarla depolanan ve herhangi bir

kişiyi belirtmekten ziyade kitlesel bir bilgi yığını olarak ortaya çıkan bu tür veriler, ilgili kişilerle ilişkilendirilmeleri mümkün olmadığı için kişisel veri sayılmamaktadır (Dülger 2015, s.50).

Ulusal ve uluslararası birçok hukuki düzenlemede, bireyin kişisel verilerinden bir kısmı ‘‘hassas veri’’ olarak kabul edilmiştir ve özel olarak korunmaya alınmıştır. Bu kategoride yer alan veri türleri genel olarak ilgili kişinin;

- Siyasi görüşüne,
- Dinsel veya felsefi inancına,
- Irksal ya da etnik kökenine,
- Sendikal üyeliğine,
- Sağlık ve cinsel yaşamına ilişkin bilgiler bu grupta yer alır. Bu bilgilerin işlenmesi kural olarak yasaktır, fakat bazı sınırlı durumlarda işlenmeleri olanaklıdır (Küzeci 2015, s.41).

Kişisel Sağlık Verileri

6698 sayılı Kişisel Verilerin Korunması Kanunu’nun ‘‘Özel nitelikli kişisel verilerin işlenme şartları’’ başlıklı 6. Maddesinde; *‘‘(1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir. (2) Özel nitelikli kişisel verilerin, ilgilinin açık rızası olmaksızın işlenmesi yasaktır’’* düzenlemesine yer verilmiştir (T.C. Resmi Gazete, 07 Nisan 2016, Sayı:29677). Bu maddeden de anlaşılacağı üzere kişiye ait sağlık verileri ‘‘özel nitelikli kişisel veriler’’ olarak ifade edilmektedir.

Bireyin kişisel verilerinden bir kısmını oluşturan kişisel sağlık verileri, bireyin ‘‘hassas verileri’’ içerisinde yer almaktadır. Kişisel sağlık verileri, bireyin hastalıklı ya da sağlıklı olduğuna ilişkin bilgi içerebileceği gibi ölümüne ilişkin bilgileri de içerebilir. Sağlık kuruluşları, sağlık hizmetinin sunumu sırasında birey hakkında birçok bilgi toplamakta, bu bilgileri değerlendirmekte ve kayıt altına almaktadır. Çünkü bireyin tedavisinin başarıya ulaşmasında bireye ait sağlık verileri hayati öneme sahiptir (Akgül 2013, s.21-22). Kişinin yaşadığı sağlık sorunu, hekim ile

arasındaki ilişkisi, kullandığı ilaçlar, hastalığının ne olduğu, kendisine uygulanan tedavi, vücut özellikleri, tahlil ve görüntüleme sonuçları ‘‘bireyin özel hayatının gizliliği ve korunması hakkı’’ kapsamına girmektedir. Bu alan prensip olarak mutlak dokunulmaz olup, hem ulusal hem de uluslararası birçok hukuki düzenlemede koruma altına alınmıştır (http://www.kisiselsaglikverileri.org/hakkinda.php?id=32, Türk Tabipleri Birliği Kişisel Sağlık Verileri Çalışma Grubu, Sağlık Hizmetlerinde Kişisel Veri Toplanması, Korunması ve Değerlendirilmesi, e.t:05.12.2016).

Kişinin sağlığı hakkında veriler hassas kişisel veri olduğu için yüksek düzeyde koruma altındadır. Bu sebeple, bu verilerin işlenmesine diğer veri türlerinden farklı olarak daha fazla sınırlama getirilmektedir (Akgül 2014, s.278).

4.5. Kişisel Sağlık Verilerinin Erişimi, Korunması ve Hasta Mahremiyeti

Sağlık hizmetlerinde bireylerin özel hayatlarının gizliliği (mahremiyet) hakkı bireyin bu hizmeti almak üzere sağlık kuruluşu ile temasa geçtiği ilk andan itibaren başlar. Hizmetin sunulması sürecinde ve sonrasında devam eder. Sağlık hizmetleri sürecinde bireyin özel hayatı ile ilgili edinilen bilgiler, hastanın fiziksel ve ruhsal sağlığı, davranışları, cinsel ilişkileri gibi ‘‘hassas’’ bilgileri içerdiği için bireyler, bu süreçte daha çok özel hayatı ile ilgili bilgilerin açıklanmaması, bilinmemesi ve bu bilgilere başkaları tarafından ulaşılmaması talebindedir (Sert 2008, s.81-82).

Sağlık Çalışanları İçin Sağlık Hizmetinde Gizliliğe ve Mahremiyete İlişkin Avrupa Kuralları Rehberi’nde kişisel sağlık verileri ile ilgili temel ilkelere yer verilmiştir. Bunlardan bazıları aşağıdaki gibidir:

- **Rıza (onam) alınması:** Hasta bilgisinin kullanılması ile ilgili olarak hastadan ya da hukuki temsilcisinden onay alınmalıdır.
- **Hastanın bilgilendirilmesi:** Veriler sadece belirli amaçlar için toplanabilir. Bu amaç ayrıntılı bir biçimde tanımlanmalı ve verisi işlenecek olan kişi anlayabileceği bir dilde bilgilendirilmelidir.
- **Hasta kimliğinin gizlenmesi ve anonimleştirme:** Hastanın kimlik bilgileri saklanmalı ve kimlik bilgisinin korunması için gerekli önlemler alınmalıdır.

- **Erişim ve düzeltme:** Kişiler kendileriyle ilgili bilgilere erişme, bu bilgileri düzeltme hakkına sahip olmalıdır.
- **Güvenlik:** Toplanan verilere yönelik güvenlik tehditlerine karşı en gelişmiş önlemler alınmalı ve uygulanmalıdır. Sağlık çalışanları hasta mahremiyetine yönelik gerekli politika ve protokolleri uygulayarak hasta bilgilerinin gizliliğini sağlamalıdır. Ayrıca sağlık çalışanları, hastalar, hastaların hukuki temsilcileri ve kendi meslektaşları ile iletişim halindeyken, mahremiyeti ve bilgi güvenliğini göz önünde bulundurmalıdır. Üçüncü kişilerle verilerin paylaşımı, ancak alıcı tarafında uygun veri koruma prensiplerini uygulaması durumunda söz konusu olmalıdır (http://www.kisiselsaglikverileri.org/hakkinda.php?id=32, Türk Tabipleri Birliği Kişisel Sağlık Verileri Çalışma Grubu, Sağlık Hizmetlerinde Kişisel Veri Toplanması Korunması ve Değerlendirilmesi, e.t:05.12.2016).

Kişisel sağlık verilerinin mahremiyeti; bireyin diğer insanların bilmesini istemediği, teşhis ve tedavi sırasında elde edilen bilgilerin gizliliğin korunması ile alakalı bir mahremiyet türüdür (Çobanoğlu 2010, s.518). Sağlık kurumlarındaki tıbbi hasta dosyaları, ilaç reçeteleri, tıbbi test kayıtları veya ödeme kayıtlarındaki tıbbi bilgilerin saklanması, korunabilmesi ve yayılması mahremiyet açısından üzerinde durulması gereken önemli bir konudur. Tıbbi bilgilerin gizliliğinin korunması yönündeki çalışmaların yetersiz kalması hastanın mahremiyetini tehdit etmektedir (Bahçecik 2011, s.139).

Türkiye'de sağlık bilgilerinin mahremiyetinin korunması ''Hasta Hakları Yönetmeliği''nde açıkça düzenlenmiştir. Yönetmeliğin konuyla ilgili maddeleri şöyledir (T.C. Resmi Gazete, 01 Ağustos 1998, Sayı:23420):

*''**Mahremiyete Saygı Gösterilmesi Madde 21-** Hastanın mahremiyetine saygı gösterilmesi esastır. Ölüm olayı, mahremiyetin bozulması hakkını vermez.*

***Bilgilerin Gizli Tutulması Madde 23-** Sağlık hizmetinin verilmesi sebebiyle edinilen bilgiler, kanun ile müsaade edilen haller dışında, hiçbir şekilde açıklanamaz.''*

Tıpta gizliliği korumanın en önemli yöntemi, hasta mahremiyetini ve gizliliğini bir hasta hakkı olarak benimseyen sağlık çalışanlarının varlığıdır. Bundan dolayı her

düzeydeki sağlık çalışanı bu konuda yükümlülük taşımaktadır (Çobanoğlu 2010, s.520). Sağlık hukukunda kişisel verilerin korunması, özellikle hasta mahremiyeti ve hekimin ‘‘sır saklama’’ yükümlülüğü açısından önem arz etmektedir (Dülger 2015, s.59). Sır saklama yükümlülüğü hastanın hekime rahat başvurabilmesi, herhangi bir endişe, korku duymadan sağlık hizmetinden yararlanabilmesi için getirilmiştir. Bundan dolayı hekim, mesleğini icra ederken öğrendiği ve gizli tutulmasında hastanın çıkarı olan, açıklanması halinde hastayı maddi ve manevi olarak zarara uğratacak sırları saklamakla yükümlüdür (http://www.kisiselsaglikverileri.org/hakkinda.php?id=32, Türk Tabipleri Birliği Kişisel Sağlık Verileri Çalışma Grubu, Sağlık Hizmetlerinde Kişisel Veri Toplanması Korunması ve Değerlendirilmesi, e.t:05.12.2016).

Tıbbi deontoloji Tüzüğün 4. Maddesi ile *‘‘Tabip ve diş tabibi, meslek ve sanatının icrası vesilesiyle muttali olduğu sırları, kanuni mecburiyeti olmadıkça, ifşa edemez. Tıbbi toplantılarda takdim edilen veya yayımlarda bahis konusu olan vakalarda, hastanın hüviyeti açıklanamaz’’* hükmü getirilmekte ve hastanın gizli bilgilerinin korunması gerekliliğini düzenlemektedir (Tengilimoğlu 2016, s.91; http://www.mevzuat.gov.tr/MevzuatMetin/2.3.412578.pdf, e.t:01.12.2016). Hekimin hastasına ilişkin bilgileri saklı tutması, mesleki değer ve etik görevi olarak kabul edilmesine rağmen, gelişen bilişim teknolojileri ve tıbbın etkisiyle ‘‘sır saklama’’ yerine getirilmesi zor bir yükümlülük haline gelmiştir. Çünkü günümüzde hastalara ait tıbbi kayıtlar sadece hekimlerin elinde değildir. Sağlık hizmetlerinin bir ekip işi olması hastalara ait kayıtların bilgisayar ortamına yüklenmesini gerekli kılmıştır (Çobanoğlu 2010, s.515).

Hastanın tıbbi bilgilerinin açıklanmasının gerekli olduğu durumlar da vardır. Genel olarak iki istisnai durumda (yasal zorunluluk dışında) hekim hastasına ilişkin bilgileri açıklamak zorundadır (Çobanoğlu 2010, s.515):

- Belirli bir kişi/kişilerin zarar görmesi,
- Toplumun sağlığının tehlikeye girmesi durumlarında bilgiler açıklanabilir.

Kişisel sağlık verilerinin hangi durumlarda ilgilinin açık rızası aranmaksızın işlenebileceği durumlar 6698 sayılı Kişisel Verilerin Korunması Kanunu’nun ‘‘Özel nitelikli kişisel verilerin işlenme şartları’’ başlıklı 6. Maddesinde; *‘‘(3) Sağlık ve*

cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebilir'' şeklinde ifade edilmiştir (T.C. Resmi Gazete, 07 Nisan 2016, Sayı:29677).

Sağlık hizmetinin sunumu sırasında kişisel sağlık verilerinin hukuka aykırı olarak işlenmesi, açıklanması ya da muhafaza edilmemesi gibi nedenlerle uğranılan zararın idarece tazmin edilmesi gerekmektedir (Akgül 2013, s.42-43).

Kişisel verilerin korunması ve veri mahremiyetinin sağlanmasına yönelik T.C. Sağlık Bakanlığı tarafından ‘‘Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik’’ çıkarılmıştır. Yönetmeliğin amacı; *‘‘**Madde 1-** Kişisel verilerin korunması ve veri mahremiyetinin sağlanmasına, kişisel sağlık verilerinin işlenmesine, bu verilere erişim için kurulacak sisteme, kişisel sağlık verisi kaydı tutulan sistemlerin güvenliği ve denetimi ile sağlık hizmeti sunumundaki personel hareketlerinin Bakanlığa bildirilmesine ilişkin işlemlerde uyulacak usul ve esasları düzenlemektir''* şeklinde tanımlanmaktadır (T.C. Resmi Gazete, 24 Kasım 2017, Sayı:30250). Yönetmelikte kanun; *‘‘**Madde 4-** (d) 6698 sayılı Kişisel Verilerin Korunması Kanununu''* ifade etmektedir. Aynı zamanda, kişisel sağlık verilerinin işlenmesi; *‘‘**Madde 4-** (g) Kişisel sağlık verilerinin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi sağlık verileri üzerinde gerçekleştirilen her türlü işlem''* olarak tanımlanmaktadır (T.C. Resmi Gazete, 24 Kasım 2017, Sayı:30250).

Yönetmeliğin üçüncü bölümü; ‘‘Kişisel Sağlık Verilerinin Korunması, İşlenmesi, Aktarılması ve Silinmesi’’ başlığı altında toplanmıştır. Yönetmeliğin konuyla ilgili bazı maddeleri şöyledir (T.C. Resmi Gazete, 24 Kasım 2017, Sayı:30250):

*''**Kişisel Sağlık Verilerinin Korunması Madde 6-** (1) Veri işleyen; kişisel sağlık verilerinin hukuka aykırı olarak işlenmesini önlemek, kişisel sağlık verilerinin muhafazasını sağlamak amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbiri almak, aldığı bu tedbirlerin veri sorumlusu tarafından denetlenmesine izin vermek zorundadır. Veri işleyen, bu görevinin gereği olarak öğrendiği kişisel verileri Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işletme amacı dışında kullanamaz. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.*

***Kişisel Sağlık Verilerinin Aktarılması Madde 8-** (1) Kişisel sağlık verileri ancak Kanunun 8 inci ve 9 uncu madde hükümleri uyarınca aktarılabilir. (2) Kişisel sağlık verileri, Kanunun 8 inci ve 9 uncu madde hükümlerinde yer alan şartların sağlanamaması halinde ancak anonim hale getirilmek suretiyle aktarılabilir.''*

Sonuç olarak; gelişen ve büyüyen sağlık sistemi ve bu sistem içinde yer alması gereken bilgi ve iletişim teknolojileri, hasta mahremiyetinin sağlanması konusunda güçlüklere neden olmaktadır. Hastanın sağlık kuruluşuna başvurması, tetkikleri, yatışı, takibi, taburcu edilmesi, tıbbi girişimleri vb. uygulamalarda görev alan pek çok sağlık çalışanının olması ve hastaya ait bilgilerin elektronik ortamda tutulması, hastanın mahremiyetinin korunmasını güçleştirmektedir (Sert 2008, s.86-87).

5. SAĞLIK BİLGİ SİSTEMLERİNDE BİLGİ GÜVENLİĞİ ve HASTA MAREMİYETİNİN ÖNEMİ

Sağlık sektöründe bilgi ve iletişim teknolojilerinin hissedilir şekilde kullanılmasıyla birlikte, teknolojinin taşıdığı bazı riskler de ortaya çıkmıştır. Elektronik ortamdaki tüm veriler gibi, kişisel sağlık bilgilerini tehdit eden riskler için güvenlik önlemlerinin alınması zorunlu hale gelmiştir. Kişisel sağlık bilgileri, kişinin doğum öncesinden ölüm sonrasına kadar geçen süreyi kapsayan sağlık bilgilerinin tümüdür. Sağlık kayıtlarının sayısallaştırılması kaliteli sağlık hizmetleri sunumu için bir gerekliliktir. Ancak güncel teknolojilerin kişisel sağlık bilgilerinin gizlilik, bütünlük ve erişilebilirlik risklerini artırmasından dolayı, sağlık bilgilerinin güvenliği sarsılmaktadır. Hiç şüphesiz ki sağlık bilgilerinin gizliliği esastır. Bu nedenle önlemlerin alınması, risklerin saptanıp en aza indirgenmesi zorunlu hale gelmiştir (Sağlık Bakanlığı 2014, s.1).

Türkiye Cumhuriyeti Sağlık Bakanlığı ‘‘bilgi güvenliğini’’ sağlamak için ‘‘Bilgi Güvenliği Politikaları Yönergesi’’ hazırlamıştır. Sağlık Bilgi Sistemleri Genel Müdürlüğü tüm kurum ve kuruluşlarda rehberlik ve danışmanlık desteği ile alt yapı geliştirme çalışmalarını yürütmektedir (Sağlık Bakanlığı 2014, s.11).

Bilgi güvenliğinin sağlanmasında yönetsel, teknik, idari, hukuki araçlar sistematik olarak kullanılmalıdır. Bilgi güvenliği bilinçlendirme süreci kurum içinde en üst seviyeden en alt seviyeye kadar çalışanların katılımını gerektirmektedir. Kurumun bilgi varlıklarına erişim gereksinimi olan herkes kullanıcı kategorisine girmektedir. Kullanıcılar, bilgi güvenliğinin sağlanmasında en büyük ve en önemli hedef kitledir. Kurum içindeki işler yürütülürken istemeden yapılan hatalar ve bilgi sisteminde oluşabilecek açıklıkları en aza indirmek onların elindedir. Yöneticiler, bilgi güvenliği bilinçlendirme ve eğitim sürecinin gereklerine, çalışanların uymasını sağlamakla sorumludur. Ayrıca başarılı ve etkin işleyen bir bilgi güvenliği süreci oluşturulabilmesi için bu alandaki görev ve sorumlulukların açık ve net bir biçimde belirlenmesi gerekmektedir (Sağlık Bakanlığı 2014, s.8).

Bilginin gizliliği, bütünlüğü ve erişebilirliğinin sağlanması olarak ifade edebileceğimiz ‘‘bilgi güvenliği’’ konusunda Uluslararası Standartlar Örgütü (ISO)

tarafından hazırlanan ISO 27000 serisi oldukça kapsamlı süreçler öngörmektedir. ISO 27799:2008 standardı ise, sağlık bilişimiyle ilgili olup, ISO/IEC 27002 kullanılarak sağlık sektöründe bilgi güvenliği yönetiminin nasıl gerçekleştirileceğini belirlemektedir (https://www.iso.org/standard/41298.html, e.t: 04.12.2016).

ISO 27799:2008 standardı son derece hassas olan kişisel sağlık bilgilerini ve bu bilgileri hem sağlık hizmetleri çalışanlarının erişiminin garanti edilmesi hem de gizliliğinin ve bütünlüğünün en doğru şekilde korunması konusunu değerlendirmekte ve bunu mümkün kılmak için eylem planı oluşturmaktadır. ISO 27799:2008, sağlık bilgilerinin saklanması, paylaşılması, şekillendirilmesi aşamasında gerekli olan tedbirlerin alınması ve güvenlik altında tutulması için kapsamlı standartlar da içermektedir. Ayrıca ilgili uluslararası standartları uygulayarak, sağlık hizmetleri kurumları ve sağlık bilgileri koruyucularına boyutlarına ve durumuna göre gerekli olan güvenlik şartlarını da sağlayabilmektedir (https://www.iso.org/standard/41298.html, e.t: 04.12.2016).

Özetle; ESK sistemlerinin faydalarının yanı sıra bu sistemlerin kullanımı, bir takım sorunları da beraberinde getirdiği de unutulmamalıdır. Bu sorunların başında güvenlik ve mahremiyet konuları gelmektedir. Elektronik ortamda toplanan sağlık kayıtları; hastanın kimlik bilgileri, uygulanmakta olan tedavi ve kullanılan ilaçlar, tıbbi geçmişi, ailesinin sağlık geçmişi, bağlı olduğu sosyal güvenlik kurumu, kişinin gelir düzeyi gibi devasa içerikte birçok güncel bilgiyi kapsamaktadır. Söz konusu bu bilgilerin istenilmeyen kişilerin eline geçmesi durumunda ‘‘özel hayatın gizliliği ilkesi’’ ne aykırı durumların ortaya çıkması olasıdır (Özata ve Güleş 2005, s.95). Güvenlik, ESK sisteminin korunması ve bilgi değişiminin sağlanması açısından ciddi bir durumdur. Güvenlik ile ilgili önlemler kurumsal düzeyde gizlilik ve güvenilirlik için desteğin sağlanması ve bilgisayardan kişisel sağlık bilgilerine ulaşmada kimlik denetiminin yapılması gerekir (Mumcu 2011, s.68).

