T.C.

KIRIKKALE ÜNİVERSİTESİ

SAĞLIK BİLİMLERİ ENSTİTÜSÜ

SAĞLIK ÇALIŞANLARININ KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDAKİ HUKUKÎ SORUMLULUKLARINA İLİŞKİN BİLGİ DÜZEYLERİ VE ELEKTRONİK SAĞLIK KAYITLARININ GÜVENLİK VE MAHREMİYET STANDARTLARINA UYUMLARININ DEĞERLENDİRİLMESİ

Faik Can YILAN

SAĞLIK YÖNETİMİ ANABİLİM DALI

YÜKSEK LİSANS TEZİ

DANIŞMAN

Doç. Dr. Meltem SAYGILI

KIRIKKALE-2023

T.C.

KIRIKKALE ÜNİVERSİTESİ

SAĞLIK BİLİMLERİ ENSTİTÜSÜ

SAĞLIK ÇALIŞANLARININ KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDAKİ HUKUKÎ SORUMLULUKLARINA İLİŞKİN BİLGİ DÜZEYLERİ VE ELEKTRONİK SAĞLIK KAYITLARININ GÜVENLİK VE MAHREMİYET STANDARTLARINA UYUMLARININ DEĞERLENDİRİLMESİ

Faik Can YILAN

SAĞLIK YÖNETİMİ ANABİLİM DALI

YÜKSEK LİSANS TEZİ

DANIŞMAN

Doç. Dr. Meltem SAYGILI

KIRIKKALE-2023

ETİK BEYANI

Kırıkkale Üniversitesi Sağlık Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

o Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,

o Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,

o Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,

o Kullanılan verilerde herhangi bir değişiklik yapmadığımı,

o Bu tezde sunduğum çalışmanın özgün olduğunu bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Faik Can Yılan
20.06.2023

ÖZET

SAĞLIK ÇALIŞANLARININ KİŞİSEL VERİLERİN KORUNMASI KANUNU KAPSAMINDAKİ HUKUKÎ SORUMLULUKLARINA İLİŞKİN BİLGİ DÜZEYLERİ VE ELEKTRONİK SAĞLIK KAYITLARININ GÜVENLİK VE MAHREMİYET STANDARTLARINA UYUMLARININ DEĞERLENDİRİLMESİ

Kırıkkale Üniversitesi

Sağlık Bilimleri Enstitüsü

Sağlık Yönetimi Anabilim Dalı, Yüksek Lisans Tezi

Danışman: Doç. Dr. Meltem SAYGILI

20.06.2023. 151 Sayfa

Bu tez çalışması, sağlık çalışanlarının 6698 sayılı kişisel verilerin korunması kanunu çerçevesinde sağlık kurumlarında elde edilen kişisel veriler ile ilgili hukukî sorumluluklarına ilişkin bilgi düzeylerini değerlendirmek, hastalara ait elektronik sağlık kayıtlarının güvenlik ve mahremiyeti konusundaki standartlara uyum düzeylerini incelemek ve ele alınan bu iki konunun birbiriyle ilişkisini ortaya koymak amacıyla gerçekleştirilmiştir. Araştırmanın evrenini Kırıkkale ilinde faaliyet gösteren 700 yataklı bir kamu hastanesinde görev yapmakta olan sağlık personelleri oluşturmaktadır. Araştırma için tabakalı örneklem yöntemi kullanılmış ve katılımcılar unvanlarına göre tabakalandırılmıştır. Araştırmada veri toplama araçları olarak, Demografik Bilgiler Soru Formu, Sağlık Çalışanlarının Kişisel Verilerin Korunması ile İlgili Hukukî Sorumlulukları Bilgi Düzeyi Ölçeği (KVK-HSBDÖ) ve Elektronik Sağlık Kayıtları Güvenlik ve Mahremiyet Standartlarına Uyum Ölçeği (ESK-GMSUÖ) kullanılmıştır. Araştırma verilerinin elde edilmesinde gönüllülük esas alınmış, yüz yüze görüşme ve anket yöntemi kullanılarak toplam 366 sağlık personelinin katılımıyla araştırma tamamlanmıştır. Verilerin analiz edilmesinde ise; tanımlayıcı analizler (yüzde, ortalama, standart sapma), normallik testleri, güvenirlik analizi, Mann Whitney U testi, Kruskal Wallis testi, Spearman Korelasyon analizi kullanılmıştır. Kruskal Wallis testinde fark çıkması durumunda çoklu karşılaştırmalar için Games-Howell Post-Hoc testi kullanılmıştır. Tez çalışmasının ilk kısmında kişisel verilerin korunması hukuku ve 6698 sayılı kanunun genel ilkeleri ile ele alınmıştır. Ardından sağlık kurumlarında hasta verilerinde mahremiyetin sağlanması, elektronik sağlık kayıtlarından kaynaklanabilecek hukukî sorunlar, bilgi güvenliği konularına değinilmiştir. İkinci kısımda araştırmanın amacı, yöntemi, sağlık çalışanlarının kişisel verilerin korunması kanunu kapsamındaki hukukî sorumluluklarına ilişkin bilgi düzeylerini değerlendirmek üzere geliştirilen ölçeğin geçerliliğine ilişkin sonuçlar ve hipotezlere ilişkin gerçekleştirilen veri analizinden elde edilen bulgular yer almaktadır. Üçüncü kısımda elde edilen sonuçlar ile

literatürdeki konu ile ilgili yapılan araştırma sonuçları kıyaslanarak tartışmalar yapılmıştır. Ardından araştırma sonuçları temelinde araştırmacı tarafından oluşturulan önerilere yer verilmiştir. Analizlerden elde edilen sonuçlar; sağlık çalışanlarının kişisel verilerin korunması ile ilgili hukukî sorumluluklarına ilişkin bilgi düzeylerinin oldukça "yüksek" seviyede (ort: 0,87 ± 0,173; min:0,20-max:1,00) olduğunu göstermiştir. Araştırmaya katılan sağlık çalışanlarının KVK-HSBD ölçeğinden elde ettikleri puan ortalamalarının; unvan, cinsiyet, Elektronik Sağlık Kayıtları (ESK) kullanma deneyimleri, kurumdaki ESK güvenlik ve mahremiyet uygulamaları konusundaki değerlendirmeleri ve ilgili konularda eğitim alma durumlarına göre anlamlı farklılıklar gösterdiği tespit edilmiştir ($p<0,05$). Sağlık çalışanlarının ESK güvenlik ve mahremiyeti standartlarına uyum düzeylerini değerlendirmek üzere gerçkeleştirilen analizlerde ise; sağlık çalışanlarının Elektronik Sağlık Kayıtları Güvenlik ve Mahremiyeti Standartlarına Uyum (ESK-GMSU Ölçeğinden yüksek düzeyde puanlar elde ettiği belirlenmiştir (ort: 3,99 ± 0,220; min:1,89-max:5,00). Araştırmaya katılan sağlık çalışanlarının ESK-GMSU ölçeğinden aldıkları puanların ise; onların yaş, eğitim düzeyi, unvan ve meslekte çalışma yılı özellikleri ve ilgili konularda eğitim alma durumlarına göre istatistiksel olarak anlamlı farklılıklar gösterdiği belirlenmiştir ($p<0,05$). Son olarak sağlık çalışanlarının kişisel verilerin korunması ile ilgili hukukî sorumluluklarına ilişkin bilgi düzeyleri ile elektronik sağlık kayıtları güvenlik ve mahremiyeti standartlarına uyum düzeyleri arasında pozitif yönlü zayıf bir ilişki ($r=0,192$; $p=0,000$) belirlenmiştir. Elde edilen sonuçlara göre; sağlık çalışanlarının kişisel sağlık verilerinin korunması ile ilgili hukukî sorumluluklarına ilişkin bilgi düzeylerinin artırılması ile elektronik sağlık kayıtları güvenlik ve mahremiyeti standartlarına uyum düzeyleri artırılacaktır.

Anahtar Kelimeler: Kişisel sağlık verilerinin korunması, Veri güvenliği ve mahremiyeti, Hukukî sorumluluk, Elektronik sağlık kayıtları.

ABSTRACT

EVALUATION OF HEALTH WORKER'S LEVEL OF KNOWLEDGE ABOUT THEIR LEGAL RESPONSIBILITIES UNDER THE LAW ON THE PROTECTION OF PERSONAL DATA AND THEIR COMPLIANCE WITH THE SECURITY AND PRIVACY STANDARDS OF ELECTRONIC HEALTH RECORDS

Kırıkkale University

Institute of Health Sciences

Department of Health Management, Master's Thesis

Supervisor: Assoc. Prof. Meltem SAYGILI

20.June 2023, 151 Pages

This thesis study was carried out in order to evaluate the level of knowledge of healthcare professionals regarding their legal responsibilities regarding personal data obtained in healthcare institutions within the framework of Law No. 6698 on the protection of personal data, to examine their level of compliance with the standards on the security and privacy of electronic health records of patients, and to reveal the relationship between these two issues. The population of the study consists of health personnel working in a 700-bed public hospital operating in Kırıkkale province. Stratified sampling method was used for the research and the participants were stratified according to their titles. Demographic Information Questionnaire, Knowledge Level Scale of Healthcare Workers' Legal Responsibilities Regarding the Protection of Personal Data (KVK-HSBDÖ) and Electronic Health Records Security and Privacy Standards Compliance Scale (ESK-GMSUÖ) were used as data collection tools in the study. Volunteerism was taken as a basis in obtaining the research data, and the research was completed with the participation of 366 health personnel using face-to-face interviews and questionnaire method. Descriptive analysis (percentage, mean, standard deviation), normality tests, reliability analysis, Mann Whitney U test, Kruskal Wallis test, Spearman Correlation analysis were used to analyze the data. In case of a difference in the Kruskal-Wallis test, Games-Howell Post-Hoc test was used for multiple comparisons. In the first part of the thesis, the law on the protection of personal data and the general principles of Law No. 6698 are discussed. Then, ensuring privacy of patient data in health institutions, legal problems that may arise from electronic health records, information security issues are mentioned. In the second part, the purpose and method of the study, the results regarding the validity of the scale developed to evaluate the level of knowledge of healthcare professionals regarding their legal responsibilities within the scope of the law on the protection of personal data, and the findings obtained from the data analysis of the hypotheses are presented. In the third part, the results obtained and the results of the research on the subject in the literature are compared and discussed. Then, the recommendations created by the researcher on the basis of the research results are given.

The results obtained from the analyzes showed that the level of knowledge of healthcare professionals regarding their legal responsibilities regarding the protection of personal data is at a very "high" level (mean: 0.87 ± 0.173; min: 0.20-max: 1.00). It was determined that the mean scores of the healthcare professionals who participated in the study obtained from the PDP-HSBD scale showed significant differences according to their title, gender, experience in using Electronic Health Records (EHR), their evaluation of EHR security and privacy practices in the organization, and their training on related issues ($p<0.05$). In the analyses carried out to evaluate the level of compliance of healthcare professionals with EHR security and privacy standards, it was determined that healthcare professionals obtained high scores from the Electronic Health Records Security and Privacy Standards Compliance (EHR-SPSCS) Scale (mean: 3.99 ± 0.220; min: 1.89-max: 5.00). It was determined that the scores obtained from the ESK-GMSU scale by the healthcare professionals participating in the study showed statistically significant differences according to their age, education level, title and years of working in the profession and their training on related issues ($p<0.05$). Finally, a weak positive correlation ($r=0.192$; $p=0.000$) was found between the level of knowledge of healthcare professionals regarding their legal responsibilities regarding the protection of personal data and their level of compliance with electronic health records security and privacy standards. According to the results obtained; increasing the level of knowledge of healthcare professionals regarding their legal responsibilities regarding the protection of personal health data will increase their level of compliance with electronic health records security and privacy standards.

Keywords: Protection of personal health data, Data security and privacy, Legal liability, Electronic health records.

İÇİNDEKİLER

ÇİZELGELER DİZİNİ

Çizelge **Sayfa**

ŞEKİLLER DİZİNİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR DİZİNİ

AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
AR-GE	: Araştır ve Geliştirme
ATT	: Acil Tıp Teknisyeni
AY	: Anayasa
BM	: Birleşmiş Milletler (United NAtions)
COVID:	: "CO" Korona "VI" Virüs "D" Hastalığı
Dr.	: Doktor
EBYS	: Elektronik Bilgi Yönetim Sistemi
ESK-GMSUÖ	: Elektronik Sağlık Kayıtları Güvenlik ve Mahremiyet Standartlarına Uyum Ölçeği
ESK	: Elektronik Sağlık Kayıtları
HBYS	: Hastane Bilgi Yönetim Sistemi
HHY	: Hasta Hakları Yönetmeliği
HIPAA	: Amerikan Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (The Health Insurance Portability and Accountability Act)
KKÜ	: Kırıkkale Üniversitesi
KMO	: Kaiser-Meyer-Olkin test
KVK-HSBD	: Kişisel Verilerin Korunması Hakkında Sağlık Çalışanlarının Bilgi Düzeyi
KVK-HSBDÖ	: Kişisel Verilerin Korunması Hakkında Sağlık Çalışanlarının Bilgi Düzeyi Ölçeği

KVKK	: Kişisel Verilerin Korunması Kanunu
Lab. Tek.	: Laboratuvar Teknisyeni
M.	: Kanun Maddesi
MÖ	: Milattan Önce
OECD	: Ekonomik Kalkınma ve İş birliği Örgütü (Organisation for Economic
Ort	: Ortalama
PIPA	: Kore Cumhuriyeti Kişisel Veri Kanunu (Personal Information Protection Act)
RG	: Resmî Gazete
SBE	: Sağlık Bilimleri Enstitüsü
SDP	: Sağlıkta Dönüşüm Programı
SPSS	: Sosyal Bilimler İçin İstatistik Programı (Statistical Package for the Social Sciences)
SS	: Standart Sapma
T.C.	: Türkiye Cumhuriyeti
TBK	: Türk Borçlar Kanunu
TCK	: Türk Ceza Kanunu
TDK	: Türk Dil Kurumu
Tek.	: Teknisyen
TMK	: Türk Medeni Kanunu
Uzm.	: Uzman
Vb	: ve benzeri
Vd	: ve diğerleri

1. GİRİŞ

Sağlık hizmetleri uygulamaları bilgi yoğundur; dolayısıyla klinik teşhis ve tedaviden hizmetlerin ödemesine kadar, doğru ve zamanında bilgiye erişim çok önemlidir. Son yirmi yılda, sağlık hizmetlerinin sunumunda, hasta sağlık verilerini yönetmek ve işlemek için bilgi teknolojisi uygulamalarının daha fazla kullanılması ile sağlık kayıtlarının ve ilgili iletişim teknolojilerinin güvenliğini sağlamak daha da önemli hale gelmiştir (Ong ve Sabapathy, 2020).

Mahremiyet kaygıları dijital gelişmeleri muazzam bir baskı altına itmektedir. Özellikle COVID-19 ile mücadelede teknolojinin yaygın olarak kullanılması nedeniyle gizlilik ihlalleri önemli ölçüde artmıştır. Dolayısıyla veri güvenliği ve gizliliğine öncelik vermek konusunda kaçınılmaz bir gereklilik vardır. Ayrıca pek çok ülke büyük veriyi ve yapay zekayı benimsediğinden, bu küresel salgında grup mahremiyeti ihlalleri bireysel ihlallerden daha olasıdır (Ali, Zaaba ve Singh 2023).

Dolayısıyla birçok kişisel sağlık verisinin yoğun olarak işlendiği ve muhafaza edildiği yerler olarak sağlık kurumlarına büyük sorumluluklar düşmektedir. Hastaneye başvurduktan sonra, çalışanlar için sadece bireyin sağlığı değil, aynı zamanda hasta mahremiyeti ve verilerini korumak da önemli bir sorumluluktur. Kişisel veriler arasında önemli bir yere sahip olan sağlık verilerinin korunması temel hak ve özgürlüklerin korunması kapsamında değerlendirildiğinden, ulusal ve uluslararası düzeyde pek çok yasal düzenleme ile de ele alınmaktadır (Durmuş, 2021). Türkiye'de hastanelerde kişisel verilerin mahremiyeti ve gizliliğinin sağlanması 2016 yılında yayınlanan Kişisel Verilerin Korunması Kanunu (KVKK) ile güvence altına alınmıştır. Bu kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir.

Birçok alanda olduğu gibi sağlık hizmetlerinde de teknolojik gelişmelerle birlikte ve maliyet-etkililik açısından daha rasyonel olan elektronik bilgi sistemlerine

geçilmiştir. Elektronik Sağlık Bilgi Sistemleri (EBYS) hasta kayıtlarının ve bilgilerinin sağlık kurum ve kuruşlarınca kaydedildiği sistemlerdir. Bu sistemde hasta ile ilgili her türlü verinin kaydı tutulabildiğinden hasta ile ilgili bilgiler toplanmakta, saklanmakta ve gerekirse kurumlar arası paylaşılmaktadır (Karaarslan, 2015).

Hastanedeki elektronik sağlık bilgi sistemleri, içinde daha küçük sistemleri barındıran entegre sistemlerdir. Sağlık kurumları için başvuran bireylerin sağlık bilgilerini içeren bu sistemlerin yönetimi, gizliliğin ve güvenliğin sağlanması noktasında çok önemlidir (Tankul, 2022). Kişinin sağlık verileri içerdiği bilgiler nedeniyle özel korumayı hak etmektedir. Bu veriler kişinin geçmiş, şimdiki ve gelecekteki fiziksel ve zihinsel sağlık ile ilgili verilerinden oluşmaktadır. Bu nedenle veriler içerisinde benzersiz özelliğe sahip olmasıyla özel bir korumaya tabidir. Çünkü bu hassas verilerin öğrenilmesi durumunda sağlık kurumuna başvuran bireylerin utanç ya da ayrımcılık yaşaması söz konusu olabilmektedir (Gostin, Halabi ve Wilson, 2018).

Hasta verilerinin gizliliği ve mahremiyeti hukukta “özel hayatın gizliliği” ile ilgilidir. Toplum sürekli olarak anlayış, düşünce, maddi ve manevi olarak değişim ve gelişim göstermektedir. Hukuk ise gelişmeleri takip eden bir bilim dalıdır. Dolayısıyla hasta verilerinin mahremiyetinde oluşan tehlikelerin maddi, manevi hasarlara yol açma ihtimali olduğundan, bu durumun hukukî ve cezaî yaptırımlar ile düzenlenmesi gerekmektedir. Bu aşamada “Kişisel Veri” kavramı özel hayatın gizliliği, mahremiyeti ve sırları ile yakın ilişki haline girmektedir. Fakat hastayla ilgili her türlü veri kişisel veri sayılmamaktadır (İstek, 2016).

1.1. KİŞİSEL SAĞLIK VERİLERİNE İLİŞKİN HUKUKÎ DÜZENLEMELER

Günümüzde sağlık hizmetlerinde artan dijital teknoloji kullanımı ile sağlık hizmeti kullanan bireylere ait verilere ilişkin bilgi güvenliği ve hasta mahremiyeti daha fazla önem kazanmıştır. Uygulamada hasta verilerinin işlenmesi, özel hayatın gizliliği başta olmak üzere bireylerin temel hak ve hürriyetleri kapsamında ele alınmakta ve kişisel verileri işleyen gerçek ve tüzel kişiler için hukukî yükümlülükler ve sorumluluklar doğurmaktadır. Dolayısıyla dijitalleşmenin artmasıyla beraber sağlık hizmetleri sunumunda kâğıt temelli sağlık kayıtlarından elektronik sağlık kayıtlarına doğru yaşanan geçişte, kurumların ve sağlık çalışanlarının yasal yükümlülükler ve sorumluluklar çerçevesinde bazı hukukî problemler yaşanması söz konusu olmaktadır. Konu ile ilgili olarak, sağlık personelinin hasta verilerine ilişkin gizlilik ve mahremiyet anlayışı bahsedilen hukukî problemlerin doğmasında belirleyici rol oynamaktadır. Bu sorunlar bireylerin anayasal haklarını ve kişilik haklarını ihlâli ile hukuka aykırılıkları oluşturmaktadır. Bu tez çalışmasında 6698 sayılı Kişisel Verilerin Korunması Kanunu'ndan yola çıkılarak sağlık kurumlarında hasta verilerinin mahremiyetinin sağlanması ve bilgi gizliliği konusu hukuk ve sağlık yönetimi perspektifinden ele alınmıştır.

Sağlık hizmetlerinde verilen hizmetin kalitesi, büyük ölçüde hastanın durumu hakkındaki bilgilere dayanır. Elektronik sağlık kayıtları yerel olarak bir ortamda depolanır ve ihtiyaç halinde erişilmek üzere bekletilir. Bilgi sağlık sisteminin bir parçası olduğunda ise artık kurumun sorumluluğu altına girmektedir. Bilginin bu şekilde kayıtlara geçmesi hastanın mahremiyeti ve güvenliği açısından bir sorunu başlatmaktadır (Haas, Wohlgemuth, Echizen, Sonehara ve Müller 2011).

Hastanın mahremiyetine saygı gösterilmesi hakkı da Tıp Meslek Ahlak Tüzüğü Madde 18 ile düzenlenmiştir: "Sır saklamak temel meslek ahlakı kuralıdır. Hastanın verdiği, bilgileri muayene bulgularını ve tedavi sonuçlarını gizli tutmak tabip ve diğer sağlık meslek gruplarının görevidir" (Serengil, 2012). Hastanın tedavi görmesi yaşam hakkıyla bağlantılı bir sağlık hakkıdır. Tedavi aşamasındaki mahremiyet hasta bilgilerinin, tedavi ve girişim bilgilerinin paylaşılmamasını ele almaktadır. Birey dış dünyadan saklamak istediği bilgilerini tedavi ve bakım amaçlı sağlık personelleriyle paylaşmak durumunda olabilir, bu da mahremiyet içerisinde değerlendirilmelidir. Bu

durumda birey, paylaştığı bilgilerin gizli kalacağına inanmakta ve kuruma güvenebilmektedir. Başvuru yapan hasta sayısı ve hastane büyüklüğü göz önüne alındığında sağlık kurumlarında çok ciddi bilgi havuzları oluşmaktadır. Sağlık kurumlarında mahremiyeti korumak ve sağlık verilerindeki güvenliği sağlamak için ciddi bir dokümantasyon alt yapısı gerekmektedir. Kişisel veriler birey mahrem alanının kapsamına girmektedir ve bu verilerin ihlâli "mahremiyet ihlâli" olarak değerlendirilmektedir. İhlâl kurumlara ve devlete olan güveni sarsan hatalardır, ekonomik ve sosyal yönden pek çok etkisi vardır (Atalay, 2021).

Sağlık çalışanları tedavi süreci boyunca hasta bilgilerine doğrudan ulaşabilmekte ve bunları gerektiğinde üçüncü kişilerle paylaşabilmektedir. Bu paylaşımlar ve hastanedeki elektronik sağlık kayıtlarının sistemsel olarak güvenliğinin incelenmesi gerekliliğini ortaya çıkarmaktadır. Bu bölümde sağlık kurumlarında elektronik olarak saklanan hasta bilgilerinin güvenliğinin sağlanmasında sağlık çalışanları ve sağlık kurumlarının hukukî sorumlulukları ilgili kanun çerçevesinde incelenecektir.

1.1.1. Temel Kavramlar ve Terminoloji

Bu bölümde konu ile ilgili kullanılan kavramlara ilişkin açıklamalara yer verilmiştir.

Kişisel Veri: Türk Dil Kurumunun büyük sözlüğünde kişisel ifadesi "kişi ile ilgili, kişiye ilişkin, kişinin kendi malı olan, şahsi, zatî" olarak tanımlanmaktadır. Veri kavramı "bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done, gözlem ve deneye dayalı sonuçlar, bilgi ve datadır" şeklinde tanımlanmıştır. (Türk Dil Kurumu [TDK], 2023). Kişisel veri kavramı ise 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3. maddesinde "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgiyi" (TDK, 2023) olarak tanımlamıştır.

T.C. Dışişleri Bakanlığı Avrupa Birliği Başkanlığı Genel Veri Koruma Tüzüğü kişisel veriler için şu şekilde tanımlama yapmıştır; "kişisel veri tanımlanmış veya tanımlanabilir bir gerçek kişiye ilişkin her türlü bilgidir". "Veri sahibi" ise tanımlanmış bir gerçek kişi özellikle bir isim, kimlik numarası, konum verileri, çevrim içi tanımlayıcı ya da söz konusu gerçek kişinin fiziksel, fizyolojik, genetik, ruhsal, ekonomik, kültürel veya toplumsal kimliğine özgü bir ya da daha fazla sayıda

faktöre atıfta bulunularak doğrudan veya dolaylı olarak tanımlanabilen bir kişidir (TDK, 2023)".

Verilen tanımlardan da anlaşılacağı üzere kişiyle ilişkilendirilemeyecek veriler kişisel veri sayılmamaktadır. Kişiye ait belirlenebilir bilgiler; ad, soyad, adres, telefon numarası, nüfus bilgileri, etnik köken, medeni hal, iş hayatına ilişkin bilgileri, sosyal medya adresleri, eğitim ve öğrenim bilgileri, biyometrik veriler vb. bilgiler tamamıyla kişisel veri olarak kabul edilmektedir. Kişinin cep telefonu markası, kullandığı arabanın markası ya da eşyası vb. ürünler o kişi ile ilişkilendirilebilirse veya başka bir bilgi ile birleştiğinde o kişiye ait olduğu anlaşılabiliyorsa kişisel veri olduğu ileri sürülmektedir (Çobansoy, 2020).

Veri Sorumlusu: Kişisel Verilerin Korunması Kanunu, veri sorumlusunu; "kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişi" şeklinde tanımlamaktadır. Tüzel kişiler, kişisel verileri işleme konusunda gerçekleştirdiği faaliyetler kapsamında "veri sorumlusu" olarak nitelendirilmektedir ve ilgili düzenlemelerde belirtilen hukukî sorumluluk tüzel kişinin şahsına aittir. Bu konuda kamu hukuku tüzel kişileri ve özel hukuk tüzel kişileri bakımından bir farklılık gözetilmemektedir. Kanuna göre veri sorumlusu kişisel verilerin işlenme amacını ve yöntemini belirleyen kişidir. Yani işleme faaliyetinin "neden" ve "nasıl" yapılacağı sorularının cevabını verecek kişidir (Kişisel Verilerin Korunması Kanunu [KVKK], 2016)."

Veri İşleyen: İşleme faaliyetini yürüten kişi olarak algılanmamalıdır. Ayrı bir aktör olarak Kişisel Verilerin Korunması Kanununda veri sorumlusunun verdiği yetkiye dayanarak veri işleme faaliyetini/hizmetini yürüten kişidir. Gerçek ya da tüzel kişi olabilir. Bazı durumlarda veri sorumlusu ile veri işleyenin saptanması uygulamada zor olabilir. Bu sorunu ortadan kaldırmak için veri işleyenin hukukî niteliğinin somut olarak saptanması gerekmektedir. Hukukî nitelik olarak veri sorumlusunun adına ya da onun verdiği yetkiyle iş yaptığı görülmektedir. Veri sorumlunun çıkarına ya da yetkilendirmesiyle işleme yapılmaktadır. Veri işlemenin amacı da veri sorumlusunun belirlediği amaca göre oluşmaktadır. İşleme faaliyetinin neden ve nasıl sorularının cevabını da veri sorumlusu belirleyecektir. Veri sorumlusuyla veri işleyen arasındaki

hukukî ilişki verilerin korunması ve tehlikelerin önlenmesinde müştereken sorumluluktur. Veri işleyen birden çok olabilir. Bazı durumlarda veri işleyen ve veri sorumlusunun tanımları birbiriyle çakışabilir veya örtüşebilir (Küzeci ve Kılıç, 2019).

Kişisel veri işleme sözleşmesi verinin öznesi ile akdedilmesinin ardından veri işleyen edimi ifa yükümlülüğü altına girmektedir. İşe göre edimlerinde olduğu gibi veri işleyen sözleşme talimatlarına uygun davranmakla ve işi özenle yapmakla yükümlüdür. Veri işleyenin aynı zamanda sır saklama yükümlülüğü de bulunmaktadır (Başara, 2020).

Özel Nitelikli Kişisel Veri: Avrupa Birliği (AB) hukukunda özel nitelikli kişisel veriler siyasi görüş, ırksal köken, etnik köken, dini/felsefi inançlar, genetik veriler, biyometrik ve kişiyi ayırt etmekte kullanılan bilgilerle ilişkilidir. Türk hukukunda AB hukukuna ek olarak dernek üyelikleri, cinsel yönelim, ceza mahkumiyeti bilgileri, mezhep, kılık ve kıyafeti gibi ek unsurlar da eklenmiştir. Bu verilerle kişiler bazı gruplar tarafından ayrımcılığa uğrayabilme ihtimali olduğundan güçlü koruma gerektirmektedir (Oguz, 2018).

Hassas Veri: Hassas veriler, kişisel verilerin diğer verilerden daha fazla koruma uygulanan kısmıdır. Bu veriler özel yaşamın gizliliği ve temel hakları ihlâl edici yapıda bulunan verilerdir. Özel korumaya layık verilerdir. Özellikle cinsel yönelim, siyasi görüş, ırksal farklılık, dini ve felsefi inançlar, sağlık durumu ve cinsel yaşam bilgileri ve sendika üyelikleri bunlara dahil edilebilir. Hassas verileri özel nitelikli kişisel verilere dahil edilebilecekken çeşitli ülkelerdeki kanun koyucular özel nitelikli kişisel veri ve hassas veri algılamasının farklı olduğunu ifade etmiştir (Kaya, 2011).

Adî Veri: Adî veriler Özel Nitelikli kişisel verilerin dışında kalmış olan bilgileri içermektedir. Kişiyle ilişkilendirilemeyen ya da kişiyi belirlemeyen bilgilerdir. Teknolojinin gelişmesiyle adi veriler kişinin tespitinde kullanılabilecek hale gelse de herhangi bir hukukî düzenleme yapılmazsa eğer halâ adi veri sayılacaktır (Oğuz, 2018).

Biyometrik Veri: Biyometri insana ait özellikleri ifade etmektedir. Biyometrik veri bireyin herhangi bir çaba sarfetmeksizin elde ettiği ve ömür boyunca beraberinde

taşıdığı verilerdir. Bunlar parmak izi, yüz, DNA, avuç içi izi, sesi, yürüyüşü ve imzası gibi çoğaltılabilmektedir. Biyometrik verideki en önemli nokta bu verilerin belirli bir kişiyle ilişkin olup onun tanımlanmasını sağlamaktadır ve bu verilerin değişmesi genelde mümkün değildir. Bu verileri kişi kendisi bizzat taşımaktadır. Biyometrik veriler hem hassas veriler hem de kritik kişisel veriler başlığında incelenebilmektedir. Biyometrik veriler aracılığıyla kişilerin sağlık verilerine de ulaşmak mümkündür. Bu yüzden biyometrik verilerin korunması önemini arttırmaktadır. Biyometrik veriler farklı alanlarda kullanılabilmektedir. Örneğin iris tanıma, ses tanıma yüz ve parmak izi tanıma ile kimlik doğrulama işlemi gerçekleştirilebilmektedir. Parmak izi biyometrik veriler içerisinde en fazla kullanılan yöntem olurken iris tanıma sistemi en güvenilir biyometrik doğrulama yöntemi olduğu doğrulanmıştır. Biyometrik verilerin işlenme ilkeleri 6698 sayılı kişisel verilerin korunması kanunu ile güvence altına alınmıştır. Bu veriler öğrenilmesi halinde kişiyi ayrımcılığa uğratma ihtimali olduğundan mağduriyete neden olabilecek türde bir veridir (Erdinç, 2020).

Anonim Veri: Anonim hale getirilmiş veridir. Veriler kimseyle ilişkilendirilemeyecek hale getirilmiştir. Kaynağı belirlenemeyecek belirli bir kişi ile bağlantısı kurulamayacak veridir (Habip, 2013). Anonim verileri genellikle sağlık, banka ve emniyet kurumlarında kullanılmak üzere avuç izi, retina izi ve parmak izi gibi veriler oluşmaktadır (Hoşnut, 2019).

1.1.2. Uluslararası Hukuk Düzenlemeleri

1948 yılından itibaren İnsan haklarını ve normları düzenleyen "İnsan Hakları Evrensel Beyannamesi" insanların özgürlük haysiyet ve haklar bakımından eşit olduklarının savunulduğu uluslararası bir sözleşmedir. Bireye saygı duyulması ve ayrımcılığın ortadan kaldırılması tüm insan hakları çalışmalarının ve çalışmacılarının konusu olmaktadır. Kişisel veriler ile ilgili uluslararası düzenlemeler bu tarihlerden itibaren hız kazanmıştır (Karaca-Dedeoğlu, 2019). 1960 ve 1970'li yıllarda kişisel verilerin etraflıca çalışmaya ve tartışılmaya başlanmıştır. Almanya'nın Hessen Eyaletinde hazırlanan "Veri Koruma Kanunu" ilk düzenlemelerden birisi olarak kabul edilmektedir. 108 sayılı sözleşme (Kişisel Verilerin Otomatik İşleme Tâbi tutulması Karşısında Bireylerin Korunması

Sözleşmesi) Türkiye'nin de tarafı olduğu ilk sözleşmelerdendir (Sultanlı, 2021).

Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı T.C. Başbakanlığı tarafından 2014 yılında yayınlanan gerekçesi aşağıdaki gibidir.

"108 sayılı sözleşme olarak da bilinen ve 27 maddeden oluşan Sözleşmenin temel amacı; her üye ülkede, uyruğu veya ikametgâhı ne olursa olsun gerçek kişilerin, temel hak ve özgürlüklerini ve özellikle kendilerini ilgilendiren kişisel nitelikteki verilerin otomatik bilgi işleme tabi tutulması karşısında özel yaşam haklarını güvence altına almaktır. Bu itibarla Sözleşme, hükümetlerin vatandaşlarını korumasına yönelik önemli bir araç niteliğindedir.