Sağlık verilerinin güvenliği ve hasta mahremiyeti, ‘‘özel yaşamın gizliliği’’ hakkının önemli bir unsurunu oluşturmaktadır. Sırlarının ve kişisel verilerinin güvende olacağından emin olamayan hastanın, sağlık kurumlarına başvurmaktan vazgeçebileceği göz önünde bulundurulduğunda, meselenin yaşam hakkı bağlamında da önemli olduğu görülmektedir. Dolayısıyla bu konuda gerek ulusal gerekse uluslararası düzeyde birçok düzenleme yapılmıştır (Dülger 2015, s.78).

Türkiye'de kişisel sağlık verilerinin mahremiyetine ilişkin ana kaynak ''Hasta Hakları Yönetmeliği''dir. Yasa ile izin verilen durumlar ve tıbbi zorunluluklar dışında hastanın özel ve aile yaşamının gizliliğine dokunulamayacağı, hasta haklarına ilişkin ilkeler kapsamında yer almıştır. Hastanın mahremiyetine saygı gösterilmesi esastır. Bu kayıtlar yalnızca hastanın tedavisiyle doğrudan ilgili olanlar tarafından görülebilir. Hastaya ilişkin olarak sağlık hizmetlerinin sunumu sırasında edinilen bilgiler, yasayla izin verilen haller dışında hiçbir şekilde paylaşılamaz (Küzeci 2010, s.340-341).

Elektronik ortamda tutulan kişisel sağlık verilerinin güvenliğini sağlamak için aşağıdaki önlemlerin alınması gerekmektedir (Odacıoğlu 2016, s.55):

- Bilgi sistemlerinde yedekleme,
- Şifreleme,
- Kriz/Acil durum yönetimi,
- Veri tabanı güvenliği,
- Sunucu güvenliği,
- Kimlik doğrulama ve yetkilendirme,
- Kişisel sağlık bilgilerinin güvenliği.

Sonuç olarak; Sağlık bilgi sistemlerinde bilgi güvenliği ve mahremiyet konusu özellikle elektronik sağlık kayıtlarının kullanımının artmasıyla daha fazla önem kazanmıştır. Verilere çok sayıda sağlık dışı kuruluşların ulaşması, bilgi güvenliği ve mahremiyet ihlallerini de beraberinde getirmiştir (Esatoğlu 2014, s.195). Elektronik ortamların yarattığı olanaklar karşısında tıbbi verilerin başkaları tarafından elde edilmesi ve paylaşılması gittikçe daha da kolaylaşır hale gelmektedir. Hasta bilgilerinin başkaları tarafından biliniyor olması kabul edilebilir bir durum değildir. Bilgilerin depolanmasını sağlayan bilgi sistemlerinin değeri ve önemi açıktır. Bilgi ve iletişim teknolojilerinin artmasıyla oluşturulan iletişim ağlarının, hastaların kayıtlarının korunmasında sorunlar yaratabileceği ve sağlık bilgilerinin güvenliğinin nasıl sağlanacağı da her zaman tartışılacaktır (Bahçecik 2011, s.140).

6. GEREÇ ve YÖNTEM

Araştırma kesitsel tipte tanımlayıcıdır. Araştırmanın evrenini Bilgisayar Mühendisliği bölümünde öğrenim gören ve mesleki temel eğitimi almış 3. ve 4. sınıf öğrenciler oluşturmaktadır. Evren olarak seçilen Bilgisayar Mühendisliği öğrencileri sağlık hizmetlerinin gelecekteki paydaşları olarak nitelendirilmektedir. Araştırmacının İstanbul'da yaşaması ve bu şehirde eğitim veren bir Bilgisayar Mühendisliği bölümünün ülkedeki diğer bölümleri temsil edebilme yeteneğinin olmasından dolayı; örneklem grubunu Marmara Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği bölümü 3. ve 4. sınıf öğrencileri oluşturmaktadır. Kontrol grubu olarak aynı üniversitenin Tıp Fakültesi 5. ve 6. sınıf öğrencileri dâhil edilmiştir. Belirlenen fakültelerin dekanlıklarından çalışma yapılabilmesi için gerekli izinler alınmıştır. Örneklem ve kontrol grubunun tümüne ulaşılması amaçlanmıştır. Ancak araştırmaya katılım gönüllülük esasına dayanmaktadır.

Araştırmanın saha uygulaması Şubat 2017 – Nisan 2017 tarihleri arasında yapılmıştır. Araştırma verileri anket formu ile elde edilmiştir. Bilgilendirme formu ve onam formunun okunması ve araştırmaya katılımın kabulü sonrasında anket uygulaması aşamasına geçilmiştir. Bilgisayar Mühendisliği bölümünde öğrenim gören 189, Tıp Fakültesinde öğrenim gören 305 öğrenciden, araştırmaya katılmayı kabul eden 163 Bilgisayar Mühendisliği ve 65 Tıp öğrencisi ile anket formu kullanılarak yüz yüze görüşme yapılmıştır. Bilgisayar Mühendisliği öğrencilerinin %86'sı (n=163), Tıp öğrencilerinin %21'i (n=65) araştırmaya katılmıştır.

Araştırmada kullanılan anket formu; bilgi sistemleri, sağlık bilişim sistemleri, bilgi güvenliği ve mahremiyet konusunda yapılan araştırmalardan yola çıkılarak hazırlanan sorulardan oluşmaktadır. Anket formunda; öğrencilere ait sosyo-demografik özellikler ile sağlık bilgi sistemlerinde bilgi güvenliği ve hasta mahremiyetine yönelik sorular yer almaktadır.

Anket sorularının oluşturulmasında Anderson (2007), Appari ve Johnson (2010), Gebrasilase ve Lessa (2011), Kılıç Aksu vd. (2015), Lekkas ve Gritzalis (2007), Aldosarı'nın (2012) çalışmalarından ve T.C. Devlet Denetleme Kurulu'nun (2013, http://www.tccb.gov.tr/ddk/ddk56.pdf, e.t:04.12.2016) raporundan yararlanılmıştır.

Anket formu tez öğrencisi ve danışmanı tarafından geliştirilmiş ve uzman görüşleri dikkate alınarak hazırlanmıştır. Ancak, araştırmanın temel amacı, yeni bir ölçek geliştirmek ya da var olan bir ölçeğin geçerlilik ve güvenilirlik çalışmasını yapmak değildir. Araştırmanın temel amacı; ülkemizdeki mevcut durum ve güncel uygulamaları dikkate alarak bir durum değerlendirmesi yapmaktır.

Anket Formu iki kısımdan oluşmaktadır. Birinci kısımdaki 1–5 numaralı sorular, katılımcının sosyo-demografik özelliklerine yöneliktir. İkinci kısımda bulunan 6-38 numaralı sorular ise sağlık bilgi sistemlerinde bilgi güvenliği ve hasta mahremiyetine yönelik sorulardan oluşmaktadır. Anket formundaki 14 soru, 5'li Likert tipi puanlama (1:Kesinlikle katılmıyorum, 2:Katılmıyorum, 3:Kararsızım, 4:Katılıyorum, 5:Kesinlikle katılıyorum) ile değerlendirilmiştir. Anket formu pilot değerlendirme olarak 10 kişiye uygulanmış ve anketin anlaşılması ile ilgili bir sorunun olmadığı görülmüştür.

6.1. Araştırmanın Hipotezleri

Hipotez 1: Bilgisayar Mühendisliği ve Tıp öğrencileri arasında bilgi güvenliği ve mahremiyet konusunda görüş farkı yoktur.

Hipotez 2: Bilgisayar Mühendisliği ve Tıp öğrencilerinin sosyo-demografik özellikleri ile bilgi güvenliğinin ve hasta mahremiyetinin korunması konusundaki görüşleri arasında fark yoktur.

Hipotez 3: Bilgisayar Mühendisliği ve Tıp öğrencilerinin sağlık hizmeti almış olmaları, bilgi güvenliği ve hasta mahremiyeti ile ilgili görüşlerini etkilemez.

Hipotez 4: Bilgisayar Mühendisliği ve Tıp öğrencilerinin elektronik sağlık kayıt sistemleri ile ilgili bilgi düzeyleri arasında fark yoktur.

Hipotez 5: E-nabız uygulaması kullanımı bilgi güvenliği ve mahremiyete yönelik görüşleri etkilemez.

6.2. İstatistiksel Değerlendirme

Veriler SPSS 22,0'nin deneme sürümü ile analiz edilmiştir. Tanımlayıcı türde olan bu araştırmada kategorik verileri özetlemek için sıklık tabloları hazırlanmıştır.

Analizinde Ki-kare testi kullanılmıştır. Anket formunda yer alan ve 5'li Likert tipi puanlama ile değerlendirilen maddelerin puan değerleri, normal dağılıma uyduğu için ANOVA ve Eşleşmemiş T testi ile analiz edilmiştir. İstatistiksel anlamlılık düzeyi olarak $p<0.05$ alınmıştır.

6.3. Sınırlılıklar

Araştırma sonucu ortaya çıkan bulgular, araştırmanın yapıldığı dönemde araştırmaya katılmayı kabul eden öğrencilerin değerlendirmelerini kapsamaktadır.

7. BULGULAR

Bu kesitsel tanımlayıcı araştırmaya, 163 Bilgisayar Mühendisliği öğrencisi (yaş ort:22,44±1.42 yıl) ve 65 Tıp öğrencisi (yaş ort:23,38±1.20 yıl) katılmıştır.

Bilgisayar Mühendisliği öğrencilerinin %56,4'ü (n=92) erkek iken, Tıp öğrencilerinin %58,5'i (n=38) kadındır (p=0.042). Son 6 ay içinde sağlık hizmeti alma oranı Tıp öğrencilerinde (%75,4 n=49); Bilgisayar Mühendisliği öğrencilerine (%60,1 n=98) göre daha yüksektir (p=0.043).

Bilgisayar Mühendisliği öğrencilerinin %87,7'si (n=143) ve Tıp öğrencilerinin %76,9'u (n=50) SGK'lıdır. Bilgisayar Mühendisliği ve Tıp öğrencilerinin sosyal güvence bilgilerinin dağılımında istatistiksel olarak anlamlı farklılık bulunmamaktadır (p>0.05) (Tablo 1).

Tablo 1: Araştırma Grubunun Sosyo-Demografik Özellikleri

Değişkenler		**Bölüm**				**p***
		Bilgisayar Mühendisliği		**Tıp**		
		n	**%**	**n**	**%**	
Cinsiyet	Kadın	71	43,6	38	58,5	**0.042**
	Erkek	92	56,4	27	41,5	
	Toplam	163	100,0	65	100,0	
Son 6 ay içinde sağlık hizmeti aldınız mı?	Evet	98	60,1	49	75,4	**0.043**
	Hayır	65	39,9	16	24,6	
	Toplam	163	100,0	65	100,0	
Sosyal güvenceniz	SGK	143	87,7	50	76,9	0.069
	Özel sağlık sigortası	10	6,1	10	15,4	
	Sosyal güvence yok	10	6,1	5	7,7	
	Toplam	163	100,0	65	100,0	

* Ki-kare testi ile analiz edilmiştir.

Araştırma grubunun bölümlere göre *''elektronik sağlık kayıt sistemi üzerinden erişim sağlanan bilgi türlerine''* ilişkin görüşleri değerlendirildiğinde;

Bilgisayar Mühendisliği öğrencileri sistem üzerinden *''İletişim bilgilerini''* (%95,1 n=155); Tıp öğrencilerine (%87,7 n=57) göre daha yüksek oranda hastane çalışanları tarafından erişilebilir olduğunu düşünmektedir (p=0.050). Buna karşın Tıp öğrencileri sistem üzerinden *''Ameliyat raporlarını''* (%78,5 n=51) ve *''Laboratuar sonuçlarını''* (%93,8 n=61); Bilgisayar Mühendisliği öğrencilerine (%63,8 n=104 ve %81,0 n=132; sırasıyla) göre daha yüksek oranda hastane çalışanları tarafından erişilebilir olduğunu düşünmektedir (p=0.047 ve p=0.026 sırasıyla) (Tablo 2).

Bilgisayar Mühendisliği öğrencilerinin %95,1'i (n=155), Tıp öğrencilerinin %98,5'i (n=64) *''Kimlik bilgilerinin''*; Bilgisayar Mühendisliği öğrencilerinin %92,6'sı (n=151), Tıp öğrencilerinin %96,9'u (n=63) *''Muayene bilgilerinin''* hastane çalışanları tarafından erişilebilir olduğunu düşünmektedir (p>0.05) (Tablo 2).

''Önceden geçirilen hastalıklar'', *''Sosyal güvence bilgileri''* ve *''Ödeme bilgileri''*nde bölümlerin kendi içlerinde benzer şekilde değerlendirme yaptığı görülmektedir (p>0.05) (Tablo 2).

Tablo 2: Araştırma Grubunun Elektronik Sağlık Kayıt Sistemi Üzerinden Erişim Sağlanan Bilgi Türleri ile İlgili Görüşleri

Değişkenler		Bölüm				p*
		Bilgisayar Mühendisliği		Tıp		
		n	%	n	%	
İletişim bilgileri	Evet	155	95,1	57	87,7	**0.050**
	Hayır	8	4,9	8	12,3	
	Toplam	163	100,0	65	100,0	
Kimlik bilgileri	Evet	155	95,1	64	98,5	0.218
	Hayır	8	4,9	1	1,5	
	Toplam	163	100,0	65	100,0	
Muayene bilgileri	Evet	151	92,6	63	96,9	0.183
	Hayır	12	7,4	2	3,1	
	Toplam	163	100,0	65	100,0	
Ameliyat raporları	Evet	104	63,8	51	78,5	**0.047**
	Hayır	59	36,2	14	21,5	
	Toplam	163	100,0	65	100,0	
Laboratuar sonuçları	Evet	132	81,0	61	93,8	**0.026**
	Hayır	31	19,0	4	6,2	
	Toplam	163	100,0	65	100,0	
Önceden geçirilen hastalıklar	Evet	115	70,6	50	76,9	0.420
	Hayır	48	29,4	15	23,1	
	Toplam	163	100,0	65	100,0	
Sosyal güvence bilgileri	Evet	130	79,8	44	67,7	0.078
	Hayır	33	20,2	21	32,3	
	Toplam	163	100,0	65	100,0	
Ödeme bilgileri	Evet	95	58,3	36	55,4	0.690
	Hayır	68	41,7	29	44,6	
	Toplam	163	100,0	65	100,0	

* Ki-kare testi ile analiz edilmiştir.

Araştırma grubunun bölümlere göre *''elektronik sağlık kayıt sistemi üzerinden erişimin kısıtlanması gereken bilgi türlerine''* ilişkin görüşleri değerlendirildiğinde;

Tıp öğrencileri sistem üzerinden *''Muayene bilgilerini''* (%40 n=26) ve *''Önceden geçirilen hastalıklarını''* (%41,5 n=27); Bilgisayar Mühendisliği öğrencilerine (%25,8 n=42 ve %25,2 n=41; sırasıyla) göre daha yüksek oranda erişimin kısıtlanmasını istemektedir (p=0.050 ve p=0.023; sırasıyla) (Tablo 3).

Bilgisayar Mühendisliği (%81,0 n=132) ve Tıp (%78,5 n=51) öğrencilerinin çoğunluğu elektronik sağlık kayıt sistemi üzerinden *''Kimlik bilgilerinin erişiminin kısıtlanmasını''* istemektedir (p>0.05) (Tablo 3).

''İletişim bilgileri'', *''Ameliyat raporları''*, *''Laboratuar sonuçları''*, *''Sosyal güvence bilgileri* ve *''Ödeme bilgileri''*nde bölümlerin kendi içlerinde benzer şekilde değerlendirme yaptığı görülmektedir (p>0.05) (Tablo 3).

Tablo 3: Araştırma Grubunun Elektronik Sağlık Kayıt Sistemi Üzerinden Erişimin Kısıtlanması Gereken Bilgi Türleri ile İlgili Görüşleri

Değişkenler		Bölüm				p*
		Bilgisayar Mühendisliği		Tıp		
		n	%	n	%	
İletişim bilgileri	Evet	66	40,5	23	35,4	0.476
	Hayır	97	59,5	42	64,6	
	Toplam	163	100,0	65	100,0	
Kimlik bilgileri	Evet	132	81,0	51	78,5	0.805
	Hayır	31	19,0	14	21,5	
	Toplam	163	100,0	65	100,0	
Muayene bilgileri	Evet	42	25,8	26	40,0	**0.050**
	Hayır	121	74,2	39	60,0	
	Toplam	163	100,0	65	100,0	
Ameliyat raporları	Evet	41	25,2	20	30,8	0.484
	Hayır	122	74,8	45	69,2	
	Toplam	163	100,0	65	100,0	
Laboratuar sonuçları	Evet	57	35,0	26	40,0	0.575
	Hayır	106	65,0	39	60,0	
	Toplam	163	100,0	65	100,0	
Önceden geçirilen hastalıklar	Evet	41	25,2	27	41,5	**0.023**
	Hayır	122	74,8	38	58,5	
	Toplam	163	100,0	65	100,0	
Sosyal güvence bilgileri	Evet	43	26,4	20	30,8	0.614
	Hayır	120	73,6	45	69,2	
	Toplam	163	100,0	65	100,0	
Ödeme bilgileri	Evet	61	37,4	25	38,5	1.000
	Hayır	102	62,6	40	61,5	
	Toplam	163	100,0	65	100,0	

* Ki-kare testi ile analiz edilmiştir.

Araştırma grubunun bölümlere göre *''kişisel sağlık verilerinin korunması ve verilere erişim''* konusundaki görüşleri değerlendirildiğinde;

''Doktordan başka bir sağlık çalışanının sağlık kayıtlarına erişiminden" Bilgisayar Mühendisliği öğrencilerinin (%93,3 n=152); Tıp öğrencilerine (%78,5 n=51) göre daha fazla rahatsız olduğu belirlenmiştir (p=0.003). Ancak Bilgisayar Mühendisliği öğrencileri (%44,2 n=72); Tıp öğrencilerine (%60,0 n=39) göre daha az oranda *"Elektronik sağlık kayıtlarının eksik ya da yanlış bilgi içerdiğini"* düşünmektedir (p= 0.031) (Tablo 4).

Bilgisayar Mühendisliği öğrencilerinin %75,5'i (n=123), Tıp öğrencilerinin %78,5'i (n=51) *''Kullanılan sistem üzerinden kişisel sağlık verilerine erişimin''* denetlendiğini düşünmemektedir. *''Kişisel sağlık verilerinin paylaşımı için onamlarının''* alınmadığını belirten Bilgisayar Mühendisliği öğrencileri %94,5 (n=154), Tıp öğrencileri %89,2 (n=58) oranındadır. Bilgisayar Mühendisliği öğrencilerinin %94,5'i (n=154), Tıp öğrencilerinin %89,2'si (n=58) *''Kişisel sağlık verilerinin nerelerde kullanılabileceği konusunda''* bilgilendirme yapılmadığını belirtmiştir. *''Kişisel sağlık verilerinin diğer sağlık kurumlarıyla paylaşılmasından''* rahatsızlık duyan Bilgisayar Mühendisliği öğrencileri %74,2 (n=121), Tıp öğrencileri %70,8 (n=46) oranındadır (p>0.05) (Tablo 4).