Ülkemizde kişisel verilerin korunması bağlamında sürdürülmekte olan ulusal mevzuat çalışmalarına da paralel olarak, söz konusu Sözleşmenin onaylanması, ülkemizin Avrupa Konseyi çerçevesinde oluşturulan ortak hukuk sistemine kişisel verilerin korunması alanında da dâhil olmasını sağlayarak, vatandaşlarımızın insan haklarının ihlal edilmesinin önüne geçilmesine ve ülkemizin saygınlığına katkıda bulunacaktır. ..." (T.C. Başbakanlık Kanunlar ve Kararlar Genel Müdürlüğü, 2014).

a. 108 Sayılı Kişisel Verilerin Otomatik İşleme Tabi Tututlması Karşısından Bireylerin Korunması Sözleşmesi

Avrupa Konseyinin faaliyetleri insan haklarına odaklı ilerlemektedir. Bu ilerlemeyle kişilik hakları Avrupa hukukunda insan hakları içerisinde kendine yer bulmaktadır. Avrupa Konseyi'nin hazırladığı 108 sayılı sözleşme, özellikle kişisel verilerin korunması için bağlayıcılığı bulunan ilk hukukî düzenleme olarak ortaya çıkmıştır. Bu sözleşme sadece Avrupa ülkeleri için değil diğer ülkelerin katılımına da açılmıştır. Bu belge kişisel verilerin işlenmesi ve aktarılması için kısıtlayıcı bir düzenleme içermektedir. Türkiye, imzaya açıldığı 1981 yılında sözleşmenin bir tarafı olmuştur. Bu sözleşmeyi onaylayan KVKK ise 2016 yılında resmî gazete yayınlanarak yürürlüğe girmiştir (Elbir, 2020).

b. İktisadi İş Birliği ve Gelişme Teşkilatı (OECD)

Kuruluş tarihi 1961 yılı olan teşkilatın merkezi Fransa'dır. Teşkilatın kuruluş amacı

Konvansiyonun giriş bölümünde 1 maddede açıklanmıştır. (İktisadi İş Birliği ve Gelişme Teşkilatı [OECD], 2023). Buna göre amaç "*Mali istikrarı koruyarak, en yüksek sürdürülebilir ekonomik büyümeyi ve istihdamı sağlayacak, üye ülkelerde hayat standardını yükseltecek ve böylece dünya ekonomisinin gelişmesine, üye olan veya olmayan ülkelerde sağlıklı ekonomik kalkınmaya, uluslararası yükümlülüklere uygun olarak çok taraflı dünya ticaretinin büyümesine ayırım yapmadan katkıda bulunacak siyasalar geliştirmek* (OECD, 2023)*"* olarak belirtilmektedir.

OECD 1980 yılında sınır ötesi kişisel verilerin korunması ve özel yaşamın gizliliğine dair ilkeleri kabul ederek, kişisel verilerinin korunması için ilk adımı atan uluslararası örgüt olmuştur. Bu ilkelerin kabul edilmesi aslında OECD üyesi devletlerin ekonomik anlamda gelişmelerini amaçlamaktadır. Ayrıca yetkisiz girişleri kontrolü, asgarîlik, verilerin hukuka aykırı elde edilmesinin önlenmesi gibi prensipler de içermektedir. Veri akışının gerçekleşmesine yönelik tavsiyeleri de aşağıdaki gibidir (Dülger, 2018);

- Açıklık
- Veri Toplamanın Sınırlı Olması
- Sınırlı Kullanım
- Hesap Verme Zorunluluğu
- Bireyin Katılımı
- Veri Kalitesi İlkesi

c. Avrupa Birliği Genel Veri Koruma Tüzüğü

1998 yılından beri geçen süreçte teknolojik gelişmelerin de yaşanmasıyla kişisel verilerin korunması ile ilgili hukukî düzenleyici bir tüzük arayışına gidilmiştir. Tüzük çalışmasına 2012 yılında başlanılmıştır. Avrupa Konseyi, Avrupa Parlamentosu ve Avrupa Komisyonu da sürece katılmıştır. Tüzük kişisel sağlık verilerinin korunmasını açıkça destekleyen ve önemini vurgulayan ifadeler içermektedir. Tüzük, özel yaşama saygı, aydınlatılmış onamın alınması ve toplanmış verilerin akıbeti gibi konuların gerekliliklerine değinmiştir (Gökçay ve Arda, 2019).

d. Veri Koruma Direktifi

Tam adı 95/46/AT Sayılı Veri Koruma Direktifidir. 1995 yılında yürürlüğe girmiştir. AB vatandaşlarının verilerinin üçüncü kişilere karşı korunması hedeflenmiştir. Şunu belirtmek gerekir ki direktifler birlik ülkelerinin hukuk sistemlerine doğrudan doğruya etki etmemektedir. Dolayısıyla direktifler hukuk sistemlerine uyumlaştırılacak şekilde yasal düzenlemelere ihtiyaç duymaktadır. Veri Koruma Direktifi genel hükümlerden sonra hukukî tedbirler, hukuka uygunluk nedenleri, verilerin üçüncü ülkelere transferi, sorumluluklar ile yaptırımlar ve denetleyici otoriteyi belirten bölümlerden oluşmaktadır. Ayrıca direktif yalnızca gerçek kişileri korumayı hedeflerken tüzel kişileri kapsam dışı bırakmıştır. Veri korumasını kapsamlı bir şekilde düzenleyen direktif istisna oluşturan halleride belirtmiştir. Veri koruması özel hayatın gizliliğini koruyan ve çıkar çatışmasını dengelen bir düzenlemedir. Birlik ülkeleri veri koruma direktifi izleyen düzenlemeleri yapmak ve gerekli denetimleri sağlamak zorundadır (Akıncı, 2017).

e. Avrupa İnsan Hakları Sözleşmesi (AİHS)

Kişisel verilerin korunması hakkı Avrupa İnsan Hakları Sözleşmesi'nde bağımsız bir hak olarak düzenlenmemiştir. Ancak özel hayatın gizliliğinden bahsedilen 8. madde özü itibariyle Kişisel Verilerin Korunmasını amaçladığı için bu hak korunmuştur. Avrupa İnsan Hakları Mahkemesi özel hayatın gizliliğini geniş yorumlayarak 8. madde ile kişisel verilerin korunması hakkı da korumaktadır (Yıldırım, 2019). AİHS 8. madde ise şu şekildedir:

> *"1. Herkes özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir.*
>
> *2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin hukuka uygun ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir. (Avrupa İnsan Hakları Sözleşmesi [AİHS], 2023)"*

f. Avrupa Birliği Temel Haklar Şartı

2000 yılında Fransa'nın Nice kentinde düzenlenen konferansta Avrupa Parlamentosu, Avrupa Konseyi ve Komisyonu, Temel Haklar Şartını kabul etmiştir. Bu konferansın amacı temel hakların daha anlaşılır bir şekilde yorumlanması ve bu haklara daha seçkin bir yer ayırma fırsatı vermektedir. Sosyal ve teknolojik değişimlerin temel hakların korunmasında yapılacak değişiklikleri de beraberinde getirdiği ve bu duruma uygun müdahalelerin de yapılması gerekliliği Temel Haklar Şartının kabulünü neredeyse zorunluluk haline getirmiştir. Temel Haklar Şartının "Özgürlükler" kısmında ise kişisel verilerin korunmasına ayrıca yer verilmiştir. Kişisel veriler bir haktır ve bu hak kişinin rızası ile meşru yollar için kullanılabilmektedir. Ayrıca kişi bu şartlara göre kendisi hakkında toplanmış bilgilerine ulaşma, bilgilerinde değişiklik ve güncelleme talep etme hakkına da sahiptir ve bağımsız makamlarca denetim yapılabilmektedir (Ağıralan, 2015).

g. Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi

Birleşmiş Milletle İnsan Hakları Komisyonu 1948 yılında Paris'te sunulan BM Genel Kurulu konferansı ardından kabul edilen evrensel bir beyannamedir. Otuz maddeden oluşan bildirinin 1,7 ve 12. maddeleri kişi mahremiyeti ile ilişkilidir. İnsanların hür, onur ve haklar eşit olduğunu vurgularken; özel yaşamın gizliliği, aile, konut ve haberleşme dokunulmazlığına da değinilmiştir (Özer, 2015).

h. Amsterdam ve Lizbon Bildirgeleri

Lizbon Bildiresi hasta hakları konusunda yapılmış ilk ve en kapsamlı bildirgelerdendir. 1981 yılında yapılmıştır. 1981 yılında yapılan bildirgenin 4. Maddesinde "*Hasta, hekimden tüm tıbbi ve özel hayatına ilişkin bilgilerin gizliliğine saygı gösterilmesi hakkına sahiptir."* İfadesi kullanılmıştır. Bildirinin 8. maddesinde gizlilik hakkı yapılması gereken usuller, bilgiye ulaşabilme hakkı ve açık izin hakkında hükümler yer almaktadır. Amsterdam bildirgesi ise 1994 Avrupa İnsan Haklarının geliştirilmesi bildirgesinin bir ürünüdür. Odak konusu "mahremiyet ve özel hayattır" 4. maddesinde ise hastanın ölümünün gerçekleşmesi durumunda dahi bilgilerinin gizliliğinin korunması düzenlenmiştir (Küçükbasmacı, 2022).

1.1.3. Türk Hukukunda Kişisel Veri Korumasının Gelişimi

Maddi ve manevi olarak bütün bir biçimde ele alınan varlık olan insanın özel alanına yapılmış tecavüz ve haksız davranış, kişinin şeref ve haysiyetini doğrudan etkileyerek haksız fiili oluşturmaktadır. Özel hayatın içinde değerlendirilen bilgi ve belgelerin gizlice öğrenilmesi ve başka kişilere aktarılması da kişilik haklarının ihlâline neden olmaktadır. Hasta verilerinin başkaları tarafından öğrenilmesi değil de gizlice öğrenilmesi burada önem arz etmektedir. Çünkü kişinin kendi iradesi ile özel alanından çıkarmış olduğu bilginin ortak alana geçmesinin sorumlusu yine kendisidir. Ortak alandaki bilgiler ve yaşantılarda gizlilik aranmamaktadır. Özel alan ve özel hayat alanında kişinin yakın çevresi tarafından bilinecek bilgileri paylaşılırken gizli alanında kişinin başkaları ile paylaşmak istemediği yazışmaları, sağlığına ait bilgi ve belgeler bulunmaktadır (Aydın, 1998).

Sağlık yalnızca işletme mantığı ve ekonomi bilimiyle yönetilememektedir. Sağlıkta vazgeçilemeyecek normatif değerler vardır ve bunlar korunmalıdır. Türkiye Cumhuriyeti Anayasasının 17. Maddesinde "Herkes, yaşama, maddi ve manevi varlığını koruma ve geliştirme hakkına sahiptir" ifadeleri herkesin sağlık hizmetini alıp, insan onuruna yakışır bir şekilde hakkaniyetle hizmete ulaşması hedeflenmektedir. Böylece hasta ve hekim arasındaki ilişkiyi müşteri ve satıcı ilişkisi olarak görmek mümkün değildir. Dolayısıyla hasta ile hekim arasında bir tüketici sözleşmesi yoktur bir vekalet sözleşmesi söz konusudur. Çünkü hekimin elinde büyük bir güç vardır hem arzı hem de talebi oluşturur. Burada hastanın yararı ve çıkarları gözetilerek işlerin yürütülmesi gerekmektedir (Özlü, 2010).

Anayasal düzenlemelerde kişisel verilerin korunması açık şekilde düzenlenmemiştir. Kişisel verilerin korunması için ilk olarak 1961 Anayasası ve 1982 Anayasalarında düzenlemeler yapılmıştır Bunlar Kişi Hak ve Ödevleri başlığında temel bir hak olarak ele alınmıştır. Dolayısıyla kişi hak ve ödevleri temel haklardandır (Eroğlu, 2011). Anayasanın 12. maddesi temel hakları şu şekilde tanımlar; "*Herkes, kişiliğine bağlı, dokunulmaz, devredilmez, vazgeçilmez temel hak ve hürriyetlere sahiptir. Temel hak ve hürriyetler, kişinin topluma, ailesine ve diğer kişilere karşı ödev ve sorumluluklarını da ihtiva eder* (T.C. Anayasası [Ay.] m.12). Ayrıca 5982 sayılı kanun ile Anayasada değişiklik yapılarak 20. maddeye ilave fıkra eklenmiştir. Eklenen fıkrada aslında herkesin kendi kişisel verisini koruma

hakkına sahip olduğundan bahsedilmektedir. Anayasanın 20. maddesinde "*Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz.* (Ay. m.20)*"* şeklinde ifade edilmiştir.

Bu hakla kişi kendi kişisel verisinin hakkında bilgilendirilme, amaç doğrultusunda kullanıldığını öğrenilme, düzeltilmesini ve silinmesini talep etme hakkına da sahiptir. Bu değişiklikte verilerin kaydedilmesinin şartı da açık rıza olarak getirilmiştir. Bu kanunda kişisel verilerin korunmasına yönelik usul ve esaslar ayrıntılı bir şekilde düzenlenmiştir. Bu ilave fıkra açık rızanın önemini vurgularken bilimsel araştırmalar için kullanılacak verilerde aydınlatılmış onamın da önemini vurgulamaktadır (Gökçay ve Arda, 2019).

Kişilik Hakları Türk Medeni Kanunu'nun 24. maddesinde genel olarak değerlendirilmektedir. Verilerin hukuka aykırı bir şekilde ele geçirilmesin hukuk açısından son bulması Türk Medeni Kanunu 25. madde ve zararın tazmini Türk Borçlar Kanunu 49. maddelerine göre gerçekleştirilmelidir. Ceza hukukunda kişisel verilerin korunması, kişilere karşı suçlar başlığında incelenmektedir. Kişilere karşı suçlar Türk Ceza Kanunu (TCK) 135. maddedeki kişisel verilerin izinsiz kaydedilmesi ve 136. maddedeki Verileri hukuka aykırı verme veya ele geçirme suçunu oluşturmaktadır. Bu suçların nitelikli hali ise TCK 137. maddede ve TCK 138. maddede ise "verilerin yok edilmemesi" suçu bulunmaktadır. 140. madde güvenlik tedbirlerini sıralamaktadır. Böylece 6698 sayılı Kişisel Verilerin Korunması Kanunu ve TCK m. 135 ile m. 140. arasında sıkı bir ilişki görülmektedir. Dolayısıyla hem Anayasanın 20. maddesi hem de Avrupa İnsan Hakları sözleşmesi TCK tarafından korunan bir değer haline gelmiş olmaktadır (Dülger, 2016).

Kişisel verilerin korunması kamu hukukunu ilgilendiren bir başlık olmasına rağmen kişilik hakkı olarak ele alındığında özel hukuku da bir parçası haline gelmektedir. Bu yüzden klasik kamu hukuku ve özel hukuk ayrımında tam olarak belirli bir yeri yoktur. Kişilik hakkı medeni hukuk ana bilim dalının bir konusudur. Kişisel verilerin korunması anayasal niteliği Anayasanın 20. maddesi ile açıklanabilse de Türk Medeni Kanunu'nda kişiliğin korunmasını da ilgilendirdiğinde bir özel hukuk boyutu da olduğunu göstermektedir (Taştan, 2017).

Kişiye değer veren hukuk düzeni, gerekli hukukî düzenlemeleri yapmak zorundadır. Kişilik hakkı kişiye her şeyden önce sırf bir birey olduğu için verilmiştir. Kişinin kişilik haklarına sahip olması için herhangi bir özelliğinin, vasfının ya da niteliğinin olmasına ihtiyacı yoktur. Kişilik hakkı kişinin toplumdaki yerini koruyan bir haktır. Herkese karşı ileri sürülebilen bir haktır (Acar, 2010).

Kişilik hakkı çağdaş hukuk düzeninin temellerini oluşturan en önemli unsurlardandır. Hukuk düzeni kişinin gelişimini temin etmek, kişiye saygı duymak ve kamu otoritesince gerekli önlemlerin alınmasını sağlayarak kişiliğin korunmasının önlemini almak zorundadır. Kişilik hakkı, kişiye karşı devlet otoritesini sınırlandıran, iktidarın sınırı çizerek kişiye özgür alan sağlayan bir haktır. Somut durağan bir hak değildir bu yüzden sınırlarını belirlemek zordur. Birçok farklı konu kişilik hakları içerisinde değerlendirilebilir. Kişilik hakkını oluşturan haklar ise; mutlak haklar, şahıs varlığı hakları, kişiye sıkı sıkıya bağlı haklar ve tekelci haklar şeklinde sıralanmaktadır (Gürbüz, 2015).

Kişisel verilerin korunması anayasal olarak bir hak olarak nitelendirilse dahi asıl korunan değer mahremiyettir. Mahremiyeti özel hayatın gizliliği olarak ele alırken aynı zamanda medeni hukukun dalı olan kişilik haklarında da değerlendirilmesi gerekmektedir. Mahremiyet kişilik haklarıyla korunan bir kişilik değeridir. Sağlık verileri taşıdığı niteliklerle özel nitelikli veriler kategorisine girmektedir ve saklanması, işlenmesi, silinmesi ve aktarılması özel kurallara tabi tutulmaktadır. Nedeni ise sağlık verileri sadece özel hayatı ilgilendirmeyip mesleki itibar, kişinin şerefi, haysiyeti gibi konuları ile de sıkı bir ilişki içerisinde olmasıdır. Bu nedenle Kişisel Verilerin Korunması Hukukunun medeni hukuk içerisinde incelenmesi gerekmektedir (Akkurt, 2020).

1.1.4. Kişisel Verilerin Korunması Kanunu

Kişisel Verilerin Korunması Kanunu teknolojinin gelişmesiyle dolayısıyla veri depolamanın ve aktarmanın günümüzde artık çok kolay hale gelmesinden kaynaklanan bir ihtiyaç olarak ortaya çıkmıştır. Fakat tek bu hususlardan dolayı kabul edildiği söylenemez. Kanun oluşumunun nedeni aslında yapılmış uluslararası anlaşmalardan doğan bir hukukî düzenleme eksikliğinden kaynaklanmaktadır.1985 yılında yürürlüğe girmiş olan 108 sayılı Kişisel Verilerin Otomatik İşleme Tabi

Tutulması Karşısında Bireylerin Korunması Sözleşmesi, 2008 yılında yapılan Avrupa Birliği İlerleme Raporu'nda Türkiye için yapılan çerçeve kanun olmaması hakkında eleştiriler ve Avrupa Yönergesindeki veri aktarımı ile ilgili maddelerin varlığı kanunun oluşumu için büyük rol oynamıştır (Kutlu ve Kahraman, 2017).

Uluslararası sözleşmeler ve antlaşmaların yanı sıra Türkiye'deki hukukî düzenlemeler de ilgili kanunu destekler niteliktedir. 2016 yılında resmî gazete yayınlanan Kişisel Sağlık Verilerinin Korunması ve Mahremiyetinin Sağlanması Hakkında Yönetmelik, 6698 Sayılı KVKK'ya dayandırılarak oluşturulmuş ve verilerin toplanması, saklanması, aktarımı gibi birçok konuya değinmiştir. Uyulacak usul ve esaslar yönetmelik maddelerinde açıkça belirtilmiştir.

6698 Sayılı Kişisel Verilerin Korunması Kanunu (KVKK) 2016 yılında kabul edilmiştir ve Resmî Gazete 'de (RG) yayınlanmıştır. Kanun'un amacı 1. madde de ifade edildiği gibi kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir (Kişisel Verilerin Korunması Kanunu [KVKK], 2016). 2010 yılı Anayasa değişikliği sonrası Anayasanın 20. maddesine ek Kişisel Verilerin Korunmasına yönelik çerçeve bir yasa olarak yürürlüğe girmiştir (Küzeci, 2010).

Kişisel Verilerin Korunması Kanunu (KVKK) 1. maddesi kanunun amacını açıkça şu şekilde belirtmiştir. *"Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir* (KVKK, 2016)*"*

Kişisel sağlık verilerinin işlenmesi, sağlık verilerinin elde edilmesinden başlanarak daha sonra veriler üzerinde yapılan her türlü işlem ya da işlemleri ifade etmektedir. Verilerin işlenme süreci, 6698 sayılı kanun kapsamın birçok aktörün koordine bir şekilde bir araya gelmesi ile gerçekleşen işlemler dizisidir. Kişisel sağlık verilerinin korunması her zaman gündemde olan bir konudur ve 6698 sayılı kanun ile düzenleme yapılmıştır. Yapılacak her türlü ihlâl kanun kapsamında sonuç doğuracaktır. Verilerin ihmali ya da kasıtlı bir şekilde korunma yükümlülüğünün

ihlâl edilmesi durumunda hukukî ve cezaî açıdan sorumlu olunması durumunu ortaya çıkaracaktır (Öget, 2020).

Ayrıca kişisel sağlık verilerinin korunmasında en öncelikli husus ihlâlin gerçekleşmemesidir. İhlâl gerçekleştikten sonraki koruma verilerin korunmasında esas olmayacaktır, ikincil olacaktır. Çünkü koruma yollarında ihlâlin geri dönüşü olmayacaktır. Ayrıca çalışmasında sağlık kurumlarında mahremiyete ilişkin ihlâllerin hiç azımsanmayacak düzeyde yüksek olduğunu ifade etmiştir (Kandilli, 2019).

1.1.5. Kişisel Verilerin Korunmasında İlkeler

Kişisel Verilerin Korunması Kanunu madde 4/2 temel ilkeleri aşağıdaki gibi sıralamıştır (KVKK, 2016):

a) Hukuka ve dürüstlük kurallarına uygun olma.

b) Doğru ve gerektiğinde güncel olma.

c) Belirli, açık ve meşru amaçlar için işlenme.

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma.

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme.

Hukuka Uygunluk ve Dürüstlük: Kişisel veriler hukuka uygun şekilde işlenmiş olmalıdır. Hukuka uygunluk için ilgili kanunun 5. ve 6. maddelerinde olan hukuka uygunluk sebepleri şartlarının sağlanmış olması gerekmektedir. Aykırılıklar bu ilke kapsamında değerlendirilmemelidir. KVKK 12. maddesi aykırılıkların bu ilke içinde değerlendirilmesi sonucunda amacına uygun olmayan genişlemeler gelmesine neden olabilecektir. KVKK'da dürüstlük kuralına göre işleme Türk Medeni Kanunu 2. maddesindeki dürüstlük kuralıyla eş anlamlı değildir. Dürüstlük kuralının kanun içerisinde kullanılması dürüstlüğün geniş bir anlamı olmasındandır (Yücedağ, 2019).

Amaca Bağlılık: Kişisel veriler daha önceden belirlenmiş bir amaç ya da amaçlarla doğru orantılı olarak işlenmelidir. Amaç hukuka uygun olmalıdır. Kurum, kişi ya da kuruluşlar verileri işlerken amacı uygunluğu her zaman gözetmelidir. Amaç dışına çıkıldığında sorumluluk ortaya çıkmaktadır. Kişisel veriler işlendikten sonra amaç değişirse eğer hastanın yeniden rızasının alınması gerekecektir. Çünkü kişi yeni

amaca rıza göstermeyebilir. Bu ilke ile kişisel verilerin önceden belirlenmiş ve şüpheye mahal vermeyecek amaçlar için işlenebilir. Gelecekte değişen şartlarla yeni amaçlar ve bilinmeyen amaçlar için geçerli değildir (Özdemir, 2009).

Güncel ve Doğru Olma: Kişisel veriler güncel tutulmalı ve doğru olmalıdır. Güncel olmayan veya hatalı olan veriler ve bu gibi durumlar için veri silinmesi ya da düzeltilmesi için gerekli olan işlemlerin yapılması gerekmektedir. Doğru olmayan bilgilerin silinmesi veya düzeltilmesi veri koruma görevlisinin sorumluluğundadır (Kılınç, 2012).

Kişisel verilerin güncelliği ve doğruluğu sadece veri öznesinin değil veri sorumlusunun da çıkarına olacağından iki taraf içinde önemlidir. Veri sorumlusu açısından aktif özen yükümlülüğü bulunmaktadır ve veri sorumlusu verileri güncel ve doğru tutulmasını sağlayacak yolları açık tutmalıdır (Özdemir, Yılmaz ve Kaya, 2022).

Bağlantılı, Sınırlı ve Ölçülü Olma: Kişisel verilerin belirlenen amacı gerçekleştirecek kadarının işlenmesini lüzum olmayan ya da amaç ile alakalı olmayan verilerin muhafaza edilmemesi gerekmektedir. Verilerin amacı gerçekleştirmeye yönelik gerekli olan kadar ile sınırlı olmalıdır. Sonradan ortaya çıkabilecek ihtiyaçlar için veri stoklaması yapılmamalıdır. Muhtemelen gerçekleşecek ihtiyaçlar değil mevcut ihtiyaçlar bu ilkede esastır. Böylece amaçlanan aslında verisi işlenen kişiyi güvenceye alıp, riski minimuma indirip, fazla veri kaydetmeyerek veri ekonomisini oluşturmaktır. Bu ilke aynı zamanda asgarîlik ilkesi olarak da ortaya çıkmaktadır (Kandilli, 2019).

Gerekli Süre Kadar Muhafaza Etme: Bu ilke ile kişisel veriler amaca hizmet etmesi gereken süre kadar saklanmalıdır. Bu ilkenin temelinde veri öznesinin kişilik haklarını korurken veri sorumlusuna da yükümlülüklerini yerine getirirken kolaylık sağlamaktır. Çünkü silinmeyen veriler zamanla büyüyerek veya çoğalarak içinden çıkılmaz bir hal alabilir. Bu sebepten dolayı makul süre içerisinde veriler ya silinmeli ya da anonim hale getirilmelidir. Makul süreyi açıklamak için ise işletmedeki hukukî düzenlemelerin olduğu metinleri anlamak gerekir eğer makul bir süre metinlerde belirlenemiyorsa hakkaniyet ilkesine göre veri sorumlusu bu süreye karar vermelidir.

Bu kararı verirken ileride lazım olur düşüncesiyle verinin daha da saklanmasına müsaade edilmemelidir (Ergüden, 2020).

1.1.6. Kişisel Verilerin Hukukî Niteliği

Kişisel verinin hangi koruma rejiminden yararlanılacağının tespiti için niteliğinin iyi belirlenmiş olması gerekmektedir. Bu konuya ilişkin farklı görüşler bulunmaktadır. Öncelikle kişisel verinin özünde hangi menfaatin ya da hukukî varlığın yattığının belirlenmemiştir. Bu veriler doğuştan kazanılmış bir hak mıdır yoksa kişinin üzerinde tasarrufta bulunabileceği bir mal olarak mı kabul edilmelidir tartışması vardır. ABD'de kişisel veriler için ekonomik-teknolojik hak olarak bakılmaktayken Avrupa sistemlerinde sosyal bir değer olarak kabul görmüştür (İmançlı, 2019).

Ekonomik Hak Görüşü: Amerikan sisteminde kabul görmüş bir görüştür. Amerikalı hukukçulara göre kişisel verilere yapılacak kapsamlı koruma ekonomik faaliyetler ve maliyetler açısından olumsuzlukları beraberinde getirecektir. Avrupalı görüşlerden farklı olarak kişisel verilerin daha düşük düzeyde korunması savunulmuştur. Bu görüş içerisinde mülkiyet hakkı görüşü ve fikri mülkiyet hakkı görüşü ele alınmaktadır (İmançlı, 2019).

Mülkiyet Hakkı Görüşü: Kişisel veriler kişiliğin bir ürünüdür. Mülkiyet hakkı esas alınarak korunan kişisel veriler ilgili kişinin malik olarak tam bir denetim hakkına sahip olması için yasal korumalardan faydalanmasını ve böylece yapacağı anlaşmalar ile verilerinin kullanımı için karşılık alabileceği ifade etmektedir. Bu şekilde verilerinin paylaşılmasına karar vermiş kişilerin özel hayatının gizliliği hakkının da ihlâl edilmeyeceği düşünülmektedir. Bu görüşün eleştirenleri de olmuştur. Kişisel verilerin kullanılmasını mülkiyet hakkına gören devir alan kişi üçüncü kişilere veri sahibinden herhangi bir rıza alınmasına gerek kalmadan devredebileceği sorunu eleştirilen husustur (Bayındır, 2019).

Fikri Mülkiyet Hakkı Görüşü: Kişisel verilerin ve fikrî hakların korunması arasında amaçsal bir birlik bulunmaktadır. Bu birlik iki hakkın da korunmasının amacının asıl olarak bilginin dağıtımının ve kullanımının korunmasından kaynaklanmaktadır. Benzerliğine rağmen kişisel veriler fikrî mülkiyetin kapsamına

girmemektedir. Farklılık irade hususundan meydana gelmektedir. Fikri mülkiyette kişilerin fikri bir çabası mevcuttur. Kişisel verilerde çaba söz konusu değildir. Bu yüzden fikri mülkiyet ve kişisel veriler tam olarak birbirini karşılamamaktadır (Özkan, 2020).

Sosyal Yaklaşım: Avrupa kökenli bir yaklaşımdır. İktisadi yaklaşım olan Amerikan ekolüne karşı sosyo-hümanist bir Kıta Avrupası yaklaşımıdır. Bu yaklaşımda kişisel veri ile veri sahibinin arasındaki bağı koparmaksızın insan hakları ve kişilik hakkı kapsamında değerlendirme yapılmaktadır. Kişilik hakları ve insan hakları birbirinden keskin çizgilerle ayrılamamasından dolayı sosyal yaklaşıma yönelik görüşler ayrıştırılmadan ele alınmıştır (Akkurt, 2020).

Kişilik Hakkı Görüşü: Kişi denildiği zaman akıllara ilk insan gelmektedir. Kişi hak ehliyetine sahip varlıktır. Ancak kişi kavramından sadece insanı anlamak yanlış olur çünkü hukuk dünyasında kişiler insanların yanı sıra mal topluluklarından da oluşmaktadır (Öğüz ve Dural, 2021). Kıta Avrupası'nda kabul gören kişilik hakkı görüşü fikri mülkiyet ve mülkiyet hakkı görüşlerine göre en geniş korumayı yapmaktadır. Kişilik hakkı kavramıyla temel olarak kişinin maddi ve manevi kişilik değerlerinin korunması amaçlanmaktadır. Bunun temelinde insan onuru ve kişiliğin serbestçe geliştirilmesi ve korunması hakkı yatmaktadır. Kişi sınırlar dahilinde nerede, ne zaman ve neyi açıklayabileceği konusunda karar vermek hakkına sahiptir (Koç, 2021).

1.1.7. Bilgi Edinme Hakkı ve Kişisel Verilerin Gizliliği

Kişisel verilerin korunması hakkı ve bilgi edinme hakkı birbiriyle sıkı bir ilişki içerisindedir. İki hak da demokratik bir toplumda olması gereken haklardandır. Kişi kendine ait bir bilgili talep ederse kişisel verilerin korunması hakkı ve bilgi edinme hakkı birbirini tamamlayıcı haklar olarak ortaya çıkar. Fakat bir başkası hakkında bilgi almak isteyen bir kişi o kişinin kişisel verilerinin korunması hakkı ise çatışmaya girer ve burada yarışan haklar konusu ortaya çıkar. 4982 sayılı bilgi edinme kanunu hakkın istisnalarını düzenlerken kişisel verilerin istisnalar arasında yer almadığı görülmektedir. Bilgi Edinme Kanununun istisnaların içerisinde özel hayatın gizliliği vardır. Özel hayatın gizliliği kişisel verilerin korunması ile

ilişkilidir. Bilgi edinme hakkı kişisel verilerin nasıl ve hangi durumlarda korunması gerektiğini kişisel verilerin korunması hakkı ve özel hayatın gizliliği arasındaki ilişki ile ele alınmalıdır (Gündüz ve Yazıcıoğlu, 2021).

Anayasa madde 26: *"Herkes, düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla tek başına veya toplu olarak açıklama ve yayma hakkına sahiptir. Bu hürriyet resmî makamların müdahalesi olmaksızın haber veya fikir almak ya da vermek serbestliğini de kapsar. Bu fıkra hükmü, radyo, televizyon, sinema veya benzeri yollarla yapılan yayımların izin sistemine bağlanmasına engel değildir* (Ay. m.26)*"* ifadesine yer vermektedir.

Bilgi edinmeyi bir özgürlük olarak ele almak durumu farklı sonuçlara götürebilir. Özgürlük devlet ve kurumlar tarafında pasif kalınması ve müdahale etmeme yükümlülüğü anlamına gelmektedir. Bilgi edinme hem hak hem de özgürlük olarak ele alınmalıdır. Bilgi edinme özgürlüğü Anayasanın 26. maddesinde düzenlenen anayasal bir haktır. İnsan hakları sözleşmesinin 10. maddesinde de bu özgürlükten bahsedilmektedir. Bilgi edinme özgürlüğünün sınırı halı ve meşru bir şekilde çizen konu ise özel hayatın gizliliği hakkıdır. İstisna olarak Bilgi Edinme Kanununda 21. maddede düzenlenmiştir. Özel hayatı; kamuya açık alan, özel alan ve gizli alan olmak üzere üçe ayırılmaktadır. Kamuya açık alan dışa açıktır müdahale tamamen serbest olmasa bile sıkı şartlara bağlı değildir. Özel alan aile ve arkadaş çevresine açılan alandır. Gizli alan ise kişilik hakkının özüdür. Bu alan kamusal müdahaleye kapalı çekirdek bir beliktir. Başkalarınca öğrenilmesi kişiye büyük tehdittir. Demokratik bir hukuk devleti, bilgi edinme hakkını topluma verirken özel ve gizli alanında korumasını sağlamalıdır. Güvence altına almak için kanuni ve idari tedbirleri almak zorundadır (Döner, 2022).

Pratik uyuşum ilkesi hakların çatışması halinde, çatışan haklar ve hükümlerin birlikte değerlendirilip uygun bir çözüm yolu bulunmasını sağlar. Bir hakkın diğer hakka hiyerarşisini gözetmeden ya da önceliğini belirlemeden çözümlemeyi sağlar. Bu şekilde bir hak çatışan diğer hakkı ortadan kaldırmayarak optimal bir düzeyde etkisinin devam etmesini sağlamaktadır. Bu şekilde anayasanın bütünlüğü de korunmuş olmaktadır. Pratik uyuşum ilkesi yarışan haklar ve anayasa normlarında denge ihdas etmektedir. Uyuşum aslında etkileşim kavramından etkilenilmiştir. Pratik uyuşum ile dengeleme sağlarken bazı durumlarda bir hakkın diğerine göre

öncelenmesi durumu da ortaya çıkabilir her olay kendi içinde değerlendirilmelidir (Keskinsoy ve Kaya, 2021).

Birbiriyle çelişen anayasal durumlarda pratik uyuşum süreci en azami ve en optimal hukuksal çözümü getirmektedir. Mevcut çelişkilerde pratik uyuşuma başvurma yolunun gerekeceği problemin çözümü için gerekli hale gelmektedir. Çünkü hak ve özgürlüklerin çatışmasında korunan değerlerin ayakta tutulması için bu süreç zorunluluk haline gelmektedir (Ergül, 2015).