Tablo 4: Araştırma Grubunun Kişisel Sağlık Verilerinin Korunması ve Verilere Erişim Konusundaki Görüşleri

Değişkenler		Bölüm				p*
		Bilgisayar Mühendisliği		Tıp		
		n	%	n	%	
Kullanılan sistem üzerinden kişisel sağlık verilerine erişimin denetlendiğini düşünüyor musunuz?	Evet	40	24,5	14	21,5	0.758
	Hayır	123	75,5	51	78,5	
	Toplam	163	100,0	65	100,0	
Kişisel sağlık verilerinizin paylaşımı için onamınız alınıyor mu?	Evet	9	5,5	7	10,8	0.134
	Hayır	154	94,5	58	89,2	
	Toplam	163	100,0	65	100,0	
Kişisel sağlık verilerinizin nerelerde kullanılabileceği konusunda bilgilendirme yapılıyor mu?	Evet	9	5,5	7	10,8	0.134
	Hayır	154	94,5	58	89,2	
	Toplam	163	100,0	65	100,0	
Kişisel sağlık verilerinizin diğer sağlık kurumlarıyla paylaşılmasından rahatsızlık duyar mısınız?	Evet	121	74,2	46	70,8	0.713
	Hayır	42	25,8	19	29,2	
	Toplam	163	100,0	65	100,0	
Sağlık kayıtlarınıza doktorunuzdan başka bir sağlık çalışanının erişiminden rahatsız olur musunuz?	Evet	152	93,3	51	78,5	**0.003**
	Hayır	11	6,7	14	21,5	
	Toplam	163	100,0	65	100,0	
Elektronik sağlık kayıt sistemindeki sağlık kayıtlarınızın, eksik ya da yanlış bilgi içerdiğini düşünüyor musunuz?	Evet	72	44,2	39	60,0	**0.031**
	Hayır	91	55,8	26	40,0	
	Toplam	163	100,0	65	100,0	

* Ki-kare testi ile analiz edilmiştir.

Araştırma grubunun bölümlere göre *''E-nabız uygulaması ile ilgili''* görüşleri değerlendirildiğinde;

Sağlık sorunlarıyla ilgili Bilgisayar Mühendisliği öğrencileri (%87,1 n=142); Tıp öğrencilerine göre (%66,2 n=43) *"Doktor ile elektronik ortamda daha fazla iletişim kurmayı"* istemektedir (p= 0.001) (Tablo 5).

Bilgisayar Mühendisliği öğrencilerinin %84,0'ü (n=137), Tıp öğrencilerinin %80,0'i (n=52) *''Kendilerine ait tüm sağlık verilerine E-nabız uygulaması gibi internet üzerinden''* erişmek istemektedir. Ancak Bilgisayar Mühendisliği (%63,2 n=103) ve Tıp (%53,8 n=35) öğrencilerinin çoğunluğu *''Bu tür bir erişimin bilgi güvenliği ve mahremiyet açısından sorun yaratacağını''* düşünmektedir (p>0.05) (Tablo 5).

Tablo 5: Araştırma Grubunun E-nabız Uygulaması ile İlgili Görüşleri

Değişkenler		**Bölüm**				**p***
		Bilgisayar Mühendisliği		**Tıp**		
		n	**%**	**n**	**%**	
Kendinize ait tüm sağlık verilerine E-nabız uygulaması gibi internet üzerinden erişmek ister misiniz?	Evet	137	84,0	52	80,0	0.590
	Hayır	26	16,0	13	20,0	
	Toplam	163	100,0	65	100,0	
Bu tür bir erişim bilgi güvenliği ve mahremiyet açısından sorun yaratır mı?	Evet	103	63,2	35	53,8	0.193
	Hayır	60	36,8	30	46,2	
	Toplam	163	100,0	65	100,0	
Doktorunuzla sağlık sorunlarınızla ilgili olarak elektronik ortamda iletişim kurmak ister misiniz?	Evet	142	87,1	43	66,2	**0.001**
	Hayır	21	12,9	22	33,8	
	Toplam	163	100,0	65	100,0	

* Ki-kare testi ile analiz edilmiştir.

Araştırma grubunun bölümlere göre *''hastanede yaşanan mahremiyet ihlalleri''* ile ilgili görüşleri değerlendirildiğinde;

Bilgisayar Mühendisliği öğrencilerinin çoğunluğu hastanede yaşanan mahremiyet ihlallerinin nedenlerini, *"Çalışanların bilgisizliğinden kaynaklı hatalar"* (%75,5 n=123) ve *''Dikkatsizlik''* (%71,8 n=117) olarak belirtirken; Tıp Öğrencileri *"Yoğunluk"* (%67,7 n=44) ve *"Sistemsel Problemler"* (%67,7 n=44) olarak belirtmiştir (Tablo 6).

Tablo 6: Araştırma Grubunun Hastanede Yaşanan Mahremiyet İhlalleri ile İlgili Görüşleri

***Hastanede yaşanan mahremiyet ihlallerinin nedenleri hangileri olabilir?**	**Bölüm**			
	Bilgisayar Mühendisliği		**Tıp**	
	n	**%**	**n**	**%**
Çalışanların bilgisizliğinden kaynaklı hatalar	123	75,5	37	56,9
Yoğunluk	98	60,1	44	67,7
Dikkatsizlik	117	71,8	32	49,2
Sistemsel problemler	105	64,4	44	67,7

* Bu soruda araştırma grubu tarafından birden fazla seçenek işaretlenmiştir.

Araştırma grubunun bölümlere göre *''mahremiyetlerinin ihlali halinde başvurmayı düşündükleri birimler''* ile ilgili görüşleri değerlendirildiğinde;

Bilgisayar Mühendisliği öğrencilerinin %62'si (n=101), Tıp öğrencilerinin %43,1'i (n=28) mahremiyet ihlali olduğunda *''Hastane yönetimine''* başvurulması gerektiğini düşünmektedir. Diğer başvuru alanları olarak; *''Sağlık Bakanlığına''* başvuranların oranı Bilgisayar Mühendisliği öğrencilerinde %53,4 (n=87), Tıp öğrencilerinde %35,4'tür (n=23). Bilgisayar Mühendisliği öğrencilerinin %25,2'si (n=41), Tıp öğrencilerinin %27,7'si (n=18) *''Hasta ve Hasta Hakları Derneği''* olarak belirtmiştir. *''Doktoruna''* başvurma oranı ise Bilgisayar Mühendisliği öğrencilerinde %8,0 (n=13), Tıp öğrencilerinde %18,5'tir (n=12) (Tablo 7).

Tablo 7: Araştırma Grubunun Mahremiyetlerinin İhlali Halinde Başvurmayı Düşündükleri Birimler

***Mahremiyetinizin ihlal edildiğini düşündüğünüz bir durumda nerelere başvurursunuz?**	**Bölüm**			
	Bilgisayar Mühendisliği		**Tıp**	
	n	**%**	**n**	**%**
Hastane yönetimine	101	62,0	28	43,1
Doktorunuza	13	8,0	12	18,5
Hasta ve Hasta Hakları Derneğine	41	25,2	18	27,7
Sağlık Bakanlığına	87	53,4	23	35,4

***** Bu soruda araştırma grubu tarafından birden fazla seçenek işaretlenmiştir.

Araştırma grubunun bölümlere göre *''sağlık kayıtlarının güvenliği''* ile ilgili görüşleri değerlendirildiğinde;

Bilgisayar Mühendisliği öğrencilerinin %82,8'i (n=135) ve Tıp öğrencilerinin %66,2'si (n=43) sağlık kayıtlarının güvenliğinden *''Devletin''* sorumlu olduğunu düşünmektedir. *''Hastaneyi''* sorumlu tutanların oranı Bilgisayar Mühendisliği öğrencilerinde %68,1 (n=111), Tıp öğrencilerinde %64,6'dır (n=42). Bilgisayar Mühendisliği öğrencilerinin %31,9'u (52), Tıp öğrencilerinin %38,5'i (n=25) *''Sağlık personelini''* sorumlu tutmaktadır. *''Kişinin kendisinin''* sorumlu olma oranı ise Bilgisayar Mühendisliği öğrencilerinde %9,2 (n=15), Tıp öğrencilerinde %12,3'tür (n=8) (Tablo 8).

Tablo 8: Araştırma Grubunun Sağlık Kayıtlarının Güvenliği ile İlgili Görüşleri

***Sağlık kayıtlarının güvenliğini sağlamaktan kimler sorumludur?**	**Bölüm**			
	Bilgisayar Mühendisliği		**Tıp**	
	n	**%**	**n**	**%**
Devlet	135	82,8	43	66,2
Hastane	111	68,1	42	64,6
Sağlık personeli	52	31,9	25	38,5
Kişinin kendisi	15	9,2	8	12,3

* Bu soruda araştırma grubu tarafından birden fazla seçenek işaretlenmiştir.

Araştırma grubunun bölümlere göre *''hasta hakları''* ile ilgili görüşleri değerlendirildiğinde; *''Hasta hakları ile ilgili bilgiye sahip olma''* ifadesine Bilgisayar Mühendisliği öğrencilerinin (%30,7); Tıp öğrencilerine (%80) göre daha az oranda bilgiye sahip olduğu belirlenmiştir (p=0.000). Beklendiği gibi Bilgisayar Mühendisliği öğrencilerinin (%9,2); Tıp öğrencilerine (%43,1) göre daha az oranda *''Hasta hakları biriminin çalışma alanı ile ilgili bilgiye''* sahip olduğu da görülmektedir (p=0.000) (Tablo 9).

Bilgisayar Mühendisliği öğrencilerinin %83,4'ü (n=136), Tıp öğrencilerinin %86,2'si (n=56) *''Mahremiyet ihlali olduğunda hizmet alımında sorun olmasın diye şikâyet edilmediğini''* belirtmektedir. *''Sağlık kurumlarında hastalara bilgi güvenliği ve mahremiyet konusunda farkındalık artırmanın gerekli olduğunu''* düşünen Bilgisayar Mühendisliği öğrencilerinin katılım oranı (%98,8 n=161); Tıp öğrencilerine göre (%93,8 n=61) daha yüksek olmasına rağmen anlamlı farklılık sınırda kalmıştır (p=0.057) (Tablo 9).

Tablo 9: Araştırma Grubunun Hasta Hakları ile İlgili Görüşleri

Değişkenler		**Bölüm**				**p***
		Bilgisayar Mühendisliği		**Tıp**		
		n	**%**	**n**	**%**	
Mahremiyet ihlali olduğunda hizmet alımında sorun olmasın diye şikâyet edilmediği olur mu?	Evet	136	83,4	56	86,2	0.759
	Hayır	27	16,6	9	13,8	
	Toplam	163	100,0	65	100,0	
Sağlık kurumlarında hastaların bilgi güvenliği ve mahremiyet konusunda farkındalığını artırmak gerekli mi?	Evet	161	98,8	61	93,8	0.057
	Hayır	2	1,2	4	6,2	
	Toplam	163	100,0	65	100,0	
Hasta hakları konusunda bilginiz var mı?	Evet	50	30,7	52	80,0	**0.000**
	Hayır	113	69,3	13	20,0	
	Toplam	163	100,0	65	100,0	
Hasta hakları biriminin çalışma alanı ile ilgili bilginiz var mı?	Evet	15	9,2	28	43,1	**0.000**
	Hayır	148	90,8	37	56,9	
	Toplam	163	100,0	65	100,0	

* Ki-kare testi ile analiz edilmiştir.

Araştırma grubunun bölümlere göre *''kişisel sağlık bilgilerinin korunmasına yönelik geliştirilen yazılım ve donanım standartlarına''* ilişkin görüşleri değerlendirildiğinde;

Bilgisayar Mühendisliği öğrencileri kişisel sağlık bilgilerinin korunmasına yönelik geliştirilen standartları, *''Şifreleme yöntemleri''* (%1,8 n=3) ve *''E-devlet güvenlik önlemleri''* (%1,2 n=2) olarak belirtirken; Tıp Öğrencileri ise *''Doktor şifreleme yöntemleri''* (%4,6 n=3) olarak belirtmiştir (Tablo 10).

Bu soruya Bilgisayar Mühendisliği öğrencilerinin %97'si (n=158), Tıp öğrencilerinin %95,4'ü (n=62) yanıt vermemiştir (Tablo 10).

Tablo 10: Araştırma Grubunun Kişisel Sağlık Bilgilerinin Korunmasına Yönelik Geliştirilen Yazılım ve Donanım Standartlarına İlişkin Görüşleri

***Kişisel sağlık bilgilerinin korunmasına yönelik hangi yazılım ve donanım standartları vardır?**	**Bölüm**			
	Bilgisayar Mühendisliği		**Tıp**	
	n	**%**	**n**	**%**
Şifreleme yöntemleri	3	1,8	0	0
E-devlet güvenlik önlemleri	2	1,2	0	0
Doktor şifreleme yöntemleri	0	0	3	4,6
Yanıt vermeyenler	158	97	62	95,4

* Açık uçlu soru.

Araştırma grubunun bölümlere göre *''sağlık bilgi sistemlerinde bilgi güvenliği ve hasta mahremiyetine''* yönelik ifadelere katılım düzeyleri bakımından karşılaştırıldığında;

''Sağlık kurumları iznim olmadan üçüncü kişilerin benim kişisel bilgilerime ulaşmasına izin verebilir" ifadesinin puanı Tıp öğrencilerinde (1,51±0.75); Bilgisayar Mühendisliği öğrencilerine (1,30±0.69) göre daha yüksektir (p=0.047). Benzer şekilde Tıp öğrencilerinin *''Hastaların sağlık verilerine, yetkisiz kişilerin erişimi olmaz*" ifadesinin puanı (4.43±0.73); Bilgisayar Mühendisliği öğrencilerine (3.87±1.24) göre daha yüksektir (p=0.000). Buna karşın *''Hastalar mahremiyet hakkı konusunda bilgi sahibidirler*" ifadesi için Bilgisayar Mühendisliği öğrencilerinin (2.37±0.96) puanı; Tıp öğrencilerine (2.08±1.0) göre daha yüksektir (p=0.042). Diğer maddelerde ise istatistiksel olarak anlamlı farklılık bulunmamaktadır (p>0.05) (Tablo 11).

Tablo 11: Araştırma Grubunun Sağlık Bilgi Sistemlerinde Bilgi Güvenliği ve Hasta Mahremiyetine Yönelik İfadelere Katılım Düzeyleri Bakımından Karşılaştırılması

Değişkenler	Bölüm				p*
	Bilgisayar Mühendisliği		Tıp		
	Ortalama	Std. Sapma	Ortalama	Std. Sapma	
Sağlık kurumuna verdiğim bilgiler, benim bilgi vermek istemeyeceğim başka kuruluşlarla da paylaşılabilir.	1,44	0,83	1,34	0,48	0.271
Sağlık kurumları iznim olmadan üçüncü kişilerin benim kişisel bilgilerime ulaşmasına izin verebilir.	1,30	0,69	1,51	0,75	**0.047**
Bilgisayar korsanları sağlık kuruluşlarının bilgi sistemlerini ele geçirerek, kişisel bilgileri rahatlıkla çalabilir.	4,07	1,15	3,78	1,11	0.086
Bir E-sağlık hizmetini kullanıp işlem yaparken kendimi savunmasız hissediyorum.	3,08	1,11	2,86	1,22	0.193
E-sağlık hizmetleri üzerinden işlem yapmak bana göre güvenli değildir.	3,06	1,10	2,91	1,18	0.372
Bilgi ve iletişim teknolojileri kullanarak, hekimin hasta ile ilgili tedavi planını oluşturması kolaydır.	3,80	0,96	3,68	1,03	0.404
Bilgi ve iletişim teknolojileri kullanarak, hekimler arasında bilgi alışverişinin yapılması kolaydır	3,90	1,00	3,97	0,98	0.644
Bilgi ve iletişim teknolojileri kullanarak hasta verilerinin transferinin yapılması, mahremiyet açısından sorun yaratmaz.	2,63	1,24	2,66	1,19	0.869
Hastalar mahremiyet hakkı konusunda bilgi sahibidirler	2,37	0,96	2,08	1,00	**0.042**
Hasta yakınları mahremiyet hakkı konusunda bilgi sahibidirler.	2,33	0,94	2,08	0,91	0.064
Mahremiyet ihlalleri ile karşılaşmamak için sağlık kurumları gerekli önlemleri alır.	2,66	0,93	2,55	1,10	0.509
Hasta verileri güvenli bir şekilde kayıt altına alınır.	2,68	0,99	2,71	1,07	0.858
Hastaların sağlık verilerine, yetkisiz kişilerin erişimi olmaz.	3,87	1,24	4,43	0,73	**0.000**
Mobil teknoloji kullanımı, bilgi güvenliği ve mahremiyeti olumsuz etkilemez.	2,63	1,21	2,72	1,15	0.602

*Eşleşmemiş T testi ile analiz edilmiştir.
1:Kesinlikle katılmıyorum - 5:Kesinlikle katılıyorum

Araştırma grubunun *''cinsiyete''* göre madde puanları karşılaştırıldığında;

Bilgisayar Mühendisliği öğrencilerinde *''Hastalar mahremiyet hakkı konusunda bilgi sahibidirler''* ifadesinin puanı, kadın öğrencilerde (2,56±0.98); erkek öğrencilere (2,22±091) göre daha yüksektir (p=0.021). Diğer maddelerde ise istatistiksel olarak anlamlı farklılık bulunmamaktadır (p>0.05) (Tablo 12).

Tıp öğrencilerinin tüm madde puanlarına katılım düzeyi cinsiyete göre istatistiksel olarak anlamlı farklılık göstermemektedir (p>0.05) (Tablo 12).

Tablo 12: Araştırma Grubunun Cinsiyete Göre Madde Puanlarının Karşılaştırılması

Değişkenler	Cinsiyet	Bölüm					
		Bilgisayar Mühendisliği			Tıp		
		Ortalama	Std. Sapma	p*	Ortalama	Std. Sapma	p*
Sağlık kurumuna verdiğim bilgiler, benim bilgi vermek istemeyeceğim başka kuruluşlarla da paylaşılabilir.	Kadın	1,51	0,84	0.337	1,37	0,49	0.552
	Erkek	1,38	0,82		1,30	0,47	
Sağlık kurumları iznim olmadan üçüncü kişilerin benim kişisel bilgilerime ulaşmasına izin verebilir.	Kadın	1,35	0,68	0.402	1,53	0,76	0.815
	Erkek	1,26	0,69		1,48	0,75	
Bilgisayar korsanları sağlık kuruluşlarının bilgi sistemlerini ele geçirerek, kişisel bilgileri rahatlıkla çalabilir.	Kadın	3,97	1,23	0.323	3,68	1,21	0.392
	Erkek	4,15	1,09		3,93	0,96	
Bir E-sağlık hizmetini kullanıp işlem yaparken kendimi savunmasız hissediyorum.	Kadın	3,21	1,12	0.183	3,11	1,13	0.056
	Erkek	2,98	1,09		2,52	1,28	
E-sağlık hizmetleri üzerinden işlem yapmak bana göre güvenli değildir.	Kadın	3,23	1,16	0.083	2,97	1,13	0.597
	Erkek	2,92	1,04		2,81	1,27	
Bilgi ve iletişim teknolojileri kullanarak, hekimin hasta ile ilgili tedavi planını oluşturması kolaydır.	Kadın	3,68	1,01	0.158	3,82	0,73	0.247
	Erkek	3,89	0,92		3,48	1,34	
Bilgi ve iletişim teknolojileri kullanarak, hekimler arasında bilgi alışverişinin yapılması kolaydır	Kadın	3,89	0,96	0.871	4,08	0,71	0.335
	Erkek	3,91	1,02		3,81	1,27	
Bilgi ve iletişim teknolojileri kullanarak hasta verilerinin transferinin yapılması, mahremiyet açısından sorun yaratmaz.	Kadın	2,46	1,24	0.132	2,47	1,08	0.132
	Erkek	2,76	1,23		2,93	1,30	
Hastalar mahremiyet hakkı konusunda bilgi sahibidirler	Kadın	2,56	0,98	**0.021**	2,08	0,91	0.985
	Erkek	2,22	0,91		2,07	1,14	
Hasta yakınları mahremiyet hakkı konusunda bilgi sahibidirler.	Kadın	2,49	0,91	0.053	2,11	0,83	0.768
	Erkek	2,21	0,96		2,04	1,02	
Mahremiyet ihlalleri ile karşılaşmamak için sağlık kurumları gerekli önlemleri alır.	Kadın	2,76	0,92	0.208	2,68	1,07	0.262
	Erkek	2,58	0,93		2,37	1,15	
Hasta verileri güvenli bir şekilde kayıt altına alınır.	Kadın	2,76	0,90	0.360	2,74	1,06	0.797
	Erkek	2,62	1,06		2,67	1,11	
Hastaların sağlık verilerine, yetkisiz kişilerin erişimi olmaz.	Kadın	3,93	1,15	0.600	4,39	0,64	0.640
	Erkek	3,83	1,31		4,48	0,85	
Mobil teknoloji kullanımı, bilgi güvenliği ve mahremiyeti olumsuz etkilemez.	Kadın	2,48	1,11	0.156	2,63	1,02	0.452
	Erkek	2,75	1,27		2,85	1,32	

*Eşleşmemiş T testi ile analiz edilmiştir.