Pratik uyuşum ile temel haklarım uyumlandırma süreci ortaya çıkmaktadır. İki temel hakkın birbiriyle çatışmasıyla pratik uyuşum ilkesi uygulanmalıdır. Ölçülülük ilkesi ve öze dokunma yasağı pratik uyuşum içinde değerlendirilmektedir. Temel hakların birbiriyle çatışması sonucu gerilim ortaya çıkmaktadır. Hak ve özgürlükler uyuşturulmaya çalışılırken kullanıldıkları ortam ve koşullar göz önünde tutulmalıdır. Bu uyumlaştırma sürecine gerçek manada bir denge getirilmenin mümkün olmadığı düşünüldüğünden karşı gelenler vardır. Bunun gibi pek çok eleştiriye rağmen pratik uyuşum süreci ya da türevleri hukuktaki hakimiyetini korumaktadır. Temel hakların ele alındığında pratik uyum en iyi çözüm olmasa bile şu an mevcut olan en iyi çözüm yöntemi denebilir. Pratik uyuşum bir anayasa siyaseti olarak dolaylı da olsa temel hak ve hürriyetlerin korunmasına ve halkın güvencesine hizmet eden bir yöntemdir. Ancak her somut olayda pratik uyuşumun dengeyi ve adaleti tesis edemeyeceği de unutulmamalıdır (Özdemir, 2014).

Hasta Yakını, Avukat ve Mirasçılarının Bilgi Edinme Hakkı: Kural olarak kişisel sağlık verisine kanunda belirtilen hukuka uygunluk nedenlerinden birisi sağlanmıyorsa erişilmemesi gerekmektedir. Hasta verisini paylaşmanın iki yolu var ya hasta verisini kendisi paylaşmalıdır ya da paylaşılmasına onay verdiğini açıklayan yazılı ve imzalı onamı vermelidir. Onam sadece onay verilmiş kişiler için geçerlidir. Acil ve ölümcül durumlarda hasta yakınlarına verilecek bilgiler hukuka uygun sayılmalıdır. Yine de bilgi verirken ilkeler göz önünde bulundurulmalı ve gerekli ölçüde kullanılmalıdır. Hasta verisini irade beyanını açıklayamayacak durumdaysa ve verilerinin saklanmasında herhangi bir fayda görülmüyorsa rızası var kabul edilir. Avukatlar ise hasta verilerine ulaşmak için veri öznesi tarafından özellikle yetkilendirilmeleri gerekmektedir. Bu izin vekaletname ile yapılmalıdır ve açık rıza ile

yapılmalıdır. Mirasçılar ölmüş olan yakınının verilerine ulaşmak istiyorsa bu erişim veraset ilamı ile mümkündür. Hasta ölmeden önce sır olarak saklanacak verilere sahipse bu yetkilendirmeyi kısıtlama hakkına sahiptir (Gülhan, 2022).

Avukatlar, kişilerin sağlık verilerine ulaşmak için öncelikle ulaşılmak istenilen amacı içeren ve iş görmenin kapsamını belirleyen vekalet yapmalıdır. Kişilerin sağlık verilerine vekaletsiz yapılacak erişimler güven ilişkisi kapsamına sokulmamalıdır. Genel vekalet verilirken olağan hukukî işlemlerin yapılması amaçlanmaktadır. Özel yetki içeren vekalet ise hususi yapılacak hukukî işlemin sınırını çizerek hukukî koruma sağlamaktadır (Konca ve Badur, 2023).

Sigorta Şirketlerinin Kişisel Sağlık Verisine Ulaşması: Sigorta ettirmek isteyen kişi beyan yükümlülüğü kapsamında sigorta sözleşmesi kurulma anında bildiği ya da bilmesi muhtemel bilgileri sigortacıya eksiksiz bildirmek zorundadır. Beyan için şekil şartı bulunmamaktadır Sigortacı ise aydınlatma yükümlülüğü kapsamında sigorta ettireni aydınlatma zorundadır. Kişisel Verilerin Korunması Kanununa göre sigortacı hem veri sorumlusu hem de veri işleyen konumundadır. Sigortacı, sigorta ettirenden açık rıza almalıdır. Bu açık rıza sağlık verilerinin işlenmesine yönelik ayrıntılı bir şekilde olmalıdır. Açık rızanın hangi amaçla yapıldığı açık ve net olmalıdır. Çünkü sigortacı, hastaneler ve bağlı kuruluşlar hastanın kişisel sağlık verilerine ulaşabilecektir. Sağlık sigortası genel şartları 13. maddesi sırların saklı tutulmasını ele almaktadır. Aydınlatmanın yeteri kadar yapılmaması kişisel verilerin korunması ve 13. madde ile tezatlık oluşturacaktır (Özcan, 2018).

1.1.8. Aydınlatma Yükümlülüğü

Aydınlatma metinleri de hak ve özgürlükler de temeli oluşturmaktadır. Şeffaflık ilkesi de aydınlatma yükümlüğünün temelidir. Aydınlatmanın şekli önemlidir ve aydınlatma karşı tarafın anlayabileceği tarzda ve açıklıkta olmalıdır bu şartları sağlamayan bir veri işleme faaliyetinde aydınlatma yetersiz ve hukuka aykırı hale gelecektir. Aydınlatma açık ama amacında bir yanlışlık ya da eksiklik bulunuyorsa da dürüstlük kuralının ihlâl edilmesiyle aydınlatmanın geçerliliği sakat olacaktır. Aydınlatmanın maddi ve şekli unsurları bulunmaktadır. Şekli unsuru şeffaf, açık, anlaşılır ve öz bilgiyle yapılmış bir aydınlatma oluştururken maddi unsuru

aydınlatmada özellikle yer verilmesi gereken unsurlar oluşturmaktadır. Maddi ve şekli unsurlarda eksiklikten dolayı ilgili kişinin yanılması söz konusu ile aydınlatmada dürüstlük kuralına aykırılıklar meydana gelecektir (Aşıkoğlu, 2019).

1.1.9. Açık Rıza

Sağlık verileri kişiyi maddi, manevi zarara uğratabilecek ve sosyal olarak kişinin toplumda ayrımcılığa uğramasına neden olabilecek verilerdir. Bu yüzden Kişisel Verilerin Korunması Kanununa göre hem özel nitelikli veriler hem de genel nitelikli kişisel veriler hastanın rızası ya da onamı alınmaksızın işlenmemelidir. Açık rıza geçerli olabilmesi kişinin aydınlatılması ile mümkündür. Aydınlatma yükümlülüğü yerine getirilmeksizin alınan rızalar hukuken sakattır. Açık rızanın aranmayacağı haller kanunda açıkça belirtilmiştir. Rıza beyanı genel hukuk ilkelerine yani ahlaka, kanuna ve adaba aykırı olmamalıdır. Kişi onam öncesi işlemin ne olduğunu, amacını ve hukukî dayanağını öğrenmiş olmalıdır. Amacı belli olmayan ve kanuni dayanağı net olmayan rıza göstermekten kaçınılabilir (Deniz, 2022)

Kişisel Verilerin Korunması Kanunu açık rıza için şekil şartı koymamıştır. Açık rıza alınırken belirli şartların sağlanmış olması gerekmektedir. Rıza belirli bir konuya ilişkin olmalıdır, Rıza alınırken bilgilendirme esas alınıp karşı tarafın anlayabileceği açıklıkta ve kolaylıkta olmalıdır. Bilgilendirmede şekil şartı da aranmamaktadır. Veri sahibinin özgür iradeyle açık rızasının alınması gerekir. Kişi teklifi reddedemiyor ya da mecburiyet hissediyorsa özgür iradenin varlığından söz edilemez. Son şart da zaman bakımında açık rızanın doğru yapılmış olmasıdır. Açık rıza en geç veri işleme faaliyet başladığında alınmalıdır. İşleme faaliyeti başlanmışsa ve rıza sonradan alınmışsa rızadan sonraki işlemler hukuka uygun hale gelirken rıza öncesi işlemler hukuka aykırı sayılır. Açık rızası alınan kişi rızasından istediği zaman geri dönebilmelidir (Orak, 2019).

Rızanın Geri Alınması Süreci: Veri işleme faaliyetinde rıza verilmesi ve verilen rızanın geri alınması birbirinden ayrı düşünülmemelidir. Rızası alınan kişiye rızasını geri alırken daha zor bir süreç izletilmesi mümkün değildir. Veri öznesini zarara uğratmadan rızanın geri alınması sağlanmalıdır. Rıza geri alınması sürecinde hizmet kalitesinde bir düşüş yaşanmaması gerekmektedir ve ek ücret ödemek zorunda bırakılmamalıdır. Rızanın geri alınması sürecinde toplanan veriler veri sorumlusu

tarafından silinmesi gerekmektedir. Veri sorumlusunu yasal olarak saklaması gereken veriler silinmeden muaf tutulabilir. Mevzuatta özel olarak süreye tabii tutulan verilen rızanın geri alınması ile silinmeyip hüküm gereği saklanması gereken süre kadar saklanmalıdır (Selek, 2019).

Açık Rızanın Aranmayacağı Haller Kişisel veriler ve içinde hassas veriler sıkı korumaya alınması gereken verilerdir. Verilerin işlenmesi için kanunda açık rıza alınması gerektiği açıkça belirtilmiştir. Fakat her zaman açık rıza almak mümkün olmayabilir. Bunun istisnaları vardır. Dikkat edilmelidir ki açık rıza aranmayan haller yalnızca istisnalar bağlıdır. Kişinin menfaatine, özgürlüklerine, temel hak ve hürriyetlerine zarar vermemek şartıyla veri işleyen ya da veri sorumlusunun meşru faaliyetleri kapsamında yapılmalıdır.

Kişisel Verilerin Korunması Kanunu madde 5/2 de açık rıza aranmayan haller belirtilmektedir (KVKK, 2016). Buna göre;

a) Kanunlarda açıkça öngörülmesi.

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukukî geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması.

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması.

d) Veri sorumlusunun hukukî yükümlülüğünü yerine getirebilmesi için zorunlu olması.

e) İlgili kişinin kendisi tarafından alenileştirilmiş olması.

f) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması.

g) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek koşuluyla veri sorumlusunun meşru menfaatleri için veri işlemesinin zorunlu olması

durumlarının varlığı gereklidir.

1.1.10. KVKK Hükümlerinin Uygulanmayacağı Haller

KVKK madde 28'de belirtilen hükümler hem özel nitelikli veriler hem de genel nitelikli veriler için uygulanabilmektedir. Açık rıza olsun ya da olmasın veriler, 28. madde hükümlerine göre işlenebilecektir. Hükme ilişkin durumlardan birisinin var olması durumunda KVKK hükümlerine aykırı bir veri işleme faaliyeti söz konusu olmayacaktır (Braun, 2021).

Kişisel Verilerin Korunması Kanunu madde 28/1 (KVKK,2016)

"*Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz"* şeklinde kanun hükümlerinin uygulanamayacağı durumlar belirtilmektedir:

a) Kişisel verilerin, üçüncü kişilere verilmemek ve veri güvenliğine ilişkin yükümlülüklere uyulmak kaydıyla gerçek kişiler tarafından tamamen kendisiyle veya aynı konutta yaşayan aile fertleriyle ilgili faaliyetler kapsamında işlenmesi.

b) Kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi.

c) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlâl etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi.

ç) Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbarî faaliyetler kapsamında işlenmesi.

d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi."

1.1.11. Kişisel Verilerin Silinmesinin Talebi

Unutulma hakkı olarak da tartışıldığı görülmektedir. Böyle bir hakkın insan hakkı olup olmaması bir tartışma konusudur. Unutulma hakkı kişilerin temel hak ve özgürlüklerini ihlâl etmeden, onları topluma karşı damlamadan şekillendirilmeye çalışılan bir haktır. Bilimsel ve tarihsel araştırmalarında, kamu yararı için arşivleme faaliyetlerinde, istatistik faaliyetlerinde ciddi olumsuzluklar oluşturacaksa ya da

çalışmaları imkânsız hale getirecekse Unutulma hakkından söz etmek mümkün olmayacaktır. Kişisel verilerin ne sürede silineceğinin mevzuatta belirtilmesi gerekmektedir. Bu süre, verinin belirli amacı gerçekleştirilmesi ve veriyi işlemek için yetecek süredir. Söz konusu biyomedikal veriler ise sürenin ne olacağı netlik kazanmalıdır. 6698 Sayılı Kanun'a göre verinin saklanması için artık bir sebep kalmamışsa veriyi ya anonim hale getirmek ya da silmek gerekmektedir. Gelecekte veriyi kullanabilme ihtimali veriyi saklamak için yeterli olmayacaktır. Veriye dayalı yapılacak gelecek yeni araştırmalar için bu hükümler tartışmalıdır (Büken ve Ünsal, 2017).

Verinin silinmenin isteme hakkı, kişinin verilerinin geleceğini belirlenme hakkıdır. Verisi işlenen kişi verinin saklanma amacının ortadan kalkması rağmen silinmeyen verinin silinmesini talep etme hakkına sahiptir. Silinme hakkı, unutulma hakkı ve silme hakkı olarak da geçmektedir. Birey verisinin dijital dünyadan bir daha hatırlanmayacak şekilde silinmesini ve üçüncü kişiler tarafından öğrenilmeyecek şekilde yok edilmesini isteyebilmektedir. Unutulma hakkı tam olarak bunu hedeflemektedir. Kişi geçmişte yaşanan ve kaydedilen bilgilerini eğerki günümüzde herhangi bir üstün kamu yararı amacına hizmet etmiyorsa ve bu bilgilerinin toplum tarafından öğrenilmesini istemiyorsa silinmesini talep etme hakkına sahiptir (Bayraktar, 2022).

KVKK, kayıtların sınırsızca yapıldığı, kaydedildiği ve kontrolsüzce aktarıldığı ortamlarda verilerin silinmesinin de talep edilmesini temin eder. Dolayısıyla unutulma hakkı ayrı bir hak olarak ortaya çıkmaktadır. Unutulma hakkı kişiye kaydedilmiş bilgilerini kontrol edebilme yetkisi veren bir haktır. Unutulma hakkı kişiye geçmişine ait izleri bir daha karşısına çıkmayacak şekilde yok edilmesini ve yeni bir sayfa açmasını sağlamaktaır. Bu hak verilerin silinmesinin yanı sıra bir daha hatırlanmayacak şekilde veri sorumlusunda gerekli önlemlerin alınmasını isteme yetkisi de vermektedir. Kanunun amacı kişilerin özel hayatının gizliliğini temin etmektir ve gerekli önlemleri alınmasını sağlayarak kişiyi korumaktır. Kanunda yer almasına rağmen her somut olayda unutulma hakkı kendi içinde tekrar değerlendirileceğinden bu durumun mutlak bir hak olmadığı da unutulmamalıdır (Taştan, 2017).

1.1.12. Kişisel Sağlık Verilerinin Aktarılması

Kişisel Verilerin Korunması Kanunu 8. maddesinde açık rıza alınmaksızın hasta verilerinin aktarılamayacağını belirtmiştir. 6. maddenin 3. fıkrasında aktarılmaya ilişkin istisnalar getirilmiştir. Bu istisnalar şu şekildedir; "sağlık ve cinsel hayat dışındaki kişisel veriler, kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilir. Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî 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 (KVKK, 2016)."

Sağlık Bakanlığı sağlık hizmetlerini yürütebilmek için sağlık verilerini aktarma ve işleme yetkisine sahiptir. Bu yetki 10.07.2018 tarihinde Resmî Gazetede yayınlamış olan 1 sayılı Cumhurbaşkanlığı kararnamesinden alınmaktadır ve 378. maddede belirtilmektedir. Aktarımın amacı sağlık hizmetinin planlanması, kamu sağlığının korunması, hekimlik faaliyetleri, tıbbi teşhis, bakım ve tedavi gibi sıralanmıştır. Kanunda öngörülmeyen maddeler dışında sağlık verilerinin paylaşılamayacağı ya da aktarılamayacağı hükmü koyulmuştur (Alçın, 2022).

Kişisel verilerin korunması kavramının yaygınlaşması ile uluslararası antlaşma metinlerinde gizliliğe ilişkin maddeler de eklenmiştir. Kişisel veri kişinin özel hayatına ilişkin olmak zorunda olmadığından yurtdışına kişisel veri aktarımını özel hayatın gizliliği içerisinde değerlendirmek yanlış olacaktır. Kişisel veriler yurtdışına aktarılırken ilgili kişinin açık rızası aranmakta ya da özel antlaşmalar yapılması gerekmedir. Bu şartlar sağlanamıyorsa hukuka uygunluk denetimleri devreye girmektedir. Kişisel Verilerin Korunmasın Kanunu 9. maddede yurtdışına aktarılmaya ilişkin hüküm düzenlenmiştir. Veriler aktarılacağı ülkede veri sorumlusu tarafından mevzuat ve uygulanma kriterleri açısından alınacak önlemlerle gönderilecektir. Kanunda yeterli korumanın bulunduğu ve bulunmadığı ülkeler olarak ikili bir ayrım mevcuttur (Gür, 2018).

1.1.13. Meslek Etiği Olarak Susma

Sağlık çalışanlarının sır saklama yükümlüğü bulunmaktadır. Etik olarak sır saklama yükümlülüğünün kaynağı sadakat yükümlülüğündendir. Sır saklamaya Türk Borçlar Kanunu ile hukukî düzenleme getirilirken ihlâli halinde Türk Ceza Kanunu hükümleri uygulanmaktadır. Sağlıkta sır saklama, meslek sırrı olarak da açıklanabilmektedir. Meslek sırrı denildiği zaman akıllara hekimin sır saklama yükümlülüğü gelmektedir. Meslek sırrı mesleğin ifası sonucunda öğrenilen sırlardan oluşmaktadır. Hasta bir hekimle mesleğini yaparken kişisel bilgisini paylaşırsa o bilgi meslek sırrı olacaktır fakat aynı bilgiyi hastane dışında paylaşırsa meslek sırrı olmaktan çıkacaktır (Karadaş, 2019).

Hekim hasta ilişkisinde meslek gereği hastayla girilen münasebet sonucunda sır kapsamında şeyler öğrenilebilir. Sır kişinin dış dünyadan saklamak istediği gizli bilgilerdir. Bu sırlar hasta tarafından hekimle paylaşılabilir ya da hekim muayene esnasında kendisi veya ekibi fark edebilir. Böylece hekimin sır saklama yükümlülüğü hekimle birlikte sır saklama yükümlülüğüne dönüşerek beraber çalışılan hemşire, laborant gibi meslekleri de içine almaktadır. Hasta verilerinin sır olarak saklamanın istisnaları ise suç ihbarında bulunmak, bilirkişi raporunda bahsetmek, doğum raporu, bildirimi zorunlu hastalıklar, zaruret halleri, hastanın rızası, muayene ücretinin alınamaması halinde mahkemeye başvurma ve hekimin kendini savunması olarak sıralanabilir. Hasta hakları yönetmeliğine göre tıbbi zorunluluklar ve müsaade edilen haller dışında hastanın özel yaşamının gizliliğine ve aile yaşamının gizliliğine dokunulamaz hükmü getirmiştir. Hasta hakları yönetmeliği böylece sır saklama yükümlülüğüne vurgu yapmaktadır. Hastanın aile hayatına dokunulmamasına karşın hasta kendi sağlık verilerini ailesinden de saklamak isteyebilir. Burada hastanın mahremiyetine saygı göstermek gerekmektedir. İstisnalar dışında hastanın ailesine de bilgi verilmesi hukuka uygun olmayacaktır (Büyükay, 2004).

Hekimlik mesleğinin en önemli yükümlülüğü hastanın teşhis ve tedavisi iken bu hizmeti icra ederken bilgileri de saklama yükümlülüğü vardır. Avrupa İnsan Hakları Sözleşmesi 8. maddesinde de vurgulanan tıbbi verilerin korunmasına ilişkin hükümler sağlık kayıtlarının korunmasının temel prensip olduğundan bahsetmektedir. Sır saklama da iki şart bulunmaktadır. Birincisi objektif şarttır. Bu

unsur bir verinin sır olabilmesi için üçüncü kişiler tarafından bilinmemesi şartıdır. İkinci şart ise subjektif şarttır. Bu şart bir şeyin sır olarak kalması için veri öznesinin de iradesinin bu yönde olmasıdır. İrade beyanı ile subjektif şart oluşmaktadır. Sır saklama meslek ile doğrudan ilişkili olduğundan yükümlülüğün yerine getirilmemesi meslek suçu olarak sonuç doğurabilecektir (Özdemir, 2010).

1.1.14. Kişisel Verilerin Korunması Kanununa Yapılan Eleştiriler

6698 sayılı KVKK kişisel veri ve kişisel sağlık veriler için hukukî koruma sağlamaktadır. Ancak kanunla ilgili boşlukların olduğu ve kişisel sağlık verilerinin gerektiği gibi korunmasını sağlamak için düzenlemeler yapılması gerektiği bazı araştırmacılar tarafından dile getirilmiştir (Küçükbasmacı, 2022; Koç, 2021; Bayraktar, 2022). Küçükbasmacı 2022 yılında yaptığı çalışmasında Kişisel Verilerin Korunması Kanunu için Avukatlık Kanunu ve İş Kanunu ile çelişkili ifadeleri bulunması nedeniyle eleştiri getirmiştir. Koç, Kişisel Verilerin Korunması Kanununda 6. maddenin boşlukları olduğunu ve bu boşluğun ihlaller için ortam hazırladığını iddia etmiştir. Sağlık verilerinin gerektiği gibi korunmasının sağlanması için 6. madde için açık bir dille yapılan bir düzenleme yapılması önerisi ile gizliliği korunması gerektiği vurgulanmaktadır (Koç, 2021). Bayraktar (2022) ise kişisel verilerin korunması kanununda "yetkili kişiler ve işleme amaçları kısmına eleştiri" getirmiştir. Bu eleştiri; iki kavram için de sınırlılıklarının belli olmaması, belirsizlik ve geniş yorumlamaya müsait unsurları içermesi nedeniyle yapılmıştır. Bu hususlarda düzenleme önermiştir (Bayraktar, 2022).

Gözmener (2019) hukukî düzenlemeler konusunda gerçekleştirdiği çalışmasında, Anayasa, Tüzük, Kanun vb. hukukî metinlerinin dilinin ağır olduğunu; öğrenilmesinde ve anlaşılmasında sorunlar yaşandığı ifade etmiştir. Sağlık ve hukukun giderek iç içe geçtiği günümüzde sağlık personelinin rahatça okuyup anlayacağı metinlerin yürürlükte olmasını tavsiye etmiştir (Gözmener, 2019).

1.2. SAĞLIK KURUMLARINDA VERİ MAHREMİYETİ

Kişisel verilerin korunması modern hukuk dünyasında yeni incelenmeye başlanan bir kavram olsa da bu kaynağın mahremiyet kökeni daha eskilere dayanmaktadır. Hasta verilerinde mahremiyeti gözetmek Hipokrat ile ortaya çıkmaktadır (Karaaslan vd 2015). Hipokrat yemininde hasta verisi mahremiyeti açısından şu hususlara değinilmiştir: "Gerek sanatımın icrası sırasında gerekse insanlarla gündelik ilişkideyken edindiğim bilgileri ortalığa saçmayacağım, bir sır olarak saklayacağım ve kimseye açmayacağım". Hipokrat yemini tarihin en eski bağlayıcı metinlerinden birisidir. Modern tıbbın babası Hipokrat M.Ö. 5. yüzyılda yaşamasına rağmen yemin metni bir asır sonra ortaya çıkmıştır. Günümüzde Hipokrat yemininin orijinal metni olmasına rağmen güncellemeler ve eklemeler getirilmiştir (Tyson, 2001).

Mahremiyet; bireyin özgür ve bağımsız oluşunun ana unsurunu oluşturan bir kavramdır. 1890'larda Amerika'da bu hak, yalnız bırakılma hakkı olarak kullanılmıştır. Yalnız bırakılma hakkı özgür insanlardan tarafından en değer verileni yani mahremiyeti, yalnız bırakma hakkını içermektedir. Avrupa kıtasında ise mahremiyet hakkının geçmişteki resmi ilk örneklerine Alman nüfus sayımında denk gelinmiştir. Halk sorulara sınırı aştığı için cevap vermeyi reddetmiştir. Anayasa Mahkemesi bu durumu "bilginin geleceğine karar verme hakkı" olarak tanımlanmıştır (Dülger, 2015).

1947 tarihli 2. Cenevre Genel Kurulu'nda hastaya ilişkin tehlikeli durumlar ile hastanın bilgisi ve isteği dahilinde meslektaş ve diğer kişilerle hasta bilgilerinin paylaşılmasının hatta kullanılmasının etik sayılması gerektiği Dünya Tıp Örgütü tarafınca kabul edilmiştir (Uysal ve Yorulmaz, 2018). 20. Yüzyılın yarısından sonra özellikle 2. dünya savaşı sonrası insan hakları ve temel haklarda önemli gelişmeler olmaya başlamıştır. Teknolojinin de bu dönemden sonra daha hızlı gelişmesiyle gizlilik ve mahremiyetin daha ciddi korunması ihtiyacı ortaya çıkmıştır (Korkmaz, 2014).

Mahremiyet kavramının insanoğlunun var olduğu ilk günlerde ortaya çıktığı varsayılsa da güvenlik kavramları gibi net bir tanım yoktur. Uzlaşılmış bir tanımın olmamasının sebebi mahremiyetin zamansal, kültürel ve mekânsal çeşitliliklerden etkilenmesidir. Mahremiyet buna rağmen tek cümleyle "gizli olan ve gizli kalması

gereken şey" olarak tanımlanabilmektedir (Aslanyürek, 2016). Kişilerin mahremiyet sınırları kendisinin koymuş olduğu erişim engeli noktasında başlamaktadır. Bu nedenle mahremiyeti korurken kişinin koymuş olduğu sınırların bilincinde hem kişinin hem de diğer kişilerin bilinçli olması gerekmektedir. Mahremiyeti yalnızca fiziksel olarak nitelendirmeyip sosyal, bilgisel, mülkî, kararsal ve ilişkisel olarak da genişletilebilmektedir. Bu genişleme ile mahremiyet bilinci toplumsal, kültürel ve inanç değerindeki değişimler ile farklılık gösterebilmektedir (Öztürk, Özçelik ve Bahçecik, 2014).

Tüm dünyada yaşanan teknolojik gelişmelerle birlikte sağlık sektöründe de köklü değişimler yaşanmaktadır. Teknolojide yaşanan hızlı değişim göz ardı edilecek gibi değildir. Sağlık hizmetleri her alanda olduğu gibi teknolojik gelişmeleri kendisine göre uygulamalarına dahil etmektedir. Bu dahil olunmalar mahremiyet sorunu doğurmaktadır. Önlemler alınmazsa mahremiyetin korunmasında sorunlar çıkması muhtemeldir. Sağlık bilgilerin mahremiyetin en büyük sorunlarından birisi de hastaya ait verilere yetkisiz ulaşımdır. İlgili olmayan kişilerin verilere ulaşımı engellenirken veriyi kimler nasıl görecek ona ne şekilde erişecek ve buradaki sınırlar ne olmalıdır soruları sorulmalıdır. Aksi takdirde hastanın bilgilerinin ilgisiz kişiler tarafından ulaşılıp, paylaşılması ve kullanılması gibi hasta için olumsuz sonuçlar doğurabilecek durumlar yaşanmaktadır (İleri ve Uludağ, 2017).

Sağlık mesleği profesyonelleri meslekleri başlamadan önce meslekî yeminler etmektedir. Bu yeminler hastanın mahrem sayılan bilgilerinin başkalarına izinsiz açıklanmamasını da içermektedir. Özellikle bunu yenilenmiş Hipokrat yemininde de görebilmekteyiz. Bu yenilenmiş yeminde hekimlerin hasta haklarına karşı sorumlulukları hatırlatılmaktadır. Mahremiyete saygı duyulurken sır olarak saklanan bilgilerin hastanın izni dahilinde açıklanmasının da etik dışı olmayacağı belirtilmiştir. Aynı zamanda sağlık profesyonellerinin hastanın tedavisi ve kamu sağlığının korunması için hastaya ait verilerin paylaşılmasındaki sınırlandırılmaya da değinilmiştir. Türkiye'de sağlıkta mahremiyetin korunmasına ilişkin köklü değişiklikler 2003 yılındaki Sağlıkta Dönüşüm Programı (SDP) dahilinde yapılan çalışmalarla halâ sürdürülmektedir (Uysal ve Yorulmaz, 2018).

Mahremiyet sorunu birçok bilim dalını ilgilendiren bir konudur. Bu nedenle disiplinlerarası olarak nitelendirilmektedir. Sağlık bilimlerinde ise mahremiyetin

önemi daha çok hissedilmektedir, çünkü mahremiyet temel bir ihtiyaç olarak nitelendirilmektedir. Hastanın mahremiyeti denildiğinde akıllara ilk olarak bedensel olarak gizlilik gelse de bilgilerin gizliliğinin de mahremiyet kapsamına girdiği unutulmamalıdır. Mahremiyet sağlanırken hastanın mahremiyetinin sosyal, bilişsel, fiziksel ve psikolojik unsurları tek tek ele alınmalıdır (Özata ve Özer, 2017).

Fiziksel Mahremiyet: Bedensel mahremiyet olarak ele alınmaktadır. Bireyin çevresindeki alanı üzerindeki kontrolü ile ilgilidir. Bireylerle fiziksel teması da bu kapsamdadır. Bireyin vücudundaki gizli alanları ve evi, iş yeri gibi kontrol alanındaki yerleri de kapsayan egemenlik alanı fiziksel mahremiyete dahildir (T.C. Sağlık Bakanlığı, 2016).

Psikolojik Mahremiyet: Bireyin kendine ait değerlerini, inançlarını ve bireyi etkileyen unsurlar üzerindeki bilgilerini kontrol etmeyi, duygu ve düşünceleri kiminle ne şartla paylaşacağına karar verme hakkı veren bir olgudur. Bu mahremiyetin göz ardı edilmesin halinde kişilerde özgüven eksikliğinin yanı sıra sosyal izolasyon gibi sorunlarda ortaya çıkabilmektedir (Aktaş ve Baykara, 2020).

Bilişsel Mahremiyet: Bireyin kendi tarafınca açığa vurulmasını ve başkaları tarafından ulaşılmasını kontrol edebilmesidir (Öztürk vd, 2014). Yani bilişsel mahremiyet kişinin kendisine ait bilginin ne şekilde ne zaman ve dış dünyaya nasıl yansıtılacağına karar vermesidir. Ayrıca bilişsel mahremiyet bireyin kendi kontrolü altındaki her şey olarak da nitelendirilmektedir. Tıp dünyasında gizlilik her zaman çok önemli olduğundan dolayı korumak ve uygun ortam sağlamak çok önemlidir. Bilişsel gizlilik ile hastalara verilen hizmetin gelişmesi de sağlanabilmektedir. Hastaya, kendisine ait verilerin gizli ve güvende kalacağının garantisini vererek gelişime katkıda bulunabilir. Bilişsel mahremiyetin en büyük tehdit unsuru teknolojik gelişmelerdir. Verilere kimin nasıl erişeceğinin kontrolden çıkması büyük bir tehdit oluşturmaktadır (Orman, 2019).

Sosyal Mahremiyet: Bireyin sosyal ilişkilerini, ilişkinin taraflarını, sıklığını ve etkileşimini kontrol edebilmesidir. İnsanları sosyal mahremiyette hem bireysel hem de topluluk halinde değerlendirmek uygun olacaktır. Çünkü her kültürde mahremiyetin kapsamı ve önemi farklı tezahür edebilir. Özellikle bu doğu ve batı toplumları arasında ciddî farklılık göstermektedir. Sosyal mahremiyete insan onuruna

saygın da son derece önemlidir. Mahremiyete saygı göstermeme bir hak ihlâli olacaktır. Hatta bu fiziksel olarak bağımlı hastaların başka türlü zarar görmesine de neden olabilmektedir. Sağlık verileri ile sosyal mahremiyetin ilişkisi hastanın mahremiyet sağlanamamasında incinebilmesi, kırılmasını meydana getirmektedir (Özata ve Özer, 2017).

Mahrem bilgilere erişilmesi kişilerin stres ve kaygı düzeyini arttıracak derecede olgulardır. Araştırma sonuçları, sağlık hizmetini sunan kişilerin bu mahremiyet konusuna olumsuz yaklaşımı ve mahremiyete özen göstermemelerinin, hastaların anksiyetelerini ve stres şiddetinin artacağını işaret etmektedir (Akar vd., 2018). Hastanın mahremiyeti, özel yaşamın gizliliğinin bir başka boyutudur. Birey, birey olabilmek için özerkliğe ihtiyaç duymaktadır. Bu özerklik mahremiyet sağlanması ile mümkün olacaktır. Dolayısıyla özerklikle mahremiyet birbiriyle bağlantılıdır. Bu durum da özerlik ile mahremiyet kavramı birbirinin yerine kullanılabilir, bunlar sadece birbiriyle doğru orantılı durumlardır (Akar vd., 2019).

ABD'de 1996'da yürürlüğe giren Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (Health Insurance Portability and Accountability Act, HIPAA) ile, kişisel sağlık bilgilerinin kullanımına yönelik ulusal gizlilik ve güvenlik standartları oluşturulması ve korunan sağlık bilgilerini bilerek yasa dışı bir şekilde elde eden veya sahte beyanlarla veya ticari kazanç sağlama veya zarar verme niyetiyle ifşa eden kapsanan kuruluşlar için yetkili cezaî para cezaları ve hapis cezaları tanımlanmasını zorunlu hale getirmiştir. Ancak yürürlüğe girdiği dönemde ABD'de HIPAA, hastaların kuruluşlara doğrudan dava açmasına izin vermemiştir. 2009 yılında Ekonomik ve Klinik Sağlık İçin Sağlık Bilgi Teknolojisi Yasası (Health Information Technology for Economic and Clinical Health Act, HITE)'nın yürürlüğe girmesi ile sistemde değişiklikler yapılmıştır (Sarpatwari, Kesselheim, Malin, Gagne ve Schneeweiss, 2014).

Türkiye'de ise, 2016 yılında kabul edilen 6698 sayılı Kişisel Verilerin Korunması Kanunu ile kişisel verilerin işlenmesinde özel hayatın gizliliği, kişilerin temel hak ve özgürlükleri kapsamında teminat altına alınmıştır.

Mahremiyet Arapça kökenlidir ve haram kökünden oluşmaktadır. Türkçesi aslında dokunulmazlıktır. Hasta dokunulmazlığı mahremiyet olarak ele alınmaktadır.