1:Kesinlikle katılmıyorum - 5:Kesinlikle katılıyorum

Araştırma grubunun *''sağlık güvencesine''* göre madde puanları karşılaştırıldığında;

Bilgisayar Mühendisliği ve Tıp öğrencilerinin sağlık güvencesi grupları arasında tüm madde puanları katılım düzeyi bakımından istatistiksel olarak anlamlı farklılık bulunmamaktadır (p>0.05) (Tablo 13).

Tablo 13: Araştırma Grubunun Sağlık Güvencesine Göre Madde Puanlarının Karşılaştırılması

Değişkenler	Sağlık güvencesi	Bölüm					
		Bilgisayar Mühendisliği			Tıp		
		Ortalama	Std. Sapma	p*	Ortalama	Std. Sapma	p*
Sağlık kurumuna verdiğim bilgiler, benim bilgi vermek istemeyeceğim başka kuruluşlarla da paylaşılabilir.	SGK	1,44	0,86	0.980	1,30	0,46	0.153
	Özel sağlık sigortası	1,40	0,52		1,60	0,52	
	Sosyal güvence yok	1,40	0,70		1,20	0,45	
Sağlık kurumları iznim olmadan üçüncü kişilerin benim kişisel bilgilerime ulaşmasına izin verebilir.	SGK	1,31	0,70	0.892	1,46	0,79	0.154
	Özel sağlık sigortası	1,20	0,42		1,90	0,57	
	Sosyal güvence yok	1,30	0,67		1,20	0,45	
Bilgisayar korsanları sağlık kuruluşlarının bilgi sistemlerini ele geçirerek, kişisel bilgileri rahatlıkla çalabilir.	SGK	4,08	1,11	0.977	3,86	1,11	0.606
	Özel sağlık sigortası	4,10	1,45		3,50	1,18	
	Sosyal güvence yok	4,00	1,49		3,60	1,14	
Bir E-sağlık hizmetini kullanıp işlem yaparken kendimi savunmasız hissediyorum.	SGK	3,02	1,10	0.193	2,92	1,26	0.260
	Özel sağlık sigortası	3,50	1,18		3,00	1,15	
	Sosyal güvence yok	3,50	1,08		2,00	0,71	
E-sağlık hizmetleri üzerinden işlem yapmak bana göre güvenli değildir.	SGK	3,01	1,09	0.369	2,98	1,27	0.558
	Özel sağlık sigortası	3,50	1,18		2,80	0,92	
	Sosyal güvence yok	3,20	1,14		2,40	0,55	
Bilgi ve iletişim teknolojileri kullanarak, hekimin hasta ile ilgili tedavi planını oluşturması kolaydır.	SGK	3,77	0,98	0.546	3,60	1,07	0.522
	Özel sağlık sigortası	4,10	0,99		4,00	1,05	
	Sosyal güvence yok	3,90	0,74		3,80	0,45	

Bilgi ve iletişim teknolojileri kullanarak, hekimler arasında bilgi alışverişinin yapılması kolaydır	SGK	3,83	1,01	0.051	3,90	1,04	0.508
	Özel sağlık sigortası	4,50	0,53		4,30	0,95	
	Sosyal güvence yok	4,30	0,95		4,00	0,00	
Bilgi ve iletişim teknolojileri kullanarak hasta verilerinin transferinin yapılması, mahremiyet açısından sorun yaratmaz.	SGK	2,63	1,23	0.668	2,54	1,18	0.324
	Özel sağlık sigortası	2,40	1,17		3,10	1,29	
	Sosyal güvence yok	2,90	1,60		3,00	1,00	
Hastalar mahremiyet hakkı konusunda bilgi sahibidirler	SGK	2,38	0,96	0.612	2,02	0,98	0.701
	Özel sağlık sigortası	2,10	0,88		2,30	1,25	
	Sosyal güvence yok	2,50	1,08		2,20	0,84	
Hasta yakınları mahremiyet hakkı konusunda bilgi sahibidirler.	SGK	2,33	0,93	0.253	2,06	0,91	0.945
	Özel sağlık sigortası	2,00	0,9.		2,10	0,99	
	Sosyal güvence yok	2,70	1,16		2,20	0,84	
Mahremiyet ihlalleri ile karşılaşmamak için sağlık kurumları gerekli önlemleri alır.	SGK	2,67	0,96	0.837	2,48	1,07	0.552
	Özel sağlık sigortası	2,60	0,70		2,90	1,20	
	Sosyal güvence yok	2,50	0,71		2,60	1,34	
Hasta verileri güvenli bir şekilde kayıt altına alınır.	SGK	2,69	1,02	0.286	2,66	1,02	0.402
	Özel sağlık sigortası	2,30	0,67		3,10	1,37	
	Sosyal güvence yok	3,00	0,82		2,40	0,89	
Hastaların sağlık verilerine, yetkisiz kişilerin erişimi olmaz.	SGK	3,84	1,24	0.242	4,44	0,79	0.322
	Özel sağlık sigortası	3,70	1,42		4,60	0,52	
	Sosyal güvence yok	4,50	0,97		4,00	0,00	
Mobil teknoloji kullanımı, bilgi güvenliği ve mahremiyeti olumsuz etkilemez.	SGK	2,60	1,20	0.299	2,54	1,13	0.060
	Özel sağlık sigortası	2,50	1,27		3,40	1,26	
	Sosyal güvence yok	3,20	1,23		3,20	0,45	

*ANOVA testi ile analiz edilmiştir.

1:Kesinlikle katılmıyorum - 5:Kesinlikle katılıyorum

Araştırma grubunun *''son 6 ay içinde sağlık hizmeti alma''* durumuna göre madde puanları karşılaştırıldığında;

Bilgisayar Mühendisliği öğrencilerinde; *''Sağlık kurumuna verdiğim bilgiler, benim bilgi vermek istemeyeceğim başka kuruluşlarla da paylaşılabilir''* ifadesinin puanı, son 6 ay içinde sağlık hizmeti alan öğrencilerde (1,56±0.95); almayanlara (1,25±0.56) göre daha yüksektir (p=0.009). *''Sağlık kurumları iznim olmadan üçüncü kişilerin benim kişisel bilgilerime ulaşmasına izin verebilir''* ifadesinin puanı, son 6 ay içinde sağlık hizmeti alan öğrencilerde (1,40±0.82); almayanlara (1,15±0.36) göre daha yüksektir (p=0.011). Benzer şekilde *''Bilgi ve iletişim teknolojileri kullanarak hekimin hasta ile ilgili tedavi planını oluşturması kolaydır''* ifadesinin puanı, son 6 ay içinde sağlık hizmeti alan öğrencilerde (3,98±0.88); almayanlara (3,52±1.02) göre daha yüksektir (p=0.004). Ancak *''Hasta yakınları mahremiyet hakkı konusunda bilgi sahibidirler''* ifadesinin puanı, son 6 ay içinde sağlık hizmeti almayan öğrencilerde (2,52±0.94); alanlara (2,20±0.93) göre daha yüksektir (p=0.034). Aynı şekilde *''Hastaların sağlık verilerine, yetkisiz kişilerin erişimi olmaz''* ifadesinin puanı, son 6 ay içinde sağlık hizmeti almayan öğrencilerde (4,12±1.04); alanlara (3,70±1.34) göre daha yüksektir (p=0.026). Diğer maddelerde ise istatistiksel olarak anlamlı farklılık bulunmamaktadır (p>0.05) (Tablo 14).

Tıp öğrencilerinde ise; *''Bilgisayar korsanları sağlık kuruluşlarının bilgi sistemlerini ele geçirerek, kişisel bilgileri rahatlıkla çalabilir''* ifadesinin puanı, son 6 ay içinde sağlık hizmeti alan öğrencilerde (3,98±0.92); almayanlara (3,19±1.42); göre daha yüksek olmasına rağmen anlamlı farklılık sınırda kalmıştır (p=0.051). Benzer şekilde *''Bilgi ve İletişim teknolojileri kullanarak, hekimin hasta ile ilgili tedavi planını oluşturması kolaydır''* ifadesinin puanı, son 6 ay içinde sağlık hizmeti alan öğrencilerde (3,82±0.97); almayanlara (3,25±1.13); göre daha yüksek olmasına rağmen anlamlı farklılık sınırda kalmıştır (p=0.056). Diğer maddelerde de istatistiksel olarak anlamlı farklılık bulunmamaktadır (p>0.05) (Tablo 14).

Tablo 14: Araştırma Grubunun Son 6 ay İçinde Sağlık Hizmet Alma Durumuna Göre Madde Puanlarının Karşılaştırılması

Değişkenler	Son 6 ay içinde sağlık hizmeti aldınız mı?	Bölüm					
		Bilgisayar Mühendisliği			Tıp		
		Ortalama	Std. Sapma	p*	Ortalama	Std. Sapma	p*
Sağlık kurumuna verdiğim bilgiler, benim bilgi vermek istemeyeceğim başka kuruluşlarla da paylaşılabilir.	Evet	1,56	0,95	**0.009**	1,37	0,49	0.397
	Hayır	1,25	0,56		1,25	0,45	
Sağlık kurumları iznim olmadan üçüncü kişilerin benim kişisel bilgilerime ulaşmasına izin verebilir.	Evet	1,40	0,82	**0.011**	1,55	0,74	0.421
	Hayır	1,15	0,36		1,38	0,81	
Bilgisayar korsanları sağlık kuruluşlarının bilgi sistemlerini ele geçirerek, kişisel bilgileri rahatlıkla çalabilir.	Evet	4,18	1,15	0.135	3,98	0,92	0.051
	Hayır	3,91	1,14		3,19	1,42	
Bir E-sağlık hizmetini kullanıp işlem yaparken kendimi savunmasız hissediyorum.	Evet	3,18	1,17	0.141	2,92	1,30	0.448
	Hayır	2,92	0,99		2,69	0,95	
E-sağlık hizmetleri üzerinden işlem yapmak bana göre güvenli değildir.	Evet	3,09	1,12	0.604	3,00	1,21	0.274
	Hayır	3,00	1,08		2,63	1,09	
Bilgi ve iletişim teknolojileri kullanarak, hekimin hasta ile ilgili tedavi planını oluşturması kolaydır.	Evet	3,98	0,88	**0.004**	3,82	0,97	0.056
	Hayır	3,52	1,02		3,25	1,13	
Bilgi ve iletişim teknolojileri kullanarak, hekimler arasında bilgi alışverişinin yapılması kolaydır	Evet	3,97	1,00	0.289	4,10	0,80	0.151
	Hayır	3,80	0,99		3,56	1,36	
Bilgi ve iletişim teknolojileri kullanarak hasta verilerinin transferinin yapılması, mahremiyet açısından sorun yaratmaz.	Evet	2,67	1,29	0.601	2,67	1,21	0.889
	Hayır	2,57	1,17		2,63	1,15	
Hastalar mahremiyet hakkı konusunda bilgi sahibidirler	Evet	2,29	0,96	0.175	2,14	1,02	0.359
	Hayır	2,49	0,94		1,88	0,96	
Hasta yakınları mahremiyet hakkı konusunda bilgi sahibidirler.	Evet	2,20	0,93	**0.034**	2,06	0,90	0.809
	Hayır	2,52	0,94		2,13	0,96	
Mahremiyet ihlalleri ile karşılaşmamak için sağlık kurumları gerekli önlemleri alır.	Evet	2,60	0,96	0.358	2,67	1,09	0.127
	Hayır	2,74	0,87		2,19	1,11	
Hasta verileri güvenli bir şekilde kayıt altına alınır.	Evet	2,61	1,02	0.279	2,84	1,09	0.089
	Hayır	2,78	0,94		2,31	0,95	
Hastaların sağlık verilerine, yetkisiz kişilerin erişimi olmaz.	Evet	3,70	1,34	**0.026**	4,49	0,62	0.256
	Hayır	4,12	1,04		4,25	1,00	
Mobil teknoloji kullanımı, bilgi güvenliği ve mahremiyeti olumsuz etkilemez.	Evet	2,64	1,23	0.887	2,78	1,19	0.525
	Hayır	2,62	1,18		2,56	1,03	

*Eşleşmemiş T testi ile analiz edilmiştir.

1:Kesinlikle katılmıyorum - 5:Kesinlikle katılıyorum

Araştırma grubunun *''doktoru ile sağlık sorunlarıyla ilgili elektronik ortamda iletişim kurmayı isteme''* durumuna göre madde puanları karşılaştırıldığında;

Bilgisayar Mühendisliği öğrencilerinde; *"Bir E-sağlık hizmetini kullanıp işlem yaparken kendimi savunmasız hissediyorum"* ifadesinin puanı, doktoru ile sağlık sorunlarıyla ilgili elektronik ortamda iletişim kurmayı istemeyen öğrencilerde (3,52±1.25); isteyen öğrencilere (3,01±1.07) göre daha yüksektir (p=0.048). Buna karşın *"Bilgi ve iletişim teknolojileri kullanarak, hekimin hasta ile ilgili tedavi planını oluşturması kolaydır"* ifadesinin puanı, doktoru ile sağlık sorunlarıyla ilgili elektronik ortamda iletişim kurmayı isteyen öğrencilerde (3,87±0.95); istemeyen öğrencilere (3,33±0.91) göre daha yüksektir (p=0.018). Diğer maddelerde ise istatistiksel olarak anlamlı farklılık bulunmamaktadır (p>0.05) (Tablo 15).

Tıp öğrencilerinde ise; *"Bilgi ve iletişim teknolojileri kullanarak hasta verilerinin transferinin yapılması, mahremiyet açısından sorun yaratmaz"* ifadesinin puanı, doktoru ile sağlık sorunlarıyla ilgili elektronik ortamda iletişim kurmayı isteyen öğrencilerde (2,91±1.09); istemeyen öğrencilere (2,18±1.26) göre daha yüksektir (p=0.019). Aynı zamanda *''Mobil teknoloji kullanımı, bilgi güvenliği ve mahremiyeti olumsuz etkilemez"* ifadesinin puanı, doktoru ile sağlık sorunlarıyla ilgili elektronik ortamda iletişim kurmayı isteyen öğrencilerde (3,00±1.13); istemeyen öğrencilere (2,18±1.01) göre daha yüksektir (p=0.006). Diğer maddelerde ise istatistiksel olarak anlamlı farklılık bulunmamaktadır (p>0.05) (Tablo 15).

Tablo 15: Araştırma Grubunun Doktoru ile Sağlık Sorunlarıyla İlgili Elektronik Ortamda İletişim Kurmayı İsteme Durumuna Göre Madde Puanlarının Karşılaştırılması

Değişkenler	Doktorunuzla sağlık sorunlarınızla ilgili elektronik ortamda iletişim kurmak ister misiniz?	Bölüm					
		Bilgisayar Mühendisliği			Tıp		
		Ortalama	Std. Sapma	p*	Ortalama	Std. Sapma	p*
Sağlık kurumuna verdiğim bilgiler, benim bilgi vermek istemeyeceğim başka kuruluşlarla da paylaşılabilir.	Evet	1,44	0,82	0.967	1,40	0,49	0.163
	Hayır	1,43	0,93		1,23	0,43	
Sağlık kurumları iznim olmadan üçüncü kişilerin benim kişisel bilgilerime ulaşmasına izin verebilir.	Evet	1,30	0,67	0.816	1,49	0,55	0.775
	Hayır	1,33	0,80		1,55	1,06	
Bilgisayar korsanları sağlık kuruluşlarının bilgi sistemlerini ele geçirerek, kişisel bilgileri rahatlıkla çalabilir.	Evet	4,07	1,15	0.927	3,86	1,06	0.446
	Hayır	4,10	1,22		3,64	1,22	
Bir E-sağlık hizmetini kullanıp işlem yaparken kendimi savunmasız hissediyorum.	Evet	3,01	1,07	**0.048**	2,86	1,13	0.992
	Hayır	3,52	1,25		2,86	1,42	
E-sağlık hizmetleri üzerinden işlem yapmak bana göre güvenli değildir.	Evet	3,01	1,11	0.216	2,77	1,13	0.183
	Hayır	3,33	1,02		3,18	1,26	
Bilgi ve iletişim teknolojileri kullanarak, hekimin hasta ile ilgili tedavi planını oluşturması kolaydır.	Evet	3,87	0,95	**0.018**	3,77	1,02	0.327
	Hayır	3,33	0,91		3,50	1,06	
Bilgi ve iletişim teknolojileri kullanarak, hekimler arasında bilgi alışverişinin yapılması kolaydır	Evet	3,96	0,98	0.062	3,95	0,95	0.859
	Hayır	3,52	1,03		4,00	1,07	
Bilgi ve iletişim teknolojileri kullanarak hasta verilerinin transferinin yapılması, mahremiyet açısından sorun yaratmaz.	Evet	2,70	1,25	0.081	2,91	1,09	**0.019**
	Hayır	2,19	1,08		2,18	1,26	
Hastalar mahremiyet hakkı konusunda bilgi sahibidirler	Evet	2,39	0,97	0.363	2,09	0,97	0.858
	Hayır	2,19	0,87		2,05	1,09	
Hasta yakınları mahremiyet hakkı konusunda bilgi sahibidir	Evet	2,35	0,93	0.629	2,09	0,87	0.843
	Hayır	2,24	1,04		2,05	1,00	
Mahremiyet ihlalleri ile karşılaşmamak için sağlık kurumları gerekli önlemleri alır	Evet	2,65	0,88	0.966	2,56	1,05	0.965
	Hayır	2,67	1,20		2,55	1,22	
Hasta verileri güvenli bir şekilde kayıt altına alınır.	Evet	2,68	0,95	0.870	2,72	1,03	0.891
	Hayır	2,71	1,27		2,68	1,17	
Hastaların sağlık verilerine, yetkisiz kişilerin erişimi olmaz.	Evet	3,90	1,20	0.498	4,44	0,63	0.865
	Hayır	3,67	1,49		4,41	0,91	
Mobil teknoloji kullanımı, bilgi güvenliği ve mahremiyeti olumsuz etkilemez.	Evet	2,65	1,21	0.661	3,00	1,13	**0.006**
	Hayır	2,52	1,21		2,18	1,01	

*Eşleşmemiş T testi ile analiz edilmiştir.

1:Kesinlikle katılmıyorum - 5:Kesinlikle katılıyorum

Araştırma grubunun *''kullanılan sistem üzerinden kişisel sağlık verilerine erişimin denetlendiğini düşünme''* durumuna göre madde puanları karşılaştırıldığında;

Bilgisayar Mühendisliği öğrencilerinde; *"Bir E-sağlık hizmetini kullanıp işlem yaparken kendimi savunmasız hissediyorum"* ifadesinin puanı, kullanılan sistem üzerinden kişisel sağlık verilerine erişimin denetlendiğini düşünmeyen öğrencilerde (3,18±1.12); düşünenlere (2,78±1.03) göre daha yüksektir (p=0.044). Buna karşın *"Mahremiyet ihlalleri ile karşılaşmamak için sağlık kurumları gerekli önlemleri alır"* ifadesinin puanı, kullanılan sistem üzerinden kişisel sağlık verilerine erişimin denetlendiğini düşünen öğrencilerde (3,18±0.87); düşünmeyen öğrencilere (2,49±0.88) göre daha yüksektir (p=0.000). *"Hasta verileri güvenli bir şekilde kayıt altına alınır"* ifadesinin puanı, kullanılan sistem üzerinden kişisel sağlık verilerine erişimin denetlendiğini düşünen öğrencilerde (3,03±0.97); düşünmeyen öğrencilere (2,57±0.98) göre daha yüksektir (p=0.011). Diğer maddelerde ise istatistiksel olarak anlamlı farklılık bulunmamaktadır (p>0.05) (Tablo 16).