Dokunulmazlıkta özel alan ve gizli alanlar bulunmaktadır. Mahremiyet bütünüyle gizlilikle ilgilidir. Bilgilerin gizliliği, beden ve zihinsel gizlilikler mahremiyet kapsamında değerlendirilmelidir. Hastanın mahremiyeti açıklamak zorunda kaldığı bilgilerin gizli kalmasını istediği yaşam alanı olarak tanımlanabilmektedir. Hasta mahremiyeti Hasta Hakları Yönetmeliği (HHY) ile mahremiyete saygı gösterilmesi başlığı altında ayrı olarak ele alınmaktadır (Gündüz ve Altıntaş, 2019). HHY 21 madde şöyle demektedir: *"Hastanın, mahremiyetine saygı gösterilmesi esastır. Hasta mahremiyetinin korunmasını açıkça talep de edebilir. Her türlü tıbbi müdahale hastanın mahremiyetine saygı gösterilmek suretiyle icra edilir.*

Mahremiyete saygı gösterilmesi ve bunu istemek hakkı;

a) Hastanın, sağlık durumu ile ilgili tıbbi değerlendirmelerin gizlilik içerisinde yürütülmesini,

b) Muayenenin, teşhisin, tedavinin ve hasta ile doğrudan teması gerektiren diğer işlemlerin makul bir gizlilik ortamında gerçekleştirilmesini,

c) Tıbben sakınca olmayan hallerde yanında bir yakınının bulunmasına izin verilmesini,

d) Tedavisi ile doğrudan ilgili olmayan kimselerin, tıbbi müdahale sırasında bulunmamasını,

e) Hastalığın mahiyeti gerektirmedikçe hastanın şahsi ve ailevi hayatına müdahale edilmemesini,

f) Sağlık harcamalarının kaynağının gizli tutulmasını, kapsar. Ölüm olayı, mahremiyetin bozulması hakkını vermez."

Hastaya ait bilgiler hasta ölse bile saklanır ve korunur. Hastanın sağlık durumu, tedavileri, kişiye özel her türlü bilgisi bunlardandır. Bu koruma usulüne uygun bir şekilde yapılmalıdır. Fakat hastanelerde bilgi mahremiyeti sağlanırken en büyük eksiliğin fiziksel koşullardaki hatalardan kaynaklandığı görülmüştür. Tüm bu belirlemeler hasta ve doktor arasındaki ilişkiyi şifrelemek ve teknolojinin getirdiği tehlikelerden korumayı sağlamaya yöneltmektedir. (Bayraklı ve Güvenoğlu, 2013).

Kamu hizmetlerinde ve tıp uzmanları arasında enfekte kişilerin verilerinin paylaşımı epidemiyolojik olarak fayda sağlamaktadır. Bulaşıcı hastalığın kontrolü sağlanırken,

bulaş riskini önlenmesi ve erken teşhis avantajı da sağlamaktadır. Covid-19 sürecinde Kore Cumhuriyetinde kişisel sağlık verilerin korunması için 2011 yılında imzalanan PIPA [Kore Cumhuriyeti Kişisel Veri Kanunu (Personal Information Protection Act)] yasasına rağmen paylaşımlar yapılmıştır. Bu yasa verilerin korunması için verilerin toplanması, ifşası ve paylaşılmasını açıkça yasaklamıştır. Fakat bulaşıcı hastalıkla mücadele için hasta verilerinin paylaşımı zorunluluk olarak gösterilmiş ve paylaşıma rağmen gizliliği koruyan yasalar getirilerek kişisel verilerin korunmasının devamlılığı sağlanmaya çalışılmıştır. Böylece hasta mahremiyeti ve kurumlar arası veri paylaşımın arasındaki dengenin gözetilmesinin önemi vurgulanmıştır (Sangchul, 2020).

Sağlık bilimlerinin her alanında tıp etiği önem arz etmektedir. Psikiyatri alanı bu konuda etik ikilemlerin en yoğun yaşandığı bilim dallarından birisidir. Kültüre göre farklılık göstermekle birlikte psikiyatri hastası bile olmak sorunken, bu hastalarda bilgilerin gizliliği sorunların başında gelmektedir. Çünkü hastalar gizliliğe dikkat edilmeyen toplum içerisinde etiketlenecek ve tecrit edilecektir. Bu etiketlenme sadece toplum üyeleri için değil sağlık personeli arasında bile gerçekleşmektedir. Etiketlenme geçmişe nazaran günümüzde daha az olmasına rağmen kaygı devam etmektedir. Etik eğitimi alan sağlık personelinin günümüzde eğitim aldıkları kurumlarda bu eğitimi aldığı görülürken yaşça büyük olanların kulaktan dolma bilgilerle etik değerlere dikkat etmeye çalışması görülmektedir. Bu yüzden damgalama, etiketleme gibi sorunlar tedavi önünde bir engel oluştururken tüm psikolojik süreci olumsuz etkileyen bir etik hata olarak ortaya çıkmaktadır (Gül, Kuzuca ve Arda, 2019).

Psikiyatrik bakımlarda gözlem hem tedavi edici hem de güvenli olmalıdır. Gözlem de en çok karşılaşılan etik sorun hastalık hakkında hastanın ailesine bilgi verilmesi sorunudur. Bu durum hastanın bireyselliğine yani otonomluğuna müdahalede bulunulması anlamına gelmektedir. Bazı uzmanlar hasta hakkında sözel bilgi vermenin etik dışı olduğu yapılan her şeyin yazılı olarak ifade edilmesini savunmuşlardır. Psikiyatride hastanın gözlem altında olması da otonomluk ve bireysellik açısından mahremiyeti zedelemektedir. Özellikle kameralı gözlem mahremiyet için risk oluştururken hastaların özkıyım girişimlerini önlemek için etkili bir yöntem olarak sayılabilmektedir. Bu bağlamda risk altındaki hastaların iyi

değerlendirilmesi ve önlemlerin her hasta için farklılık göstermesi gerekmektedir (Sabancıoğulları, Açıl ve Hallaç, 2014).

Ancak bazı durumlarda uluslararası düzeyde, yönergeler gizliliğin mutlak olmadığını iddia etmektedir ve sağlık uzmanlarına belirli koşullar altında gizliliği ihlâl etme "ayrıcalığı" vermektedir. (Godard vd., 2006). Birleşik Krallık Genel Tıp Konseyi Yönergeleri (General Medical Council. Confidentiality. General Medical Council: London, 2009) sağlık uzmanlarının, özellikle ifşanın yararı halkın çıkarına ağır bastığı durumlarda (örneğin bulaşıcı hastalıklar ya da genetik hastalıklar gibi) ve hastanın bilgilerinin gizli tutması ve ifşa edilmemesinin başkalarını ölüm veya ciddi zarar riskine sokması durumunda, hastanın açık rızası olmadan bilgi paylaşabileceğini belirtmektedir.

Türkiye'de ise kişisel sağlık verilerinin paylaşılmasında istisnai haller açıkça belirtilmiştir. Bu haller kişinin rızasına bakılmaksızın kişisel verinin kaydedilip aktarılmasına imkân sağlamaktadır. İstisnalar kısmı KVKK madde 3 ve madde 28'de düzenlenmektedir (KVKK.2016).

KVKK 3. maddesi *"Sağlık ve cinsel hayata ilişkin kişisel veriler ise ancak kamu sağlığının korunması, koruyucu hekimlik, tıbbî 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."* ve KVKK madde 28'deki *"Kişisel verilerin millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini veya ekonomik güvenliği sağlamaya yönelik olarak kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından yürütülen önleyici, koruyucu ve istihbari faaliyetler kapsamında işlenmesi."* hükümleri ile istisna oluşturan durumlar belirtmiştir.

İnternet erişimiyle sağlık bakım hizmetleri her yerde bulunan hizmetlere dönüşmüştür. Hastalığın tedavisi ve uzaktan erişim için yapay zekâ kullanılmaktadır. Geleceğin sağlık sistemleri yapay zekaya doğru evrilmektedir. Mahremiyet sorunu burada çıkmaktadır. Birçok alanda da olduğu gibi mahremiyetin korunmasını gerçekleştirmek için sızıntıyı önlemekle başlayacaktır. Bilginin dışarıya sızmasını engellemek için uzmanlar saldırı modellerini oluşturmaktadırlar. Kişiyi

tanımlayabilen algoritmalar bunun için çözüm olarak sunulabilmektedir. Sağlık kurumları işletmecileri kimin hangi verilere eriştiğini algoritmalar sayesinde fark edebilir duruma gelmiştir. Bu aslında bir önleme mekanizmasıdır (Ali, Naeem, Tarıq ve Kaddoum, 2022).

1.2.11. Sağlıkta Mahremiyet ve Veri Koruması İçin Uluslararası Uygulamalar

Sağlık hizmetleri için 3. milenyum hızlı değişimlerle başlamıştır ve bu değişim sürmektedir. Teknolojinin ve dijitalleşmenin hızlı yükselişi sağlık verilerinin dijital ortamlarda saklanabilmesini ve kullanılabilmesini sağlamıştır. Maalesef bu durum farklı zararlı kullanımlara da kapılar açmıştır. Örneğin sağlık ekonomisi alanındaki firmalar arasındaki rekabet, onları bireylerin yasal yollardan elde edilemeyen sağlık verilerini yasal olmayan yollardan elde etmeye yöneltmiştir. Her geçen gün yapılan AR-GE (Araştırma-Geliştirme) çalışması sayısı artmakta ve bu çalışmalar için güncel hasa verilerine ihtiyaç duyulmaktadır. Son yıllarda yapılan çalışmalar medikal hırsızlığa meyilin arttığını göstermektedir. Bu tür hırsızlıkların önüne ancak alt yapı iyileştirmesi yapılarak geçilebilmektedir ve gerekli çalışmalara önem verilmelidir (Ağıralan, 2015).

Sağlık işletmelerinde bilgi güvenliğinin sağlanması temel bir faktördür. Bu nedenle sağlık yönetiminde bilgi güvenliğinde entegrasyon, senkronizasyon odaklı anlayış ön plana çıkmalıdır. Sağlık yönetimi insan kaynakları, yönetim ve bilgi güvenliğinin denetlenmesi faaliyetlerini kapsamaktadır. Güvenlik önlemlerini alan kurum maliyet tasarrufu ve verimlilik konularında da çağdaş sağlık modellerine ulaşma fırsatını yakalayacaktır (Marşap, Akalp ve Yeniman, 2010).

Bir kişinin mahremiyet ihlalinden dolayı zarar görmemiş olması, haksızlığa uğramadığı anlamına gelmemelidir. Kişi belki bu ihlali asla öğrenemeyebilir. Verileri inceleyen kişiler yurtdışında yaşıyor ve zarara uğrayanın zarar vereni görme ihtimali de olmayabilir. Böylesi bir sonuçta görünür bir zarardan bahsetmek zordur fakat verilerde olan kontrol kaybının başta etik değerler olmak üzere birçok yönden zararı dokunmaktadır. Sağlık verileri de bu şekilde ihlallere maruz kalabilir (Price ve Cohen, 2019).

Hasta hakları bireyleri sırf bir insan oldukları için uluslararası antlaşmalar, anayasa ve kanunlarla korumaya almıştır. Hasta hakları, kurumlara ve personele karşı

hastanın haklarını ifade etmektedir. Hasta hakları Türkiye'de yalnızca ölüm ve sakatlanma durumlarında varmış gibi görülse de insan olarak saygı görme ve güvenlik hasta haklarının temelidir. Mahremiyet, özel hayata saygı, tıbbi araştırmalara için hasta verilerinin kullanımı da hasta haklarının konusudur. Bu hususlar göz önünde bulundurulur ise sağlık hizmetinin sunucuları, hastalarla ilgili ortaya çıkan gereksinimlere cevap vermenin kolaylıklarına ulaşmış olacaklardır. Tıp etiğinin de çalışma konusu olan bu haklar tüm sağlık personeline önemli görev ve sorumluluklar yüklemektedir (Kılıçarslan, Yılmaz ve Tarım, 2012).

Genel olarak, kullanıcıların sağlık durumları ile ilgili her türlü veri sağlık verisi olarak görülebilir. En önemli sağlık verileri klinik verilerdir, özellikle farklı düzeylerdeki hastaneler tarafından üretilen elektronik tıbbi kayıtlardır. Sağlık bilgi teknolojisinin gelişmesi ve giyilebilir sağlık cihazlarının yaygınlaşmasıyla birlikte, izlenen fizyolojik veriler ve diyet veya egzersiz verileri gibi sağlıkla ilgili çok miktarda veri, başka yerlerden hem pasif hem de aktif olarak kişilerden ve kuruluşlardan toplanmaktadır. Bir hastanın tıbbi kaydı; kimlik bilgileri, tıbbi teşhis geçmişi, dijital tıbbi görüntüler, uygulanan tedaviler, beslenme alışkanlıkları, cinsel tercihler, genetik bilgiler, psikolojik profiller ve zihinsel durum, çalışma geçmişi, gelir ve doktorun öznel kişilik değerlendirmeleri dahil olmak üzere birey hakkında önemli kişisel bilgileri içermektedir (Ong ve Sabapathy, 2020). Sağlıkla ilgili veriler; sağlık sistemi tarafından üretilen sağlık verileri ve tüketici sağlığı verileri olmak üzere iki ana başlık altında ele alınabilir (Xiang ve Cai, 2021).

Sağlık sistemi tarafından üretilen sağlık verileri klinik verilerdir ve hasta bir hastanede veya klinikte sağlık hizmeti aldığında ilgili veriler klinik uzmanları veya tıbbi cihazlar tarafından kaydedilir. Klinik veriler arasında elektronik sağlık kayıtları, reçeteler, laboratuvar verileri, patoloji görüntüleri, radyografi ve ödeme yapan kişi talepleri verileri yer alır. Tedavi gereksinimi için hastaların geçmiş durumu ve mevcut durumu kaydedilir. Hastalara daha iyi sağlık hizmeti sunabilmek için hastaların yaşam boyu klinik verilerinin takip edilmesi ve farklı sağlık hizmeti sunucuları arasında klinik veri paylaşımının yapılması önemlidir. Bu tür sağlık verileri, bu verilerin bakımın analiz edilmesi ve iyileştirilmesi amacıyla kullanılması amacıyla sağlık hizmeti sürecinde rutin olarak oluşturulur ve toplanır. Klinik tedavi amacıyla ve ayrıca tüketicilerin sağlık uzmanlarına ve kurumlarına olan kesin

güvenleri nedeniyle, klinik veriler yüksek derecede sağlıkla ilgili mahremiyet içerir. Bu nedenle, sağlık mahremiyeti yasalarının çoğu, esas olarak klinik verilerin mahremiyetinin korunmasını kapsar (McGraw ve Mandl, 2021).

Tüketici sağlığı verileri ise klinik verilerin önemli bir tamamlayıcısıdır. Tüketicilerin sağlık tutumları pasif tedaviden aktif sağlığa doğru; IoT, e-Sağlık, akıllı telefon ve giyilebilir cihaz gibi yeni nesil bilgi teknolojilerinin yaygın olarak uygulanmasıyla büyük ölçüde değişmiştir. Tüketicilerin sağlık verileri, giyilebilir kondisyon izleme cihazları, insülin pompaları ve kalp pilleri gibi tıbbi giyilebilir cihazlar, tıbbi veya sağlık izleme uygulamaları ve çevrimiçi sağlık hizmeti aracılığıyla üretilmeye başlanmıştır. Bu sağlık verileri arasında nefes, kalp atış hızı, kan basıncı, kan şekeri, yürüyüş, kilo, diyet tercihi, pozisyon ve çevrimiçi sağlık danışmanlığı yer alabilir. Bu ürünler veya hizmetler ve sağlık verileri, özellikle kronik hastalığı olan hastalar için tüketicilerin günlük sağlık yönetiminde önemli bir rol oynamaktadır (Xiang ve Cai, 2021).

Tıbbi kayıtlar, sağlık hizmetlerinde en önemli iletişim araçlarından biridir. Elektronik tıbbi kayıtların amacı, sağlık kayıtlarının yetkili kişiler arasında erişilebilirliğini ve paylaşımını artırmaktır. Elektronik sağlık kaydı sistemleri, sağlık bakım sistemlerini çoğunlukla kâğıt tabanlı bir endüstriden, sağlayıcıların hastalarına daha yüksek kalitede bakım sunmalarına olanak veren, hastalarla ilgili klinik ve klinik olmayan bilgileri kullanan bir endüstriye dönüştürme potansiyeline sahiptir (Menachemi ve Collum, 2011). Ancak sağlık hizmeti süreçleri sırasında toplanan bilgilerin gizliliğini sağlamak, kişisel sağlık bilgileri ifşa edildiğinde bireylere gelebilecek önemli ekonomik, psikolojik ve sosyal zararlar nedeniyle gereklidir.

Sağlık hizmetlerinde mahremiyet ve gizlilik sağlık hizmeti sunucusu ile hasta arasındaki ilişki, yakınlık ve güven ile karakterize edilen bir ilişkidir ve gizlilik, hasta-sağlayıcı etkileşimlerinde mutlak olarak yer alır. Aslında gizlilik, bilgilerin bu ilişkiler içinde nasıl paylaşılacağını yöneten kurallarla ilgilidir. Bu nedenle gizlilik, mahremiyeti korumak için bir araç veya özel konuların ifşasını sınırlayan bir eylem olarak tanımlanır. Sağlık bakımı bağlamında amaç, bireysel sağlık bilgilerinin yalnızca amaçlanan amaç için kullanılmasını ve herhangi bir ifşa için hastanın onayının alınmasını sağlamaktır. Bu nedenle, sağlık çalışanı-hasta ilişkisinde gizliliği korumanın anahtarı, bilgilere yalnızca yetkili kişilerin erişebildiğinden emin olmaktır

(Ong ve Sabapathy, 2020).