Tıp öğrencilerinde ise; *"Hastalar mahremiyet hakkı konusunda bilgi sahibidirler"* ifadesinin puanı, kullanılan sistem üzerinden kişisel sağlık verilerine erişimin denetlendiğini düşünen öğrencilerde (2,64±1.15); düşünmeyen öğrencilere (1,92±0.91) göre daha yüksektir (p=0.016). *"Hasta yakınları mahremiyet hakkı konusunda bilgi sahibidirler"* ifadesinin puanı, kullanılan sistem üzerinden kişisel sağlık verilerine erişimin denetlendiğini düşünen öğrencilerde (2,50±0.94); düşünmeyen öğrencilere (1,96±0.87) göre daha yüksektir (p=0.048). Benzer şekilde *"Mahremiyet ihlalleri ile karşılaşmamak için sağlık kurumları gerekli önlemleri alır"* ifadesinin puanı, kullanılan sistem üzerinden kişisel sağlık verilerine erişimin denetlendiğini düşünen öğrencilerde (3,43±0.94); düşünmeyen öğrencilere (2.31±1.03) göre daha yüksektir (p=0.001). *''Hasta verileri güvenli bir şekilde kayıt altına alınır"* ifadesinin puanı, kullanılan sistem üzerinden kişisel sağlık verilerine erişimin denetlendiğini düşünen öğrencilerde (3,50±1.09); düşünmeyen öğrencilere (2,49±0.97) göre daha yüksektir (p=0.001). Diğer maddelerde ise istatistiksel olarak anlamlı farklılık bulunmamaktadır (p>0.05) (Tablo 16).

Tablo 16: Araştırma Grubunun Kullanılan Sistem Üzerinden Kişisel Sağlık Verilerine Erişimin Denetlendiğini Düşünme Durumuna Göre Madde Puanlarının Karşılaştırılması

Değişkenler	Kullanılan sistem üzerinden kişisel sağlık verilerine erişimin denetlendiğini düşünüyor musunuz?	Bölüm					
		Bilgisayar Mühendisliği			Tıp		
		Ortalama	Std. Sapma	p*	Ortalama	Std. Sapma	p*
Sağlık kurumuna verdiğim bilgiler, benim bilgi vermek istemeyeceğim başka kuruluşlarla da paylaşılabilir.	Evet	1,35	0,62	0.455	1,29	0,47	0.644
	Hayır	1,46	0,89		1,35	0,48	
Sağlık kurumları iznim olmadan üçüncü kişilerin benim kişisel bilgilerime ulaşmasına izin verebilir.	Evet	1,28	0,51	0.787	1,57	0,51	0.724
	Hayır	1,31	0,74		1,49	0,81	
Bilgisayar korsanları sağlık kuruluşlarının bilgi sistemlerini ele geçirerek, kişisel bilgileri rahatlıkla çalabilir.	Evet	3,98	1,29	0.535	3,50	1,16	0.283
	Hayır	4,11	1,11		3,86	1,10	
Bir E-sağlık hizmetini kullanıp işlem yaparken kendimi savunmasız hissediyorum.	Evet	2,78	1,03	**0.044**	2,86	1,23	0.988
	Hayır	3,18	1,12		2,86	1,23	
E-sağlık hizmetleri üzerinden işlem yapmak bana göre güvenli değildir.	Evet	2,78	1,12	0.064	2,57	1,16	0.232
	Hayır	3,15	1,08		3,00	1,18	
Bilgi ve iletişim teknolojileri kullanarak, hekimin hasta ile ilgili tedavi planını oluşturması kolaydır.	Evet	3,85	1,05	0.693	4,00	0,88	0.188
	Hayır	3,78	0,94		3,59	1,06	
Bilgi ve iletişim teknolojileri kullanarak, hekimler arasında bilgi alışverişinin yapılması kolaydır	Evet	4,00	0,88	0.474	4,21	0,80	0.296
	Hayır	3,87	1,03		3,90	1,02	
Bilgi ve iletişim teknolojileri kullanarak hasta verilerinin transferinin yapılması, mahremiyet açısından sorun yaratmaz.	Evet	2,68	1,10	0.801	2,79	1,31	0.663
	Hayır	2,62	1,29		2,63	1,17	
Hastalar mahremiyet hakkı konusunda bilgi sahibidirler	Evet	2,33	1,02	0.744	2,64	1,15	**0.016**
	Hayır	2,38	0,94		1,92	0,91	
Hasta yakınları mahremiyet hakkı konusunda bilgi sahibidir	Evet	2,28	0,99	0.665	2,50	0,94	**0.048**
	Hayır	2,35	0,93		1,96	0,87	
Mahremiyet ihlalleri ile karşılaşmamak için sağlık kurumları gerekli önlemleri alır	Evet	3,18	0,87	**0.000**	3,43	0,94	**0.001**
	Hayır	2,49	0,88		2,31	1,03	
Hasta verileri güvenli bir şekilde kayıt altına alınır.	Evet	3,03	0,97	**0.011**	3,50	1,09	**0.001**
	Hayır	2,57	0,98		2,49	0,97	
Hastaların sağlık verilerine, yetkisiz kişilerin erişimi olmaz.	Evet	4,03	1,03	0.369	4,29	0,47	0.404
	Hayır	3,82	1,31		4,47	0,78	
Mobil teknoloji kullanımı, bilgi güvenliği ve mahremiyeti olumsuz etkilemez.	Evet	2,93	1,14	0.077	3,14	1,03	0.125
	Hayır	2,54	1,22		2,61	1,17	

*Eşleşmemiş T testi ile analiz edilmiştir.

1:Kesinlikle katılmıyorum - 5:Kesinlikle katılıyorum

Araştırma grubunun *''sağlık kayıtlarına doktorundan başka bir sağlık çalışanının erişiminden rahatsız olma''* durumuna göre madde puanları karşılaştırıldığında;

Bilgisayar Mühendisliği öğrencilerinde; *"Sağlık kurumları iznim olmadan üçüncü kişilerin benim kişisel bilgilerime ulaşmasına izin verebilir"* ifadesinin puanı, sağlık kayıtlarına doktorundan başka bir sağlık çalışanının erişmesinden rahatsız olan öğrencilerde (1,32±1.0.71); olmayan öğrencilere (1,00±0.00) göre daha yüksektir (p=0.000). Diğer maddelerde ise istatistiksel olarak anlamlı farklılık bulunmamaktadır (p>0.05) (Tablo 17).

Tıp öğrencilerinde ise; *"Sağlık kurumuna verdiğim bilgiler, benim bilgi vermek istemeyeceğim başka kuruluşlarla da paylaşılabilir"* ifadesinin puanı, sağlık kayıtlarına doktorundan başka bir sağlık çalışanının erişmesinden rahatsız olmayan öğrencilerde (1,57±0.51); olan öğrencilere (1,27±0.45) göre daha yüksektir (p=0.038). Benzer şekilde *"Bilgi ve iletişim teknolojileri kullanarak hasta verilerinin transferinin yapılması, mahremiyet açısından sorun yaratmaz"* ifadesinin puanı, sağlık kayıtlarına doktorundan başka bir sağlık çalışanının erişmesinden rahatsız olmayan öğrencilerde (3,29±1,38); olan öğrencilere (2,49±1.08) göre daha yüksektir (p=0.025). Diğer maddelerde ise istatistiksel olarak anlamlı farklılık bulunmamaktadır (p>0.05) (Tablo 17).

Tablo 17: Araştırma Grubunun Sağlık Kayıtlarına Doktorundan Başka Bir Sağlık Çalışanının Erişiminden Rahatsız Olma Durumuna Göre Madde Puanlarının Karşılaştırılması

Değişkenler	Sağlık kayıtlarınıza doktorunuzdan başka bir sağlık çalışanının erişiminden rahatsız olur musunuz?	Bölüm					
		Bilgisayar Mühendisliği			Tıp		
		Ortalama	Std. Sapma	p*	Ortalama	Std. Sapma	p*
Sağlık kurumuna verdiğim bilgiler, benim bilgi vermek istemeyeceğim başka kuruluşlarla da paylaşılabilir.	Evet	1,45	0,85	0.069	1,27	0,45	**0.038**
	Hayır	1,18	0,40		1,57	0,51	
Sağlık kurumları iznim olmadan üçüncü kişilerin benim kişisel bilgilerime ulaşmasına izin verebilir.	Evet	1,32	0,71	**0.000**	1,49	0,81	0.724
	Hayır	1,00	0,00		1,57	0,51	
Bilgisayar korsanları sağlık kuruluşlarının bilgi sistemlerini ele geçirerek, kişisel bilgileri rahatlıkla çalabilir.	Evet	4,11	1,12	0.193	3,92	1,02	0.057
	Hayır	3,64	1,57		3,29	1,33	
Bir E-sağlık hizmetini kullanıp işlem yaparken kendimi savunmasız hissediyorum.	Evet	3,11	1,12	0.275	2,94	1,10	0.429
	Hayır	2,73	0,90		2,57	1,60	
E-sağlık hizmetleri üzerinden işlem yapmak bana göre güvenli değildir.	Evet	3,06	1,11	0.864	3,02	1,17	0.147
	Hayır	3,00	1,00		2,50	1,16	
Bilgi ve iletişim teknolojileri kullanarak, hekimin hasta ile ilgili tedavi planını oluşturması kolaydır.	Evet	3,77	0,98	0.171	3,63	1,06	0.465
	Hayır	4,18	0,60		3,86	0,95	
Bilgi ve iletişim teknolojileri kullanarak, hekimler arasında bilgi alışverişinin yapılması kolaydır	Evet	3,88	1,01	0.201	3,98	0,97	0.863
	Hayır	4,27	0,65		3,93	1,07	
Bilgi ve iletişim teknolojileri kullanarak hasta verilerinin transferinin yapılması, mahremiyet açısından sorun yaratmaz.	Evet	2,60	1,26	0.205	2,49	1,08	**0.025**
	Hayır	3,09	0,94		3,29	1,38	
Hastalar mahremiyet hakkı konusunda bilgi sahibidirler	Evet	2,38	0,98	0.733	2,02	0,95	0.384
	Hayır	2,27	0,65		2,29	1,20	
Hasta yakınları mahremiyet hakkı konusunda bilgi sahibidir	Evet	2,35	0,96	0.273	2,02	0,84	0.426
	Hayır	2,09	0,70		2,29	1,14	
Mahremiyet ihlalleri ile karşılaşmamak için sağlık kurumları gerekli önlemleri alır	Evet	2,66	0,94	0.941	2,49	1,05	0.379
	Hayır	2,64	0,81		2,79	1,31	
Hasta verileri güvenli bir şekilde kayıt altına alınır.	Evet	2,66	1,01	0.300	2,63	1,00	0.252
	Hayır	2,91	0,70		3,00	1,30	
Hastaların sağlık verilerine, yetkisiz kişilerin erişimi olmaz.	Evet	3,89	1,25	0.370	4,43	0,78	0.990
	Hayır	3,55	1,13		4,43	0,51	
Mobil teknoloji kullanımı, bilgi güvenliği ve mahremiyeti olumsuz etkilemez.	Evet	2,66	1,23	0.098	2,65	1,13	0.314
	Hayır	2,27	0,65		3,00	1,24	

*Eşleşmemiş T testi ile analiz edilmiştir.

1:Kesinlikle katılmıyorum - 5:Kesinlikle katılıyorum

Araştırma grubunun *''E-nabız uygulamasının bilgi güvenliği ve mahremiyet açısından sorun yaratma''* durumuna göre madde puanları karşılaştırıldığında;

Bilgisayar Mühendisliği öğrencilerinde; *"Bir E-sağlık hizmetini kullanıp işlem yaparken kendimi savunmasız hissediyorum"* ifadesinin puanı, E-nabız uygulaması bilgi güvenliği ve mahremiyet açısından sorun yaratır diyen öğrencilerde (3,33±1.12); sorun yaratmaz diyen öğrencilere (2,65±0.94) göre daha yüksektir (p=0.000). Benzer şekilde *"E-sağlık hizmetleri üzerinden işlem yapmak bana göre güvenli değildir"* ifadesinin puanı, E-nabız uygulaması bilgi güvenliği ve mahremiyet açısından sorun yaratır diyen öğrencilerde (3,33±1.05); sorun yaratmaz diyen öğrencilere (2,58±1.03) göre daha yüksektir (p=0.000). Buna karşın *"Bilgi ve iletişim teknolojileri kullanarak, hekimin hasta ile ilgili tedavi planını oluşturması kolaydır"* ifadesinin puanı, E-nabız uygulaması bilgi güvenliği ve mahremiyet açısından sorun yaratmaz diyen öğrencilerde (4,00±0.99); sorun yaratır diyen öğrencilere (3,68±0.93) göre daha yüksektir (p=0.040) (Tablo 18).

"Bilgi ve iletişim teknolojileri kullanarak hasta verilerinin transferinin yapılması, mahremiyet açısından sorun yaratmaz" ifadesinin puanı, E-nabız uygulaması bilgi güvenliği ve mahremiyet açısından sorun yaratmaz diyen öğrencilerde (3,07±1.18); sorun yaratır diyen öğrencilere (2,38±1.21) göre daha yüksektir (p=0.001). Benzer şekilde *"Mobil teknoloji kullanımı, bilgi güvenliği ve mahremiyeti olumsuz etkilemez"* ifadesinin puanı, E-nabız uygulaması bilgi güvenliği ve mahremiyet açısından sorun yaratmaz diyen öğrencilerde (3,05±1.19); sorun yaratır diyen öğrencilere (2,39±1.16) göre daha yüksektir (p=0.001). Diğer maddelerde ise istatistiksel olarak anlamlı farklılık bulunmamaktadır (p>0.05) (Tablo 18).

Tıp öğrencilerinde ise; *"E-sağlık hizmetleri üzerinden işlem yapmak bana göre güvenli değildir"* ifadesinin puanı, E-nabız uygulaması bilgi güvenliği ve mahremiyet açısından sorun yaratır diyen öğrencilerde (3,29±1.05); sorun yaratmaz diyen öğrencilere (2,47±1.20) göre daha yüksektir (p=0.004). Buna karşın *"Bilgi ve iletişim teknolojileri kullanarak hasta verilerinin transferinin yapılması, mahremiyet açısından sorun yaratmaz"* ifadesinin puanı, E-nabız uygulaması bilgi güvenliği ve mahremiyet açısından sorun yaratmaz diyen öğrencilerde (3,10±1.32); sorun yaratır diyen öğrencilere (2,29±0.93) göre daha yüksektir (p=0.005). *''Mobil teknoloji*

kullanımı, bilgi güvenliği ve mahremiyeti olumsuz etkilemez" ifadesinin puanı E-nabız uygulaması bilgi güvenliği ve mahremiyet açısından sorun yaratmaz diyen öğrencilerde (3,10±1.18); sorun yaratır diyen öğrencilere (2,40±1.03) göre daha yüksektir (p=0.013). Diğer maddelerde ise istatistiksel olarak anlamlı farklılık bulunmamaktadır (p>0.05) (Tablo 18).

Tablo 18: Araştırma Grubunun E-nabız Uygulamasının Bilgi Güvenliği ve Mahremiyet Açısından Sorun Yaratma Durumuna Göre Madde Puanlarının Karşılaştırılması

Değişkenler	E-Nabız uygulaması bilgi güvenliği ve mahremiyet açısından sorun yaratır mı?	Bölüm					
		Bilgisayar Mühendisliği			Tıp		
		Ortalama	Std. Sapma	p*	Ortalama	Std. Sapma	p*
Sağlık kurumuna verdiğim bilgiler, benim bilgi vermek istemeyeceğim başka kuruluşlarla da paylaşılabilir.	Evet	1,41	0,82	0.577	1,29	0,46	0.339
	Hayır	1,48	0,85		1,40	0,50	
Sağlık kurumları iznim olmadan üçüncü kişilerin benim kişisel bilgilerime ulaşmasına izin verebilir.	Evet	1,33	0,73	0.474	1,49	0,82	0.802
	Hayır	1,25	0,60		1,53	0,68	
Bilgisayar korsanları sağlık kuruluşlarının bilgi sistemlerini ele geçirerek, kişisel bilgileri rahatlıkla çalabilir.	Evet	4,16	1,14	0.237	3,94	1,03	0.217
	Hayır	3,93	1,18		3,60	1,19	
Bir E-sağlık hizmetini kullanıp işlem yaparken kendimi savunmasız hissediyorum.	Evet	3,33	1,12	**0.000**	3,11	1,25	0.072
	Hayır	2,65	0,94		2,57	1,14	
E-sağlık hizmetleri üzerinden işlem yapmak bana göre güvenli değildir.	Evet	3,33	1,05	**0.000**	3,29	1,05	**0.004**
	Hayır	2,58	1,03		2,47	1,20	
Bilgi ve iletişim teknolojileri kullanarak, hekimin hasta ile ilgili tedavi planını oluşturması kolaydır.	Evet	3,68	0,93	**0.040**	3,49	1,01	0.107
	Hayır	4,00	0,99		3,90	1,03	
Bilgi ve iletişim teknolojileri kullanarak, hekimler arasında bilgi alışverişinin yapılması kolaydır	Evet	3,83	0,95	0.199	3,94	0,91	0.818
	Hayır	4,03	1,06		4,00	1,08	
Bilgi ve iletişim teknolojileri kullanarak hasta verilerinin transferinin yapılması, mahremiyet açısından sorun yaratmaz.	Evet	2,38	1,21	**0.001**	2,29	0,93	**0.005**
	Hayır	3,07	1,18		3,10	1,32	
Hastalar mahremiyet hakkı konusunda bilgi sahibidirler	Evet	2,48	0,93	0.059	2,17	1,01	0.417
	Hayır	2,18	0,98		1,97	1,00	
Hasta yakınları mahremiyet hakkı konusunda bilgi sahibidirler.	Evet	2,42	0,96	0.127	2,09	0,89	0.934
	Hayır	2,18	0,91		2,07	0,94	
Mahremiyet ihlalleri ile karşılaşmamak için sağlık kurumları gerekli önlemleri alır.	Evet	2,61	0,94	0.420	2,69	1,02	0.302
	Hayır	2,73	0,90		2,40	1,19	
Hasta verileri güvenli bir şekilde kayıt altına alınır.	Evet	2,57	1,00	0.068	2,74	1,04	0.777
	Hayır	2,87	0,96		2,67	1,12	
Hastaların sağlık verilerine, yetkisiz kişilerin erişimi olmaz.	Evet	3,85	1,29	0.822	4,37	0,88	0.482
	Hayır	3,90	1,16		4,50	0,51	
Mobil teknoloji kullanımı, bilgi güvenliği ve mahremiyeti olumsuz etkilemez.	Evet	2,39	1,16	**0.001**	2,40	1,03	**0.013**
	Hayır	3,05	1,19		3,10	1,18	

*Eşleşmemiş T testi ile analiz edilmiştir.

1:Kesinlikle katılmıyorum - 5:Kesinlikle katılıyorum

8. TARTIŞMA ve SONUÇ

Sağlık bilgi sistemleri, sağlık verilerini üretir, yönetir ve paylaşımında yer alır (Mumcu vd. 2013, s.87). Bilgi sistemlerinin sağlık alanındaki esas kullanımı, hasta kayıtlarının elektronik ortama kaydedilmesi ile gerçekleşmektedir (Keser vd. 2014, s.39). Kişisel sağlık verilerinin elektronik ortamdaki varlığı, bilgi güvenliği ve hasta mahremiyeti açısından tehdit oluşturmaktadır (Appari ve Johnson 2010, s.28; Kılıç Aksu vd. 2015, s.55). Bu sebeple de bilgi güvenliği ve mahremiyeti, sağlık hizmetlerinin sunumunda önemlidir (Gebrasilase ve Lessa 2011, s.73).

Ülkemizde sağlık hizmetlerinin sunumunda bilginin elektronik ortama aktarıldığı, kurumlar ve sağlık çalışanları arasında paylaşımının olduğu bir süreç yaşanmaktadır. Sağlıkta Dönüşüm Programı ile birlikte, e-reçete sistemine geçilmiş ve SGK-sağlık kurumları-eczaneler arasında dijital ağ oluşturulmuştur. SGK'nın yanı sıra Sağlık Bakanlığı da, kendine bağlı ya da denetiminde bulunan sağlık kurumlarından, hastaların kişisel bilgileri ile birlikte sağlık verilerini toplamaktadır. Engelli bakım merkezleri, üreme sağlığı merkezleri, kordon kanı bankacılığı, genetik tanı merkezleri de kişisel sağlık verilerini elektronik ortamda tutmaktadır. Kamu ve özel sağlık kuruluşlarından da Sağlık-Net kapsamında bilgiler Sağlık Bakanlığına gönderilmektedir. Kamu ve özel bütün sağlık kuruluşlarının bilgi yönetimi sistemlerinde; kimlik, iletişim, sosyal güvence ve ödeme bilgileri, sağlık geçmişi, gebelik durumu, bulaşıcı hastalıklar, bütün tetkik sonuçları, ameliyat raporları, izlem (kadın, gebe, lohusa) kayıtları gibi birçok kişisel veri toplanmaktadır. Toplanan tüm kişisel sağlık verileri, Sağlık Bakanlığı, SGK, özel sağlık sigorta şirketleri, eczaneler, laboratuarlar ve çalışanları, hekimler ve diğer sağlık çalışanları, hasta yakınları, sağlık hizmet kurumları idari personel ve yöneticileri ve adli süreç kapsamında adli makamlar tarafından da kolaylıkla izlenebilmektedir. Toplanan kişisel sağlık verilerinin, ancak bireyin izni alınarak erişimi ve kullanımı söz konusu olmalıdır (http://www.kisiselsaglikverileri.org/hakkinda.php?id=32, Türk Tabipleri Birliği Kişisel Sağlık Verileri Çalışma Grubu, Sağlık Hizmetlerinde Kişisel Veri Toplanması Korunması ve Değerlendirilmesi, e.t: 20.07.2017).

Araştırmada; sağlık hizmetlerinin multidisipliner yapısı içinde gelecekteki iç paydaş aynı zamanda dış paydaşlarından da olan Bilgisayar Mühendisliği öğrencilerinin, sağlık bilgi sistemlerinin güvenliği ve hasta mahremiyeti hakkında görüşlerinin değerlendirilmesi amaçlanmıştır.

Araştırmaya, 163'ü Bilgisayar Mühendisliği ve 65'i Tıp öğrencisi olmak üzere toplam 228 öğrenci katılmıştır. Araştırma grubunun ESK sistemi üzerinden erişim sağlanan bilgi türlerine ilişkin görüşleri değerlendirildiğinde; ağırlıklı olarak *''Kimlik bilgilerinin''* ve *''Muayene bilgilerinin''* erişilebilir olduğunu düşündükleri görülmektedir. Sistem üzerinden erişim sağlanan diğer bilgiler kapsamında; Bilgisayar Mühendisliği öğrencileri *''İletişim bilgilerinin''*, Tıp öğrencileri ise *''Ameliyat raporlarının''* ve *''Laboratuar sonuçlarının''* ESK sistemi üzerinden erişilebilir olduğunu düşünmektedir. Araştırmada, Bilgisayar Mühendisliği ve Tıp öğrencilerinin hemen hemen tamamı ESK sistemi üzerinden *''Kimlik bilgilerinin erişiminin kısıtlanmasını''* istemektedir. Sistem üzerinden erişimin kısıtlanması istenilen diğer bilgiler için; Tıp öğrencileri sistem üzerinden *''Muayene bilgilerini''* ve *''Önceden geçirilen hastalıklarını''*; Bilgisayar Mühendisliği öğrencilerine göre daha yüksek oranda erişimin kısıtlanmasını istemektedir. Bu noktada sisteme erişimin rol tabanlı olmasının gerekliliği ve hasta mahremiyetinin korunması için Tıp öğrencilerinin verdiği cevaplar olağandır. Rol tabanlı erişim kontrolü, erişim kriteri olarak kullanılan en yaygın yöntemdir. Çalışanların kurum içinde hangi bilgilere erişebileceği ve bu erişimin hangi seviyede olacağı önem arz etmektedir (Kılıç Aksu vd. 2015, s.64-65).

Araştırma grubunun bölümlere göre kişisel sağlık verilerinin korunması ve verilere erişim konusundaki görüşleri değerlendirildiğinde; Bilgisayar Mühendisliği ve Tıp öğrencilerinin *''Kullanılan sistem üzerinden kişisel sağlık verilerine erişimin''* denetlendiğini düşünmedikleri görülmektedir. Aynı zamanda her iki öğrenci grubunun çoğunluğu da *''Kişisel sağlık verilerinin paylaşımı için onamlarının''* alınmadığını belirtmiştir. Gruplar arasında istatistiksel olarak anlamlı farklılık bulunmamaktadır. Onam alınması, hastaya ait bilgilerin kullanılması ile ilgili hastadan veya yasal temsilcisinden izin alınması anlamına gelmektedir (Tengilimoğlu 2016, s.87). Hastalara ait bilgilerin işlenebilmesi ve paylaşılabilmesi için hastalardan izin (aydınlatılmış onam) alınması gerekmektedir.

Araştırmada, kişisel sağlık verilerinin korunması ve verilere erişim konusunda diğer görüşlere bakıldığında; Bilgisayar Mühendisliği ve Tıp öğrencilerinin büyük çoğunluğu *''Kişisel sağlık verilerinin nerelerde kullanılabileceği konusunda''* bilgilendirme yapılmadığını belirtmiştir. Benzer şekilde her iki öğrenci grubunun çoğunluğu *''Kişisel sağlık verilerinin diğer sağlık kurumlarıyla paylaşılmasından''* da rahatsızlık duyacaklarını belirtmişlerdir. Gruplar arasında istatistiksel olarak anlamlı farklılık bulunmamaktadır. Hasta ve hastalığa ait veriler toplanırken ve elektronik ortama aktarılırken, hastanın bu bilgilerin nerede depolanacağı ve hangi amaçlarla kullanılabileceği gibi konularda bilgilendirilmesi gerekmektedir (Ay 2008, s.166). Araştırmada, *''Doktordan başka bir sağlık çalışanının sağlık kayıtlarına erişiminden''* Bilgisayar Mühendisliği öğrencilerinin; Tıp öğrencilerine göre daha fazla rahatsız olduğu belirlenmiştir. Gruplar arasında istatistiksel olarak anlamlı farklılık bulunmaktadır. Sağlık hizmetlerinde mahremiyet, hasta-hekim ilişkisinde temel bir faktördür (Appari ve Johnson 2010, s.281). Bununla birlikte, sağlık hizmetleri ekip hizmeti şeklinde sunumu gerektirdiğinden, bir başka sağlık çalışanının erişimi ilk planda çok büyük bir sorun teşkil etmemektedir. Doğru tanı veya tedaviyi kolaylaştırmak için veri paylaşımı gereklidir. Bilgisayar Mühendisliği öğrencileri; Tıp öğrencilerine göre daha az oranda *''Elektronik sağlık kayıtlarının eksik ya da yanlış bilgi içerdiğini''* düşünmektedir. Gruplar arasında istatistiksel olarak anlamlı farklılık bulunmaktadır. Bu noktada Tıp öğrencilerinin hizmet üretimi odaklı, Bilgisayar Mühendisliği öğrencilerinin teknik boyutta durumu değerlendirdikleri düşünülebilir. Elektronik sağlık kayıtlarında güvenlik ve mahremiyetin yeterince sağlanamaması ve sisteme girilmiş yanlış ya da eksik bir hasta verisinin fark edilmeyip bütün kayıtlarda yanlışlığın sürdürülmesi, sistemin en önemli eksiklikleridir (Ay 2008, s.167). Nitelikli sağlık hizmeti sunumu için bilgi, hayati bir öneme sahiptir. Hastalar, kendilerine uygulanacak tedaviye ilişkin kararların doğru bilgilere dayanmasını isterler. Bu nedenle hasta hakkında tutulan sağlık kayıtlarının doğru ve eksiksiz olması önem arz etmektedir (Akgül 2013, s.37-38).

Araştırma grubunun bölümlere göre E-nabız uygulaması ile ilgili görüşleri değerlendirildiğinde; Bilgisayar Mühendisliği ve Tıp öğrencilerinin *''Kendilerine ait tüm sağlık verilerine E-nabız uygulaması gibi internet üzerinden''* erişmek istedikleri

görülmektedir. Ancak her iki öğrenci grubunun çoğunluğu da *''Bu tür bir erişimin bilgi güvenliği ve mahremiyeti açısından sorun yaratacağını''* düşünmektedir. Gruplar arasında istatistiksel olarak anlamlı farklılık bulunmamaktadır. Bu noktada hem teknik açıdan hem de sağlık hizmetlerinin sunumu açısından hasta mahremiyetinin sağlanması önemlidir. Güvenlik ve hasta mahremiyeti E-nabız sisteminin dışarıya açık en önemli zafiyetlerindendir. Bu nedenle Bakanlıkça belirlenen güvenlik seviyelerine uygun şekilde, sistemle ilgili güvenlik testleri yaptırılmaktadır. E-nabız uygulamasında tüm veriler gelişmiş şifreleme yapılarıyla gizli hale getirilerek (kriptolanmış halde) saklanmaktadır. Toplum içinde kişiyi yalnızlaştırabilecek hastalıklar da erişime kapalıdır (Sağlık Bakanlığı 2016, s.60-63). Bu konuyla ilgili Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelikte; *''**Madde 16-** (3) İlgili kişi tarafından açık rıza verilmesi halinde kişisel sağlık verilerine kendisinin belirleyebileceği üçüncü kişiler tarafından da erişilebilir. (5) İlgili kişi, kişisel sağlık kaydı sistemi üzerinden kendisine ilişkin sağlık verilerini görüntüleyebilir, eksik bilgilerinin sisteme eklenmesini, yanlış bilgilerinin düzeltilmesini veya silinmesini talep edebilir, kullanıcı hesabını dondurabilir''* hükmü yer almaktadır (T.C. Resmi Gazete, 24 Kasım 2017, Sayı:30250). Maddeden de anlaşılacağı üzere; kişinin hangi tür bilgilerinin kimler tarafından görüntülenebileceğine (aile bireyleri, doktoru vb.) ilişkin yetki verme hakkı vardır. Kişi verdiği yetkiyi istediği zaman geri alabilmektedir. Böylece hasta verilerinin yetkisiz kişilerce kullanımının da önüne geçilmektedir.

Araştırmada, sağlık sorunlarıyla ilgili olarak Bilgisayar Mühendisliği öğrencilerinin; Tıp öğrencilerine göre *"Doktoru ile elektronik ortamda daha fazla iletişim kurmayı"* istedikleri görülmektedir. Gruplar arasında istatistiksel olarak anlamlı farklılık bulunmaktadır. Bu durum Bilgisayar Mühendisliği öğrencilerinin mesleklerinin doğası gereği beklenen bir durumdur.

Araştırma grubunun bölümlere göre hastanede yaşanan mahremiyet ihlalleri ile ilgili görüşleri değerlendirildiğinde; Bilgisayar Mühendisliği öğrencilerinin çoğunluğu hastanede yaşanan mahremiyet ihlallerinin nedenlerini, *"Çalışanların bilgisizliğinden kaynaklı hatalar"* ve *''Dikkatsizlik''* olarak belirtirken; Tıp öğrencileri *"Yoğunluk"* ve *"Sistemsel Problemler"* olarak belirtmiştir.

2013 yılında Devlet Denetleme Kurulunun (DDK) yayınladığı raporda, artan veri işleme süreçleri karşısında kişisel verilerin korunması ve veri güvenliğinin sağlanmasında önemli eksikliklerin olduğu tespit edilmiştir. Denetim çalışmaları kapsamında ulaşılan sonuçlardan biri, bilgi güvenliği ve kişisel verilerin korunması konusundaki farkındalık eksikliğine ilişkindir. Bu eksiklik, kurumlarda bilgi güvenliği ve kişisel verilerin korunması konusunda yaşanan birçok yanlış uygulamaya sebep olabilmektedir (http://www.tccb.gov.tr/ddk/ddk56.pdf, DDK 2013, s.784, e.t:04.12.2016). Sonuç olarak; sağlık hizmetlerinin birden fazla disiplini içinde barındırması ve sisteme farklı noktalardan erişimin olması, güvenlik ve mahremiyet konularını daha önemli hale getirmektedir (Lekkas ve Gritzalis 2007, s.442). Bilgi güvenliği sağlık kuruluşları için önemli bir konudur ve kullanıcılar güvenlik sürecinde aktif rol oynamaktadırlar (Kılıç Aksu vd. 2015, s.55).

Araştırmada, Bilgisayar Mühendisliği ve Tıp öğrencileri mahremiyet ihlali olduğunda ağırlıklı olarak *''Hastane yönetimine''* ve *''Sağlık Bakanlığına''* başvurulması gerektiğini düşünmektedir. Bu durumu sırasıyla *''Hasta ve Hasta Hakları Derneğine''* ve en az oranla *''Doktoruna başvurma''* takip etmektedir. Sağlık hizmet sunucuları hem tıbbi hem de yasal nedenlerden dolayı, dijital ortamlarda tutulan hasta kayıtlarının güvenliğini ve mahremiyetini sağlamak için kapsamlı denetim işlevlerine sahip olmalıdır (Aldosarı 2012, s.496).

Araştırmada, Bilgisayar Mühendisliği ve Tıp öğrencileri sağlık kayıtlarının güvenliğinden ağırlıklı olarak *''Devletin''* ve *''Hastanenin''* sorumlu olduğunu düşünmektedir. Bu durumu sırasıyla *''Sağlık personeli''* ve en az oranla *''Kişinin kendisi''* takip etmektedir. Bilgi güvenliği sağlık hizmetlerinin her alanında sağlanması gereken bir unsurdur (Mumcu vd. 2014, s.2). Sağlık kurumlarında bilgi yönetiminde önemli sorumluluklardan biri, bilginin güvenliğinin korunmasıdır (Esatoğlu 2014, s.195). Kurumlardan (sigorta şirketleri, resmi makamlar vb.) sağlık bilgilerine erişim amaçlı taleplerde sürekli bir artış vardır. Ancak, bilginin ifşa edilmesi, hukuki ve cezai sorumluluğu da beraberinde getirmektedir (Dülger 2015, s.71). Bu durumda, kişisel sağlık verilerinin korunması süreçlerinde, sağlık kurumları yönetimlerinin sorumluluğu esastır (Esatoğlu 2014, s.196).

Araştırma grubunun bölümlere göre hasta hakları ile ilgili görüşleri değerlendirildiğinde; *''Hasta hakları ile ilgili bilgiye sahip olma ifadesine''*

Bilgisayar Mühendisliği öğrencilerinin; Tıp öğrencilerine göre daha az oranda bilgiye sahip olduğu belirlenmiştir. Benzer şekilde Bilgisayar Mühendisliği öğrencilerinin; Tıp öğrencilerine göre daha az oranda *''Hasta hakları biriminin çalışma alanı ile ilgili bilgiye''* sahip olduğu da görülmektedir. Gruplar arasında istatistiksel olarak anlamlı farklılık bulunmaktadır. Bu noktada Tıp öğrencilerinin verdiği cevaplar mesleki eğitimlerinden dolayı beklenen bir durumdur. Hasta hakları, insan haklarının bir uzantısıdır. Başka bir deyişle insan haklarının sağlık hizmetlerine uyarlanması anlamına gelmektedir (Sert 2004, s.62). Hasta hakları, sağlık hizmetlerinden yararlanan bireylerin kanunlar ve mevzuatlar ile koruma altına alınmış haklarını ifade etmektedir (Odyakmaz 2011, s.3). Hasta Hakları Yönetmeliği'ne göre; *''Müracaat, Şikâyet ve Dava Hakkı Madde 42- Hastanın ve hasta ile ilgili bulunanların, hasta haklarının ihlalinde, mevzuat çerçevesinde her türlü müracaat, şikayet ve dava hakları vardır''* hükmü yer almaktadır (T.C. Resmi Gazete, 01 Ağustos 1998, Sayı:23420). Bu noktada hastaların hasta hakları konusunda bilinçlendirilmeleri gereklidir (Erbay ve Şen 2012, s.8). Türkiye'de 15 Şubat 2004 tarihinde hastanelerde hasta hakları birimi ve hasta hakları kurulları oluşturularak ''Hasta Hakları'' uygulamasına başlanmıştır. Hastalar, bir hasta hakkı ihlali olduğunda bizzat, telefonla ya da internet üzerinden Sağlık Bakanlığı'na ya da hasta hakları birimlerine başvurabilmektedirler (Hakeri 2013, s.33).

Araştırmada, Bilgisayar Mühendisliği ve Tıp öğrencileri *''Mahremiyet ihlali olduğunda hizmet alımında sorun olmasın diye şikâyet edilmediğini''* ve *''Sağlık kurumlarında hastalara bilgi güvenliği ve mahremiyet konusunda farkındalık artırmanın gerekli olduğunu''* düşünmektedir. Gruplar arasında istatistiksel olarak anlamlı farklılık bulunmamaktadır. Sağlık hizmetlerinden faydalanan bireyler, sağlık hizmeti sunumunun bir paydaşı olarak, kişisel sağlık veri güvenliği ve mahremiyeti konusunda, sürecin ilgili yönetmelikler doğrultusunda nasıl ilerlediği konusunda bilinçli olmalıdırlar.

Araştırmada, Bilgisayar Mühendisliği öğrencileri kişisel sağlık bilgilerinin korunmasına yönelik geliştirilen yazılım ve donanım standartlarını, *''Şifreleme yöntemleri''* ve *''E-devlet güvenlik önlemleri''* olarak belirtirken; Tıp öğrencileri ise *''Doktor şifreleme yöntemleri''* olarak belirtmiştir. Bu soruya Bilgisayar Mühendisliği öğrencilerinin %97'si (n=158), Tıp öğrencilerinin %95,4'ü (n=62)

yanıt vermemiştir. Yanıt vermeyenlerin oldukça yüksek oranda oluşu, araştırma grubunun kişisel sağlık bilgilerinin korunmasına yönelik uygulamalar hakkında yeterli bilgiye sahip olmadıklarını düşündürmektedir. Kişisel sağlık bilgilerine, sağlık kuruluşu dışından birinin yanlışlıkla veya kötü niyetle erişimine engel olmak için bilişim sistemlerinde firewall (güvenlik duvarı) ve şifreli güvenlik sistemlerinin bulunması gerekmektedir. Firewall, tehditlere karşı bir önlem oluşturarak güvensiz ağ aracılığıyla yapılan bağlantıları denetler. Diğer bir tedbir ise ağ üzerinden iletilen mesajlar, gizliliğin sağlanması için yetkilendirilmeli ve şifrelenmelidir. Yetkilendirme, mesajın doğru kişiden geldiğinin ve doğru kişiye gönderildiğinin garanti edilmesidir. Şifreleme ise gönderilen mesajın hat üzerinden bir başka kişi tarafından ele geçirilmesi durumunda anlaşılmasının engellenmesidir. Tüm bu önlemlere karşın riskler yine de oluşabilmektedir (Bahçecik 2011, s.122-123).

Araştırma grubunun bölümlere göre *''sağlık bilgi sistemlerinde bilgi güvenliği ve hasta mahremiyetine''* yönelik ifadelere katılım düzeyleri bakımından karşılaştırıldığında; *''Sağlık kurumları iznim olmadan üçüncü kişilerin benim kişisel bilgilerime ulaşmasına izin verebilir*" ifadesinin puanının Tıp öğrencilerinde; Bilgisayar Mühendisliği öğrencilerine göre daha yüksek olduğu görülmektedir. Benzer şekilde Tıp öğrencilerinin *''Hastaların sağlık verilerine, yetkisiz kişilerin erişimi olmaz*" ifadesinin puanı, Bilgisayar Mühendisliği öğrencilerine göre daha yüksektir. Bu noktada Tıp öğrencilerinin sağlık politikaları açısından istatistik birimlerinin, politika yapıcıların, sağlık sigorta şirketlerinin vb. bilgilere erişebileceği konusunda bilgi sahibi oldukları, ancak bunun da yetkilendirmeyle olabileceğini düşündükleri söylenebilir. *''Hastalar mahremiyet hakkı konusunda bilgi sahibidirler''* ifadesi için ise Bilgisayar Mühendisliği öğrencilerinin puanı, Tıp öğrencilerine göre daha yüksek olduğu görülmektedir. Bu noktada Tıp öğrencileri, hastaların mahremiyet hakkı konusunda farkındalıklarının yetersiz olduğunu düşündükleri söylenebilir. Diğer maddelerde ise istatistiksel olarak anlamlı farklılık bulunmamaktadır.

Araştırma grubunun *''son 6 ay içinde sağlık hizmeti alma''* durumuna göre madde puanları karşılaştırıldığında; Bilgisayar Mühendisliği öğrencilerinde, son 6 ay içinde sağlık hizmeti *''alan''* öğrencilerde; *''Bilgi ve iletişim teknolojileri kullanarak hekimin hasta ile ilgili tedavi planını oluşturması kolaydır'', ''Sağlık kurumuna*

verdiğim bilgiler, benim bilgi vermek istemeyeceğim başka kuruluşlarla da paylaşılabilir'' ve *''Sağlık kurumları iznim olmadan üçüncü kişilerin benim kişisel bilgilerime ulaşmasına izin verebilir''* ifadelerinin puanı daha yüksektir. Ancak son 6 ay içinde sağlık hizmeti *''almayan''* öğrencilerde; *''Hasta yakınları mahremiyet hakkı konusunda bilgi sahibidirler''* ve *''Hastaların sağlık verilerine, yetkisiz kişilerin erişimi olmaz''* ifadelerinin puanının daha yüksek olduğu görülmektedir. Bu noktada Bilgisayar Mühendisliği öğrencilerinin sağlık hizmetlerine çok fazla hakim olmamalarından dolayı, hizmet sunumunda veriye hekim dışında kimlerin erişebileceği konusunda bilgi sahibi olmadıkları söylenebilir. Aynı zamanda sağlık hizmetlerinde bilgi ve iletişim teknolojilerinin kullanılabileceğini ancak teknik süreçleri çok iyi bildikleri için bilgi güvenliği ve hasta mahremiyeti açısından sorunların olabileceğini de düşündükleri söylenebilir. Tıp öğrencilerinde ise son 6 ay içinde sağlık hizmeti *''alanlar''* ile *''almayanlar''* arasında tüm madde puanlarına katılım düzeyi bakımından istatistiksel olarak anlamlı farklılık bulunmamaktadır.

Araştırma grubunun *''kullanılan sistem üzerinden kişisel sağlık verilerine erişimin denetlendiğini düşünme''* durumuna göre madde puanları karşılaştırıldığında; Bilgisayar Mühendisliği öğrencilerinde, sistem üzerinden erişimin denetlendiğini *''düşünmeyen''* öğrencilerde; *"Bir E-sağlık hizmetini kullanıp işlem yaparken kendimi savunmasız hissediyorum"* ifadesinin puanı daha yüksektir. Tıp öğrencilerinde ise, sistem üzerinden erişimin denetlendiğini *''düşünen''* öğrencilerde; *"Hastalar mahremiyet hakkı konusunda bilgi sahibidirler"* ve *"Hasta yakınları mahremiyet hakkı konusunda bilgi sahibidirler"* ifadelerinin puanının daha yüksek olduğu görülmektedir. Her iki öğrenci grubunda da sistem üzerinden erişimin denetlendiğini *''düşünen''* öğrencilerde; *"Mahremiyet ihlalleri ile karşılaşmamak için sağlık kurumları gerekli önlemleri alır"* ve *"Hasta verileri güvenli bir şekilde kayıt altına alınır"* ifadelerinin puanının daha yüksek olduğu görülmektedir. Tıp öğrencilerinde ifadelere katılımın daha olumlu olduğu görülmektedir. Bu durum Bilgisayar Mühendisliği öğrencilerinin veri güvenliğini sağlama sürecinde yaşanabilecek teknik sorunları bilmeleri ile ilgili olabilir.

Araştırma grubunun *''sağlık kayıtlarına doktordan başka bir sağlık çalışanının erişiminden rahatsız olma''* durumuna göre madde puanları karşılaştırıldığında; Bilgisayar Mühendisliği öğrencilerinde, sağlık kayıtlarına doktordan başka bir sağlık

çalışanının erişiminden *''rahatsız olan''* öğrencilerde; *"Sağlık kurumları iznim olmadan üçüncü kişilerin benim kişisel bilgilerime ulaşmasına izin verebilir"* ifadesinin puanı daha yüksektir. Tıp öğrencilerinde ise, sağlık kayıtlarına doktordan başka bir sağlık çalışanının erişiminden *''rahatsız olmayan''* öğrencilerde; *"Sağlık kurumuna verdiğim bilgiler, benim bilgi vermek istemeyeceğim başka kuruluşlarla da paylaşılabilir"* ve *"Bilgi ve iletişim teknolojileri kullanarak hasta verilerinin transferinin yapılması, mahremiyet açısından sorun yaratmaz"* ifadelerinin puanının daha yüksek olduğu görülmektedir. Bu durum sağlık hizmetleri sürecinde veri paylaşımının hizmet üretimi açısından gerekli olması ile ilgili olabilir.

Araştırma grubunun *''E-nabız uygulamasının bilgi güvenliği ve mahremiyet açısından sorun yaratma''* durumuna göre madde puanları karşılaştırıldığında; Bilgisayar Mühendisliğinde, E-nabız uygulaması, bilgi güvenliği ve mahremiyeti açısından *''sorun yaratır''* diyen öğrencilerde; *"Bir E-sağlık hizmetini kullanıp işlem yaparken kendimi savunmasız hissediyorum"* ifadesinin puanı daha yüksektir. Buna karşın, *''sorun yaratmaz''* diyen öğrencilerde; *"Bilgi ve iletişim teknolojileri kullanarak, hekimin hasta ile ilgili tedavi planını oluşturması kolaydır"* ifadesinin puanının daha yüksek olduğu görülmektedir. Her iki öğrenci grubunda da E-nabız uygulaması bilgi güvenliği ve mahremiyeti açısından *''sorun yaratır''* diyen öğrencilerde; *"E-sağlık hizmetleri üzerinden işlem yapmak bana göre güvenli değildir"* ifadesinin puanı daha yüksektir. Buna karşın *''sorun yaratmaz''* diyen öğrencilerde; *"Bilgi ve iletişim teknolojileri kullanarak hasta verilerinin transferinin yapılması, mahremiyet açısından sorun yaratmaz"* ve "*Mobil teknoloji kullanımı, bilgi güvenliği ve mahremiyetini olumsuz etkilemez"* ifadelerinin puanının daha yüksek olduğu görülmektedir. E-sağlık uygulamaları gerçek zamanlı veri üretir ve sağlık hizmetlerinin kalitesini artırmaktadır. Aynı zamanda birden fazla kullanıcı ile iletişim kurarak kolay veri paylaşımına da olanak tanımaktadır (Mumcu vd. 2014, s.32). İletişim teknolojisindeki gelişmeler, hastaneler hakkında geniş miktarda bilgi ve hizmetlere erişimi sağlayan bilgisayar ağlarının geliştirilmesini ve farklı teknolojilerin kullanılmasını da sağlamaktadır (Köksal vd. 2012, s.14).

Araştırma grubunun *''doktoru ile sağlık sorunlarıyla ilgili elektronik ortamda iletişim kurmayı isteme''* durumuna göre madde puanları karşılaştırıldığında; Bilgisayar Mühendisliği öğrencilerinde, doktoru ile sağlık sorunlarıyla ilgili

elektronik ortamda iletişim kurmayı *''istemeyen''* öğrencilerde; *"Bir E-sağlık hizmetini kullanıp işlem yaparken kendimi savunmasız hissediyorum."* ifadesinin puanı daha yüksektir. Buna karşın doktoru ile sağlık sorunlarıyla ilgili elektronik ortamda iletişim kurmayı *''isteyen''* öğrencilerde; *"Bilgi ve iletişim teknolojileri kullanarak, hekimin hasta ile ilgili tedavi planını oluşturması kolaydır"* ifadesinin puanının daha yüksek olduğu görülmektedir. Bu durumda elektronik ortamda iletişim kurmak istemeyen öğrencilerin E-sağlık sistemlerinde sorunlar olabileceğini düşündükleri söylenebilir. Elektronik ortamda iletişim kurmak isteyen öğrenciler ise bilgi ve iletişim teknolojilerinin sağlık hizmeti üretiminde kolaylık sağladığını düşünmektedir. Bilgi ve iletişim teknolojilerinin sağlık alanında kullanılması, sağlık hizmetlerinin toplumun bütün kesimlerine kolaylıkla ulaşmasını sağlamaktadır (Kopmaz 2016, s.17). Tıp öğrencilerinde ise, doktoru ile sağlık sorunlarıyla ilgili elektronik ortamda iletişim kurmayı *''isteyen''* öğrencilerde; *"Bilgi ve iletişim teknolojileri kullanarak hasta verilerinin transferinin yapılması, mahremiyet açısından sorun yaratmaz"* ve "*Mobil teknoloji kullanımı, bilgi güvenliği ve mahremiyetini olumsuz etkilemez"* ifadelerinin puanının daha yüksek olduğu görülmektedir. Bu noktada Tıp öğrencilerinin hizmet üretimi odaklı, Bilgisayar Mühendisliği öğrencilerinin ise teknik boyutta durumu değerlendirdikleri söylenebilir. Bilgi ve iletişim teknolojileri, sağlık hizmetlerinin kalitesini artırmaktadır. Bilgi teknolojileri ile hekim istemleri kolaylaşmış ve tıbbi hatalar önemli derecede azalmıştır (Anderson 2007, s.480). Aynı zamanda bilgi ve iletişim teknolojilerindeki gelişmeler sağlık çalışanlarının sürekli eğitiminde yapısal değişimlerin olmasına yardımcı olmaktadır (Mumcu vd. 2011, s.74).

Sonuç olarak;

- Tıp öğrencileri günümüzde bilgi ve iletişim teknolojileri kullanılmadan sağlık hizmeti sunumunun mümkün olamayacağını, sağlık hizmeti sunumu sırasında iş yoğunluğunun fazla olması ve sistemsel sorunların bilgi güvenliğini ve mahremiyeti olumsuz yönde etkileyebileceğini düşünmektedirler.
- Bu noktada sağlık hizmeti sunum sürecinde teknik açıdan oluşabilecek çoğu sorunlara yönelik farkındalıklarının geliştirilmesi önemlidir.
- Bilgisayar Mühendisliği öğrencileri ise, sağlık hizmetleri açısından bilgi ve iletişim teknolojilerini yaygın olarak kullanılmasını istediklerini belirtirken, bilgi güvenliği ve mahremiyeti açısından soruların oluşabileceğini de düşünmektedirler.
- Sağlık hizmeti sunumunun ekip çalışması ile sağlandığı düşünüldüğünde, kişisel sağlık verilerine erişim ve paylaşım konusunun eğitim programlarına dahil edilmesinin, gelecekte bu sektörde çalışacak mühendisler için önemli bir altyapı sağlayacağı unutulmamalıdır.
- Bu açıdan sağlık hizmetlerinin multidisipliner yapısı içinde Bilgisayar Mühendisliği öğrencileri gelecekteki önemli iç paydaşlardandır.
- Bu grubun bilgi güvenliği ve mahremiyet açısından, sağlık hizmetleri ile mesleki eğitimlerini ilişkilendirmeleri sağlık yönetimi perspektifinden oldukça önemlidir.
- Bu noktada geleceğin hekimleri ve Bilgisayar Mühendislerini ortak bir platformda buluşturmak ve gerekli eğitim programlarını organize etmek süreç yönetimi açısından oldukça önemlidir.
- Sağlık hizmetleri yönetimine yönelik seçmeli ders almaları da faydalı olabileceği düşünülmektedir.

9. KAYNAKÇA

Akbolat M. (2014). Hastane Bilgi Sistemleri. İçinde: *Sağlık Kurumlarında Bilgi Sistemleri,* Ed: Ali Yılmaz, Anadolu Üniversitesi Yayınları, 2. Baskı, Eylül, Eskişehir, s.108-135.

Akca N. (2014). E-sağlık. İçinde: S*ağlık Kurumlarında Bilgi Sistemleri,* Ed: Ali Yılmaz, Anadolu Üniversitesi Yayınları, 2. Baskı, Eylül, Eskişehir, s.158-189.

Akdağ R. (2012). Türkiye Sağlıkta Dönüşüm Programı Değerlendirme Raporu (2003-2011). T.C. Sağlık Bakanlığı Yayını, Aralık.

Akdur R. (1999). Türkiye'de Sağlık Hizmetleri ve Avrupa Topluluğu Ülkeleri ile Kıyaslanması. Ankara Üniversitesi Basımevi, 3. Baskı, Ankara.

Akdur R. (2006). Sağlık Sektörü: Temel Kavramlar, Türkiye ve Avrupa Birliği'nde Durum ve Türkiye'nin Birliğe Uyumu. Ankara Üniversitesi Basımevi, 2. Baskı, Ankara.

Akgül A. (2013). Danıştay Kararları Işığında Kişisel Sağlık Verilerinin Korunması. *Danıştay Dergisi,* Sayı:133, s.21-45.

Akgül A. (2014). Danıştay ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması. Beta Yayım, 1. Baskı, Haziran, İstanbul.

Aldosarı B. (2012). An Evaluation of EHR System Audit Functions in a Saudi Arabian Hospital. *Journal of Health Informatics in Devoloping Countries,* 6(2), p.496-508.

Anderson J. G. (2007). Social, Ethical and Legal Barriers to E-Health. International Journal of Medical Informatics, Vol:76, p.480-483.

Appari A, Johnson M. E. (2010). Information Security and Privacy in Healthcare: Current State of Research. *Int. J. Internet and Enterprise Management,* 6(4), p.279-314.

Aslandağ K. (2010). Bilgi Güvenliği Kavramı ve Bilgi Güvenliği Yönetim Sistemleri ile Şirket Performansı İlişkisine Dair Bir Uygulama, Gebze İleri teknoloji Enstitüsü Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Gebze (Danışman: Prof. Dr. Halit Keskin).

Ay F. (2008). Elektronik Hasta Kayıtları: Güvenlik, Etik ve Yasal Sorunlar. *Anadolu Üniversitesi Bilim ve Teknoloji Dergisi,* Mart, Cilt:9, Sayı:2, s.165-175.

Bahçecik N. (2011). Sağlıkta Bilişim Teknolojileri ve Etik. İçinde: *Sağlık Hizmetlerinde Bilişim Teknolojisinin Uygulama Alanları,* Ed: Deniz Şelimen, Gonca Mumcu, Bedray Yayıncılık, Ankara, s.131-146.

Bahçecik N. (2011). Evde Bakım Uygulamalarında Bilişim Teknolojileri, İçinde: *Sağlık Hizmetlerinde Bilişim Teknolojisinin Uygulama Alanları,* Ed: Deniz Şelimen, Gonca Mumcu, Bedray Yayıncılık, Ankara, s.119-129.

Baraz B. A. (2015). Bilgi İşleme Sistemleri ve Mobil İletişim. İçinde: *Büro Teknolojileri,* Ed: Ekrem Özkul, Anadolu Üniversitesi Yayınları, 4. Baskı, Nisan, Eskişehir, s.112-136.

Baraz B. A. (2015). Bilgi Güvenliği ve Yönetimi. İçinde: *Büro Teknolojileri,* Ed: Ekrem Özkul, Anadolu Üniversitesi Yayınları, 4. Baskı, Nisan, Eskişehir, s.138-163.

Bekaroğlu Ş. B. (2011). Sağlık Kurumlarında Pazarlama Yönetimi ve Organizasyonu. İçinde: *Sağlık Yönetimi,* Ed: Ayşegül Yıldırım Kaptanoğlu, Beşir Kitabevi, 1. Baskı, İstanbul, s.151-185.

Çamcı M. (2007). Sağlık Yönetimi, Mersin Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Mersin (Danışmanı: Yrd. Doç. Dr. Cemal Altan).

Çimen M. (2010). Sağlık Yönetimi ve Sağlık Yönetim Eğitimi. *Acıbadem Üniversitesi Sağlık Bilimleri Dergisi,* Temmuz, 1(3), s.136-139

Çobanoğlu N. (2010). Tıp Etiği Açısından Tıbbi Bilgilerin Mahremiyeti. *Ankara Barosu III. Sağlık Hukuku Kurultayı,* 7-8 Mayıs, Ankara, s.512-525.

Devlet Denetleme Kurulu. (2013). Kişisel Verilerin Korunmasına İlişkin Ulusal ve Uluslararası Durum değerlendirmesi ile Bilgi Güvenliği ve Kişisel Verilerin Korunması Kapsamında Gerçekleştirilen Denetim Çalışmaları. T.C. Cumhurbaşkanlığı Denetleme Raporu, Ankara

Dursun Ö. (2016). E-Devlet Uygulamalarının Kamuya Entegrasyonu. İçinde: *Bilgi Toplumu ve E-Devlet,* Ed: Yücel Güney, Muhammet Recep Okur, Anadolu Üniversitesi Yayınları, 1. Baskı, Haziran, Eskişehir, s.146-175.

Dülger M. V. (2015). Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi,* 1(2), s.43-80.

Dülger M V. (2016). Kişisel Verilerin Korunması Kanunu ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi,* 3(2), s.101-167.

Ekiz P. (2017). Sağlıkla ilgili Bilgilere Erişimde İnternetin Rolü, Marmara Üniversitesi Sağlık Bilimleri Enstitüsü, Yüksek Lisans Tezi, İstanbul (Danışman: Prof. Dr. Gonca Mumcu).

Erbay E, Şen C. B. (2012). Ankara Üniversitesi İbni Sina Hastanesinde Yatan Hastaların Hasta Hakları Hakkında Bilgi Düzeylerinin Belirlenmesi. *Toplum ve Sosyal Hizmet. Hacettepe Sosyal Hizmet Bölümü Dergisi,* Ekim, 23(2), s.7-20.

Esatoğlu A. E. (2014). Sağlık Kayıtları ve Etik. İçinde: *Sağlık Kurumlarında Bilgi Sistemleri,* Ed: Ali Yılmaz, Anadolu Üniversitesi Yayınları, 2. Baskı, Eylül, Eskişehir, s.190-211.

Ganbat O. (2013). Bilgi Güvenliği Yönetim Sistemi ISO/IEC 27001 ve Bilgi Güvenliği Risk Yönetimi ISO/IEC 27005 Standartlarının Uygulanması. Ege Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, İzmir (Danışman: Prof. Dr. Ata Önal).

Gebrasilase T, Lessa F. L. (2011). Information Security Culture in Public Hospitals: The Case of Hawassa Referral Hospital. *The African Journal of Information Systems,* 3(3), p.71-86.

Gürgan M. (2011). Teletıp Uygulamalarında Hekim Hasta İlişkisi ve Etik Sorunlar. İçinde: *Medikal Etik-10,* Ed: Hüsrev Hatemi, Hanzade Doğan, Yüce Yayım, İstanbul, s.35-40.

Hakeri H. (2013). Tıp Hukuku El Kitabı. Seçkin Yayıncılık, 6. Baskı, Mart, Ankara.

Hayran O. (1998). Sağlık ve Hastalık Kavramları. İçinde: *Sağlık Hizmetleri El Kitabı,* Ed: Osman Hayran, Haydar Sur. Yüce Yayım, İstanbul, s.1-14.

Hayran O. (1998). Sağlık Hizmetleri. İçinde: *Sağlık Hizmetleri El Kitabı,* Ed: Osman Hayran, Haydar Sur, Yüce Yayım, İstanbul, s.15-32.

Işık O. (2014). Sağlık Bilgi Sistemlerinin Gelişimi. İçinde: *Sağlık Kurumlarında Bilgi Sistemleri,* Ed: Ali Yılmaz, Anadolu Üniversitesi Yayınları, 2. Baskı, Eylül, Eskişehir, s.2-23.

İzgi M. C. (2014). Mahremiyet Kavramı Bağlamında Kişisel Sağlık Verileri. *Türkiye Biyoetik Dergisi,* (1)1, s.25-37.

Kavuncubaşı Ş, Yıldırım S. (2015). Hastane ve Sağlık Kurumları Yönetimi. Siyasal Kitabevi, 4. Baskı, Ankara.

Keser L, Kaya B. M, Kınıkoğlu B, Şahbaz U, Alpaslan İ, Sökmen A. (2014). Türkiye'de Kişisel Verilerin Korunmasının Hukuki ve Ekonomik Analizi. Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü, TEPAV, Mayıs, Cilt:1.

Kılıç Aksu P, Kitapçı Şişman N, Çatar R. Ö, Köksal L, Mumcu G. (2015). An Evaluation of Information Security from the Users' Perspective in Turkey. *Journal of Health Informatics in Devoloping Countries,* 9(2), p.55-67.

Kılıç T. (2016). e-Sağlık ve Tele-Tıp. Az Kitap Yayınevi. 1. Baskı, İstanbul.

Koçdar S. (2016). Bilgi Toplumu. İçinde: *Bilgi Toplumu ve E-Devlet,* Ed: Yücel Güney, Muhammet Recep Okur, Anadolu Üniversitesi Yayınları, 1. Baskı, Haziran, Eskişehir, s.2-24.

Kopmaz B. (2016). Ağız ve Diş Sağlığı Hizmeti Veren Kurumların Web Sitelerinin İncelenmesi, Marmara Üniversitesi Sağlık Bilimleri Enstitüsü, Yüksek Lisans Tezi, İstanbul (Danışman: Prof. Dr. Gonca Mumcu).

Köksal L, Mumcu G, Şişman N, Çatar R. Ö. Sur H. (2012). The use of Web Pages as a Health Communication Tool in Private and Public Hospitals. *Journal of Marmara University Institute of Health Sciences,* 2(1), p.14-19.

Küzeci E. (2010). Kişisel Verilerin Korunması, Turhan Kitabevi, Ankara.

Küzeci E. (2015). Bilişim, İnsan Hakları ve Kişisel Verilerin Korunması. İçinde: *Bilişim Hukuku,* Ed: Gökhan Güneysu, Anadolu Üniversitesi Yayınları, 1. Baskı, Aralık, Eskişehir, s.24-48.

Küzeci E. (2015). Türkiye'de Kişisel Verilerin Korunması. İçinde: *Bilişim Hukuku,* Ed: Gökhan Güneysu, Anadolu Üniversitesi Yayınları, 1. Baskı, Aralık, Eskişehir, s.50-69.

Lekkas D, Gritzalis D. (2007). Long-Term Verifiability of Healthcare Records Authenticity. *International Journal of Medical Informatics,* Vol:76, p.442-448.

Mumcu G. (2011). Bilişim Teknolojileri ve Sağlık Hizmetlerinde Kullanımı. İçinde: *Sağlık Hizmetlerinde Bilişim Teknolojisinin Uygulama Alanları,* Ed: Deniz Şelimen, Gonca Mumcu, Bedray Yayıncılık, Ankara, s. 1-13.

Mumcu G. (2011). Elektronik Sağlık Kayıt Sistemi, İçinde: *Sağlık Hizmetlerinde Bilişim Teknolojisinin Uygulama Alanları,* Ed: Deniz Şelimen, Gonca Mumcu, Bedray Yayıncılık, Ankara, s. 61-70.

Mumcu G, Köksal L, Şişman N, Çatar Ö. (2011). Continuing Medical Education and E-Learning for Health Professionals. *Journal of Marmara University Institute of Health Sciences,* 1(1), p.74-78.

Mumcu G, Köksal L, Şişman N, Çatar R. Ö. (2013). The Effectiveness and Outcomes of Computerized Provider Order Entry in Emergency Care Department of Private Hospitals. *Journal of Marmara University Institute of Health Sciences,* 3(2), p.83-90.

Mumcu G, Köksal L, Şişman N, Çatar R. Ö. Tarım M. (2014). The Effect of Pharmacy Information Management System on Safety Medication Use: A Study from Private Hospitals in İstanbul. *Marmara Pharmaceutical Journal,* 18: p.1-4.

Mumcu G, Köksal L, Kopmaz B, Gök M, Bulu B, Şişman N, Aksu Kılıç P, Tarım M. (2014). The Healthcare Quality and Hospital Information Management System: A Sample From Turkey. *Acıbadem Üniversitesi Sağlık Bilimleri Dergisi,* 5(1), p.31-37.

Odacıoğlu Y. (2016). Hasta Dosyaları ve Elektronik Hasta Dosyaları. İçinde: *Tıbbi Belgeleme,* Ed: Nedim Ünal, Anadolu Üniversitesi Yayınları, 1. Baskı, Mayıs, Eskişehir, s.32-59.

Odyakmaz Z. (2011). İdare Hukuku Açısından Hasta Hakları Uygulamaları. *Türkiye Adalet Akademisi Dergisi,* Nisan, 1(5), s.1-56.

Ömürbek N, Altın F. G. (2009). Sağlık Bilişim Sistemlerinin Uygulanmasına İlişkin Bir Araştırma: İzmir Örneği. *SDÜ Fen Edebiyat Fakültesi Sosyal Bilimler Dergisi,* Mayıs, Sayı:19, s.211-232.

Önel D, Dinçkan A. (2007). Bilgi Güvenliği Yönetim Sistemi Kurulumu. TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Ağustos, s.1-16.

Özata M, Güleş H. K. (2005). Sağlık Bilişim Sistemleri. Nobel Yayın Dağıtım, Eylül, Ankara.

Sağlık Bakanlığı. (2004). Türkiye Sağlık Bilgi Sistemi Eylem Planı. T.C. Sağlık Bakanlığı Bilgi İşlem Daire Başkanlığı Yayını, Ocak, Ankara.

Sağlık Bakanlığı. (2007). Sağlık-Net Entegrasyonu için Hastane Bilgi Sistemlerinin Temel Gereksinimleri. T.C. Sağlık Bakanlığı Bilgi İşlem Daire Başkanlığı Yayını, Ekim, Ankara.

Sağlık Bakanlığı. (2014). Bilgi Güvenliği Politikaları Kılavuzu. T.C. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü Yayını, Ankara.

Sağlık Bakanlığı. (2016). Kişisel Sağlık Sistemi Platformu ‘‘e-Nabız’’ Tanıtım Dokümanı. T.C. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü Yayını, Ankara.

Saluvan M, Şahin İ. (2014). Hastane Bilgi Sistemlerinin İşlevselliği Sağlık Hizmetlerinin Kalitesini Etkiler mi? *Sağlıkta Performans ve Kalite Dergisi,* Sayı:8, s.43-76.

Sert G. (2004). Hasta Hakları: Uluslararası Bildirgeler ve Tıp Etiği Çerçevesinde. Babil Yayınları, İstanbul.

Sert G. (2007). Tıp Etiği ve Tıp Hukuku Açısından Sağlık Hizmetlerinde Mahremiyet Hakkı Kavramı. Marmara Üniversitesi Sağlık Bilimleri Enstitüsü, Doktora Tezi, İstanbul (Danışman: Prof. Dr. Şefik Görkey).

Sert G. (2008). Tıp Etiği ve Mahremiyet Hakkı. Babil Yayınları, 1. Baskı, İstanbul.

Sert G, Kaynak R, Sert T. (2011). Sağlık Kurumlarında Etik. İçinde: *Sağlık Yönetimi,* Ed: Ayşegül Yıldırım Kaptanoğlu, Beşir Kitabevi, 1. Baskı, İstanbul, s.486-493.

Somunoğlu S. (2012). Sağlık-Sağlık Hizmetleri ve Türk Sağlık Sistemi. İçinde: *Sağlık Kurumları Yönetimi-1,* Ed: Mehtap Tatar, Anadolu Üniversitesi Yayınları, 1. Baskı, Eskişehir, s.2-25.

T.C. Resmi Gazete. 12 Ocak 1961, Sayı: 10705. 224 Sayılı Sağlık Hizmetlerinin Sosyalleştirilmesi Hakkında Kanun.

T.C. Resmi Gazete. 01 Ağustos 1998, Sayı: 23420. Hasta Hakları Yönetmeliği.

T.C. Resmi Gazete. 07 Nisan 2016, Sayı: 29677. Kişisel verilerin Korunması Kanunu.

T.C. Resmi Gazete. 24 Kasım 2017, Sayı: 30250. Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik.

Tekin Ş. P. (2016). Sağlık Hizmetlerinde Bilgi ve Belge Yönetimi. İçinde: *Tıbbi Belgeleme,* Ed: Nedim Ünal, Anadolu Üniversitesi Yayınları, 1. Baskı, Mayıs, Eskişehir, s.2-30.

Tengilimoğlu D. (2016). Sağlık Kayıtlarının Hukuki Yönleri. İçinde: *Tıbbi Belgeleme,* Ed: Nedim Ünal, Anadolu Üniversitesi Yayınları, Eskişehir, s.84-112.

Vardal N. (2009). Yükseköğretimde Bilgi Güvenliği: Bilgi Güvenlik Yönetim Sistemi İçin Bir Model Önerisi ve Uygulaması. G.Ü. Eğitim Bilimleri Enstitüsü, Doktora Tezi, Ankara (Danışman: Prof. Dr. Halil İbrahim Yalın).

Yıldız Ç. (2009). Telekomünikasyon Sektöründe Firma İçindeki Bilgi Güvenliğini Etkileyen Faktörler ve Bu Faktörlerin Çalışanlar Üzerindeki Etkileri. Gebze Yüksek Teknoloji Enstitüsü, Yüksek Lisans Tezi, Gebze (Danışman: Doç. Dr. Salih Zeki İmamoğlu).

Yılmaz B. (2013). E-Dönüşüm Sistemlerinin Bilgi Güvenliği Açısından İncelenmesi E-Devlet Kullanıcıları Üzerine Bir Araştırma, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, İstanbul (Danışman: Doç. Dr. Cem Sefa Sütçü).

Zengin N. (2010). Sağlık Hakkı ve Sağlık Hizmetlerinde Sunumu. *Sağlıkta Performans ve Kalite Dergisi,* Ocak, Sayı:1, s.44-52.

10. EKLER

EK1. ANKET FORMU

Sayın Katılımcı,
Marmara Üniversitesi, Sağlık Bilimleri Enstitüsü, Sağlık Yönetimi Anabilim Dalı Yüksek Lisans bitirme tezi kapsamında yürütülen bu araştırma, ***Sağlık Bilgi Sistemlerinde Bilgi Güvenliği ve Hasta Mahremiyetine*** yönelik sorulardan oluşmaktadır. Lütfen aşağıdaki ifadelerde size en uygun gelen seçeneği işaretleyiniz. Bu araştırmadaki veriler yalnızca bilimsel amaçlı olarak kullanılacaktır. Katkılarınızdan dolayı teşekkür ederiz.

Yüksek Lisans Öğrencisi
Esra Sevimli

Tez Danışmanı
Prof. Dr. Gonca MUMCU

1. Yaşınız: ….....
2. Okuduğunuz Bölüm:……..
3. Cinsiyetiniz: **1)** Kadın **2)** Erkek
4. Son 6 ay içinde sağlık hizmeti aldınız mı? **1)** Evet **2)** Hayır
5. Sosyal güvenceniz**: 1)** SGK **2)** Özel sağlık sigortası **3)** Sosyal güvencem yok
6. Sizce hastane çalışanları elektronik sağlık kayıt sistemi üzerinden hangi bilgilerinize erişebiliyor?(Birden fazla seçenek işaretleyebilirsiniz)

1) İletişim bilgileri
2) Kimlik bilgileri
3) Muayene bilgileri
4) Ameliyat raporları
5) Laboratuar sonuçları
6) Önceden geçirilen Hastalıklar
7) Sosyal güvence bilgileri
8) Ödeme bilgileri
9) Diğer……..

7. Kullanılan elektronik sağlık kayıt sistemi üzerinden hangi bilgilerinize erişimin kısıtlanmasını istersiniz**?**(Birden fazla seçenek işaretleyebilirsiniz)

1) İletişim bilgileri
2) Kimlik bilgileri
3) Muayene bilgileri
4) Ameliyat raporları
5) Laboratuar sonuçları
6) Önceden geçirilen hastalıklar
7) Sosyal güvence bilgileri
8) Ödeme Bilgileri
9) Diğer……

8. Kullanılan sistem üzerinden kişisel sağlık verilerine erişimin denetlendiğini düşünüyor musunuz? **1)** Evet **2)** Hayır

9. Kişisel sağlık verilerinizin paylaşımı için onamınız alınıyor mu? **1)** Evet **2)** Hayır

10. Kişisel sağlık verilerinizin nerelerde kullanılabileceği konusunda bilgilendirme yapılıyor mu? **1)** Evet **2)** Hayır

11. Kişisel sağlık verilerinizin diğer sağlık kurumlarıyla paylaşılmasından rahatsızlık duyar mısınız? **1)** Evet **2)** Hayır

12. Sağlık kayıtlarınıza doktorunuzdan başka bir sağlık çalışanının erişiminden rahatsız olur musunuz? **1)** Evet **2)** Hayır

13. Elektronik sağlık kayıt sistemindeki sağlık kayıtlarınızın, eksik ya da yanlış bilgi içerdiğini düşünüyor musunuz? **1)** Evet **2)** Hayır

14. Kendinize ait tüm sağlık verilerine E-nabız uygulaması gibi internet üzerinden erişmek ister misiniz? **1)** Evet **2)** Hayır

15. Bu tür bir erişim bilgi güvenliği ve mahremiyet açısından sorun yaratır mı?
1) Evet **2)** Hayır

16. Doktorunuzla sağlık sorunlarınızla ilgili olarak elektronik ortamda iletişim kurmak ister misiniz? **1)** Evet **2)** Hayır

17. Hastanelerde yaşanan mahremiyet ihlallerinin nedenleri hangileri olabilir?
(Birden fazla seçenek işaretleyebilirisiniz)
1) Çalışanların bilgisizliğinden kaynaklı hatalar **2)** Yoğunluk **3)** Dikkatsizlik
4) Sistemsel problemler **5)** Diğer……

18. Mahremiyet ihlali olduğunda, hizmet alımında sorun olmasın diye şikâyet edilmediği olur mu? **1)** Evet **2)** Hayır

19. Mahremiyetinizin ihlal edildiğini düşündüğünüz bir durumda nerelere başvurursunuz?(Birden fazla seçenek işaretleyebilirisiniz)
1) Hastane yönetimine
2) Doktorunuza
3) Hasta ve Hasta Hakları Derneğine
4) Sağlık Bakanlığına
5) Diğer……

20. Sağlık kayıtlarının güvenliğini sağlamaktan kimler sorumludur?
(Birden fazla seçenek işaretleyebilirisiniz)
1) Devlet **2)** Hastane **3)** Sağlık Personeli **4)** Kişinin kendisi **5)** Diğer……

21. Sağlık kurumlarında hastaların bilgi güvenliği ve mahremiyet konusunda farkındalığını artırmak gerekli mi? **1)** Evet **2)** Hayır

22. Hasta hakları konusunda bilginiz var mı? **1)** Evet **2)** Hayır

23. Hasta hakları biriminin çalışma alanı ile ilgili bilginiz var mı? **1)** Evet **2)** Hayır

24. Kişisel sağlık verilerinin korunmasına yönelik hangi yazılım ve donanım standartları vardır? ……

Lütfen size en uygun gelen seçeneği çarpı işareti (X) ile belirtiniz ve tüm maddeleri yanıtlayınız. **(1=Kesinlikle Katılmıyorum, 2=Katılmıyorum, 3=Kararsızım, 4=Katılıyorum, 5=Kesinlikle Katılıyorum)**	**Kesinlikle Katılıyorum**	**Katılıyorum**	**Kararsızım**	**Katılmıyorum**	**Kesinlikle Katılmıyorum**
25. Sağlık kurumuna verdiğim bilgiler, benim bilgi vermek istemeyeceğim başka kuruluşlarla da paylaşılabilir.	**5**	**4**	**3**	**2**	**1**
26. Sağlık kurumları iznim olmadan üçüncü kişilerin benim kişisel bilgilerime ulaşmasına izin verebilir.	**5**	**4**	**3**	**2**	**1**
27. Bilgisayar korsanları sağlık kuruluşlarının bilgi sistemlerini ele geçirerek, kişisel bilgileri rahatlıkla çalabilir.	**5**	**4**	**3**	**2**	**1**
28. Bir E-sağlık hizmetini kullanıp işlem yaparken kendimi savunmasız hissediyorum.	**5**	**4**	**3**	**2**	**1**
29. E-sağlık hizmetleri üzerinden işlem yapmak bana göre güvenli değildir.	**5**	**4**	**3**	**2**	**1**
30. Bilgi ve iletişim teknolojileri kullanarak, hekimin hasta ile ilgili tedavi planını oluşturması kolaydır.	**5**	**4**	**3**	**2**	**1**
31. Bilgi ve iletişim teknolojileri kullanarak, hekimler arasında bilgi alışverişinin yapılması kolaydır	**5**	**4**	**3**	**2**	**1**
32. Bilgi ve iletişim teknolojileri kullanarak hasta verilerinin transferinin yapılması, mahremiyet açısından sorun yaratmaz.	**5**	**4**	**3**	**2**	**1**
33. Hastalar mahremiyet hakkı konusunda bilgi sahibidirler	**5**	**4**	**3**	**2**	**1**
34. Hasta yakınları mahremiyet hakkı konusunda bilgi sahibidirler.	**5**	**4**	**3**	**2**	**1**
35. Mahremiyet ihlalleri ile karşılaşmamak için sağlık kurumları gerekli önlemleri alır.	**5**	**4**	**3**	**2**	**1**
36. Hasta verileri güvenli bir şekilde kayıt altına alınır.	**5**	**4**	**3**	**2**	**1**
37. Hastaların sağlık verilerine, yetkisiz kişilerin erişimi olmaz.	**5**	**4**	**3**	**2**	**1**
38. Mobil teknoloji kullanımı, bilgi güvenliği ve mahremiyeti olumsuz etkilemez.	**5**	**4**	**3**	**2**	**1**

EK2. ETİK KURUL ONAY FORMU

T.C.
MARMARA ÜNİVERSİTESİ
Sağlık Bilimleri Enstitüsü
Etik Kurulu

PROJENİN ADI : Sağlık Yönetiminin Gelecekteki Paydaşlarından Bilgisayar Mühendisliği Öğrencilerinin, Sağlık Bilgi Sistemlerini Bilgi Güvenliği ve Hasta Mahremiyeti Açısından Değerlendirmesi
PROJE YÜRÜTÜCÜSÜ: Prof.Dr.Gonca MUMCU
PROJEDEKİ ARAŞTIRICILAR : Esra SEVİMLİ
ONAY TARİHİ VE ONAY SAYISI: 05.12.2016-99

Sayın Prof.Dr.Gonca MUMCU

99 protokol nolu "Sağlık Yönetiminin Gelecekteki Paydaşlarından Bilgisayar Mühendisliği Öğrencilerinin, Sağlık Bilgi Sistemlerini Bilgi Güvenliği ve Hasta Mahremiyeti Açısından Değerlendirmesi" isimli projeniz Enstitümüz Etik Kurulu tarafından incelenmiş ve etik yönden uygunluğuna karar verilmiştir.

Prof. Dr. Göksel ŞENER
Komisyon Başkanı

Yrd.Doç.Dr. Pınar MEGA TİBER

Prof. Dr. Dilşad SAVE

Prof.Dr. Hülya AŞÇI

Prof.Dr. Tuğba TUNALI AKBAY

Prof.Dr. Nefise BAHÇECİK

Doç.Dr.Oya ORUN

Doç.Dr. Hakkı ARIKAN

Doç.Dr.Gürkan SERT

Yrd.Doç.Dr. Betül OKUYAN

Yrd.Doç.Dr. M. Ümit UĞURLU

Yrd.Doç.Dr.İlksan DEMİRBÜKEN

Av. Funda IŞIK ÖZCAN

Marmara Üniversitesi Göztepe Kampüsü Sağlık Bilimleri Enstitüsü 34688 Kadıköy / İSTANBUL
0 (216) 414 44 23/12 (Faks)
0 (216) 414 44 23
saglik.ogrenci@marmara.edu.tr
http://saglik.marmara.edu.tr
Ayrıntılı bilgi için:
Süleyman
TÜRKMENOĞLU

11. ÖZGEÇMİŞ

Adı	Esra	**Soyadı**	SEVİMLİ
Doğum Yeri	Amasra	**Doğum Tarihi**	24.02.1990
Uyruğu	T.C.	**Tel**	(554) 751 40 69
E-mail	esra.sevimli429@gmail.com		

Eğitim Düzeyi

	Mezun Olduğu Kurumun Adı	**Mezuniyet Yılı**
Doktora/Uzmanlık		
Yüksek Lisans	Marmara Üniversitesi	-----
Lisans	Marmara Üniversitesi	2012
Lise	Amasra Lisesi	2008

İş Deneyimi

Görevi	**Kurum**	**Süre (Yıl - Yıl)**
Gece İdari Amiri	Özel Erdem Hastanesi	2013-2015

Yabancı Dilleri	**Okuduğunu Anlama***	**Konuşma***	**Yazma***
İngilizce	İyi	Orta	İyi

Yabancı Dil Sınav Notu								
YDS	YÖKDİL	IELTS	TOEFL IBT	TOEFL PBT	TOEFL CBT	FCE	CAE	CPE
	62,50							

	Sayısal	**Eşit Ağırlık**	**Sözel**
ALES Puanı		71,82	
(Diğer) Puanı			

Bilgisayar Bilgisi

Microsoft Office	Çok iyi
SPSS	İyi

***Çok iyi, iyi, orta, zayıf olarak değerlendiriniz.