Sağlık hizmetlerinde bilgi güvenliğinin amaçları basitçe şu şekilde ifade edilebilir (Barrows ve Clayton, 1996);

- Hastaların mahremiyetinin ve sağlık hizmeti verilerinin gizliliğinin sağlanması (bilgilerin izinsiz ifşasının önlenmesi)
- Sağlık hizmeti verilerinin bütünlüğünü sağlamak (bilgilerin izinsiz değiştirilmesini önlemek)
- Yetkili kişiler için sağlık verilerinin mevcudiyetini sağlamak (bilgi veya kaynakların yetkisiz veya kasıtsız olarak saklanmasının önlenmesi).

Birçok ülkede verilerin güvenliği ve korunması adına ciddi çabalar gösterilmektedir. Örneğin Almanya'da veri koruması için kriptografi konusunda özel çalışmalar yürütülmektedir. Kriptografi bilgisayar bilimi ve teknoloji ile uğraşanların alanıdır. Teknoloji olmadan yaşanılmayacak bu dönemde sistemleri daha güvenli hale getirmek için kriptografi biliminden yararlanılabilir. Gizlilik sorununun arttığı, veri hırsızlığı çoğaldığı bir dönemde kişisel verileri depolayan ve işleyen sistemlere güvenin sağlaması iç. Veri uzmanları ile yapılan görüşmede uzmanlar öncelikle kişileri tehlikenin farkında olmalarını sağlanmasının büyük bir adım olduğunu ifade etmektedir (Mannhardt, Koschmider, Baracaldo, Weidlich ve Michael, 2019).

Tıbbi kayıtlar doğal afetler ve fiziki tehditlere karşı mutlaka elektronik ortamda saklanmalıdır. Elektronik sağlık kayıtları kişiye özel kayıtlardır ve yalnızca yetkili kullanıma izin verilmiş olmalıdır. Farklı yerlerden erişimin mümkün olduğu sağlık kayıtları ise günümüzde yeni popüler olarak "blockchain" yani "zincir tabanlı güvenlik kontrolü" ile sağlanmalıdır. Blockchain sistemi kriptografi üzerine kuruludur. İnsan müdahalesi olmadan bile güvenliği sağlayabilen zincirleme yöntemler geleceğin kripto yöntemidir. En çok da günümüzde korumayı sağlık kadar çok hak eden para sistemleri kullanmaktadır (Sharma ve Balamurugan, 2020).

Elektronik sağlık kayıtlarının güvenliği ve korunması konusunda köklü değişimler yaşanan bir diğer ülke ise Hindistan'dır. Hindistan'da elektronik sağlık kayıtlarının korunması için 2000 yılından itibaren pek çok değişim gerçekleştirilmeye başlanmıştır. Değişimlerin kılavuzu olan yasa aslında Amerika'dan ithal edilen

Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasasıdır (Health Insurance Portability and Accountability Act [HIPAA]). Ayrıca Hindistan hükümeti sağlığın bilgisayar ortamındaki kayıtlara geçmesini desteklemiştir. Bu da kayıtlar için gerekli olan sektörün büyüyüp gelişmesini sağlamıştır. Bu destekteki amaç sağlık hizmetleri sunucularının hasta bilgilerine zamanında, eksiksiz, yeterli ve doğru zamanda ulaşmasını sağlamaktır. Verilerin güvenliğini sağlamak da bulut tabanlı sistemlerle gerçekleştirilmiştir. Etik standartlara uyum sağlamayı hedefleyen bu teknolojik sistem koruyucu, iyileştirici ve rehabilite edici tüm kurumlarda yani sağlığın her seviyesin kullanmaya imkân sağlarken, güvenli ve mahremiyet tabanlı etik bir sistem haline gelmiştir (Pai, Ganiga, Pai ve Sinha, 2021).

HIPAA zorunluluğunun getirdiği iyilik sağlığı iyileştirme ve sunumu optimize etmektir. Bir standart oluşturmak hedeflenmiştir ve başarılı olunmuştur. Hastaların ve çıkarlarının korunmasının yanında kurumlarında korunduğu akıl bir yaklaşım haline gelmiştir. Bilgileri devretme, silme, koruma tıp hizmetleri dijital hale geldikçe önem gösterilecek konular arasında yerini almıştır. Bu kavramları bulundurduğu hükümlerle güçlendiren HIPAA yasasıdır (Mandl ve Perakslis, 2021)

Keshta ve Odeh'in tarafından gerçekleştirilen bir araştırmada Amerika Birleşik Devletleri'nde sağlık kuruluşlarının %68'i yakın zamanda önemli güvenlik sorunları yaşadığını Sağlık Hizmetleri Bilgi Yönetim Sistemi Topluluğu'na bildirmiştir. Bildirilmeyen olayların da olduğu var sayılırsa bu oran artacaktır. Bildirilen olaylar incelendiğinde ise; kurum içinde daha çok olmak üzere kurum dışı ihlâllerin de olduğu fark edilmiştir. Kurum içindeki ihlâller, sağlık verilerine erişmek için geçerli ve yeterli sebebi olan çalışanların sahip olduğu yetkiyle yapmış olduğu ihlâli içeren erişimlerdir (Keshta ve Odeh, 2021).

Carroll ve Frakt ise, sağlık ekonomisinin Amerika için çok büyük bir ekonomi olması ve çok büyük çıkar gruplarını içinde barınması nedeniyle, hizmet sunumunda ciddi değişikliklere gidilmesi gerektiğini vurgulanmıştır. Amerika Birleşik Devletleri bazında bakıldığında sağlık harcamalarının tüm dünya ülkelerinden daha fazla bir artış gösterdiği görülmektedir. Artan maliyetler kalitenin korunması ve artırılması gerektiğini işaret etmektedir. Kaliteyi artırmak için maliyet verimliliğinin yanında eşi benzeri görülmemiş sağlık sistemleri oluşturarak, veri sistemlerinin güvenliğini ve erişimini de güçlendirmek gerekmektedir. Elektronik tıbbi kayıtların teşvik edilmesi

kalite için her zaman teşvik edilmiştir. Kalite isteniyorsa eğer bahsedilen değişimin yapılmasının artık bir zorunluluk olduğu ifade edilmektedir (Frakt ve Carroll, 2013).

Kurumlar hastaların sağlık verilerini korumakla yükümlüdür. Bu yükümlülük bir takım kimlik doğrulama yöntemleri ve önlemleri almayı gerektirmektedir. Bu gereklilikler yasalardan ve tıp etiğinden kaynaklanmaktadır. 1996 tarihli Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası sağlık hizmetleri sunucuları arasında mahremiyet kültürünü teşvik etmiştir (Terry, 2013). 2001 yılında itibaren ise HIPAA, Tıp Enstitüsü ile hastaların sağlık bilgileri üzerinde daha fazla kontrole sahip olunması gerektiğini vurgulamıştır. Sağlık sisteminin hastaların elektronik sağlık kayıtlarına güvenli, web tabanlı bir portal olan Patient Gateway aracılığıyla erişmesini sağlamaya yönelik yaklaşıma karar vermişlerdir. Patient Gateaway sistemi güvenliği ve gizliliği korurken elektronik sağlık kayıtlarına erişim için prosedürleri içinde barındırmaktadır. Yetkilendirme ve şifrelendirme odaklıdır. Herhangi bir hastanın bilgisine erişmeden önce kimlik doğrulama devreye girmektedir. Ayrıca kullanıcılar bilgiye ulaşamadan önce Patient Gateaway kullanım sözleşmesini ve gizlilik politikasını okuyup kabul ettiğini beyan etmek zorundadır. Fakat internet ortamı her zaman birtakım verilere erişmek güvenlik sorunlarını beraberinde getirmektedir. Patient Gateaway sistemi güvenlik önlemi almak uğruna giriş yapması gereken kişileri sisteme kabul etmediği de olmuştur. Yaşanan sorunlara rağmen HIPAA kapsamında güvenlik düzeyi olağanüstü bir uygulama olmuştur (Wang vd., 2004).

1.2.12. Elektronik Sağlık Kayıtları

Elektronik Sağlık Kayıtları, sağlık sistemlerinde bilginin depolanması, değişimi ve yönetilmesi için önemli rol oynamaktadır. Kurumlar hastalara ait bilgileri son derece korunaklı tutmak zorundadır fakat bilgiye ihtiyacı olduğu zaman erişmek isteyen sağlık personelini de en kısa sürede bilgiye erişimini sağlamalıdır. Erişilebilirlik sağlık meslekleri için önemlidir. Elektronik sağlık kayıtlarının bilgi depolama haricinde yönetimi, süreçleri yürüme, karar verme, raporlama gibi süreçlere de katkısı bulunmaktadır. Elektronik sağlık sisteminin bütünlüğünün bozulması durumunda istenmeyen sonuçlar meydana gelebilmektedir. Bu sistemlerde yetki faktörü önemlidir. Yetkisiz giriş çıkışların önlenmiş olması ve yetkisi olanlarında bilgiye ulaşmasının kolaylığı sağlanmalıdır (Turaç, 2022).

Elektronik hasta kayıtları sistematik hasta bilgisi koleksiyonudur. Karar vermede yardımcı olmaktadır ve bilgileri güncel tutmayı sağlamaktadır. Elektronik sağlık kayıtları kullanıp başarısız olan kurumlar da var olabilmektedir. Kullanıcıları elektronik sağlık kayıtları hakkında bilgilendirmek, sistem konusunda eğitmek, kayıtların sisteme faydalarını göstermek ve kayıtları güncel tutabilmek bu tür kurumlarda uygulanması gereken strateji olmalıdır. Bu şekildeki stratejiler sağlık personelinin elektronik sağlık kayıtlarına olan direncini kırıp, sistemin optimum şekilde kullanılmasını sağlayacaktır (Campanella, Lovato, Marone, Fallacara, Mancuso, Ricciardi ve Specchia, 2016).

Tıbbi kayıtlar fiziki olarak tutulsa da elektronik olarak tutulup arşivlere kaydedilmektedir. Yetkili kişilerin erişimi mahremiyet sağlanması açısından önem arz etmektedir. Bilgi sistemleri; verilerin işlendiği, bilgilerin aktarıldığı, akışın sağlandığı karar vericilerin ihtiyaçlarını karşılamak için kurulmuş birbiriyle ilişkin sistemlerden oluşmaktadır. Bu sistemler ile araştırma ve denetim faliyetleri dahilinde veriler her an erişilip kullanılmak üzere hazırdır. Verilerin elektronik ortamda tutulmasıyla sistemlere ciddi yatırımlar yapılmaktadır. Hasta mahremiyetinin sağlanmasında hasta bilgilerinin önemi tartışılmaz boyuttadır. Meslek profesyoneli tüm bilimlerden aldığı verileri mesleğini yaparken kullanırken diğer profesyonellerin de faydalanması için elektronik sağlık kayıt sistemine kaydeder (Atalay, 2021).

Elektronik sağlık kayıtları büyük ölçekli bilgileri içinde bulundurur. İçinde bulundurduğu nitelikli bilgilerden dolayı elektronik sağlık kayıtları nitelikli kullanıcılara ihtiyaç duymaktadır. Sağlık personeli ya da başka personel bu sistemi kullanacaksa eğer yönetim bu sistemi yetkin kişilere bırakmalıdır. Kullanıcı bireylerin hukukî olarak çalışmaları ele alırken etik değerleri de göz önünde bulundurması istenmektedir. Ciddiyetsizlik ve sorumsuzluk telafisi mümkün olmayan hataların yapılmasına neden olabilir. Çünkü bilgi güvenliği sağlanırken bir zincir oluşur ve bu zincirin en zayıf ve kırılgan halkası insan faktöründen oluşur. Çalışanların elektronik sağlık kayıtlarını kullanırken bilgi güvenliği kültüründen haberdar olması gerekir (Çelikçöp ve Yarar, 2019).

Elektronik hasta kayıtlarının yönetimi pahalıdır. Dijital olarak yetersiz kurumlar bu maliyeti karşılayamayabilirler. Kurumlar bu çalışmalara katılım sağlayamamış da olabilir. Elektronik veri yönetiminin standardı olmalıdır. Tam olarak dijitalleşemeyen

kurumlarda bile kesin ve caydırıcı bir veri koruması düzenlemesine gidilmesi gerekliliktir (Kaissis vd., 2020).

1.2.13. Hastane Bilgi Yönetimi Sistemi (HBYS)

Hastaneler topluma sağlık hizmeti sunarken karmaşık iletişim ağına sahip sağlık sistemleri kullanırlar. Hastanelerde nitelikli işgücü görev aldığı için HBYS kullanımı da zorunlu hale gelmiştir. HBYS ile hastaneler hastalar ile ilgili tüm verileri sisteme kaydeder. Kayıt yapan kişiler sağlık profesyonelleridir. HBYS özel sektör ya da kamu ayrımı gözetilmeksizin her türlü sağlık kurumunda kullanılabilmektedir. HBYS sistemlerinde hastanın tedavi ve bakım süreçlerini kolaylaştırmak için modüller bulunmaktadır. Klinik süreçlerin ve denetim süreçlerinin tamamlanması için modüller önemli rol oynamaktadır (Özaslan, 2019).

Yapılan çalışmalarla görülmektedir ki sağlık sektöründe kişilerarası ilişki son derece yoğun yaşanmaktadır. Tedavi ve bakım süreçlerinde hasta ile en çok iletişim halinde olan meslek gruplarının başında hemşireler ve ebeler gelmektedir. Hemşirelik mesleğinin eğitim sürecinde ilk öğretilen ilkenin hasta mahremiyeti olması da tesadüf değildir. Hasta mahremiyetinin sağlanması hukuk alanının konusu iken, hasta memnuniyeti ile ekonomik iyileşme de sağlanmaktadır. Çünkü memnuniyet temel kalite göstergelerinden birisidir (Candan ve Bilgili, 2018).

1.2.14. Bilgi Güvenliği

Günümüz dünyasında elektronik ortamdaki veriler kişiler için bir tehdittir ve bu verilerin izinsiz kullanımı artık insanoğlunun yeni korkusu haline gelmiştir. Çünkü günümüzde bilginin irade dışı kullanımı yoğunlaşmıştır. Bu nedenden dolayı bilgi güvenliği günümüzde korunması gereken bir değer olmuştur (Koçak ve Memiş, 2018).

Bilgi güvenliği teknolojinin artmasıyla değer kazanan bir konudur. Bilginin doğru kullanılması, kesintisiz erişimi ve risk faktörlerinin önlenmesi konuları bilgi güvenliğinin kapsamındadır. Özellikle sağlık kurumlarında elektronik sağlık kayıtlarının kullanımının yaygınlaşmasıyla her alanda bilgi güvenliğine ihtiyaç duyulmaktadır. Her kurum kendisine uygun bir bilgi güvenliği politikası geliştirmek zorundadır. Bu politikalarla birlikte erişimde sınırlılıkların bilinmesi, faaliyetlerin sorgulanması ve yöntemlerin belirlenmesi mümkün hale gelecektir. Temel amaç ise

dört tanedir ve aşağıdaki gibidir (Baran ve Şener, 2019);

- Veri bütünlüğünün korunması,
- Yetkisiz erişimin engellenmesi,
- Mahremiyet ve gizliliğin korunması,
- Sistemin devamlılığının sağlanmasıdır.

Bilgi güvenliğini sağlamak üzere tarihte pek çok yönteme başvurulmuştur. Güvenlik insanoğlu ile yakın ilişkili bir kavramdır ve eskiden beridir var olmuştur. Günümüzde ise bilgi güvenliği birçok alt başlıkla kategorize ederek incelemek uygulama kolaylığı sağlamaktadır. Bunlar fiziksel ve çevresel önlemler, iletişim güvenliği, bilgisayar güvenliği, ağ güvenliği, güvenlik duvarı önlemleri, saldırı önleme olarak verilebilir (Gülmüş, 2010).

Sağlıkta ise son 20 yılda ciddi değişimler yaşanarak bilgi güvenliği sorunu ortaya çıkmıştır. Bu nedenle bilgi güvenliği dönüşümünden de en çok nasibini alan sağlık kurumları olmuştur. Sağlık sistemlerinin birbiri ile uyumu için standardizasyona ihtiyacı vardır. Bilgi sistemlerinin çalışanlar tarafından da kabul görmesi uyumu yakalamak da çok önemlidir. Hastanelerde bilgi sistemlerinin yoğun olarak kullanılmasına rağmen yapılan çalışma sayısı oldukça azdır. Göktaş ve arkadaşlarının 2017 yılına yapmış olduğu çalışmada Türkiye'nin dünya sıralamasında sağlık bilişimini en başarılı olduğu ülkeler arasında olduğunu fakat kurumların hızı yakalamakta sıkıntı çektiğini tespit edilmiştir. Maliyetlerin de fazla olması bilişim açısından sistemleri zorlamaktadır (Göktaş vd., 2017).

Hasta güvenliği sağlık hizmetlerinde sunuma bağlı hataların önlenmesi ve hataların neden olduğu hasarın ortadan kaldırılmasını hedeflemektedir. Hasta güvenliği hastanenin kalitesini gösteren bir göstergedir. Sağlık kurumları kaliteyi üst seviyede tutmak için hasta ile ilgili her türlü güvenlik önlemlerini almak durumundadır. Hasta güvenliğinin içeriğinde hastalara ait bilgilerin güvenliği de vardır. Bilgi güvenliği verilerin ihtiyaç duyulduğu an kullanıma hazır, güncel, güvenilir ve doğru şekilde tutulmasıyla gerçekleşmektedir (Eriş, Havlioğlu ve Doni, 2017).

1.2.15. Sağlık Kurumlarında Bilgi Güvenliğinin Amacı

Bilgi güvenliğinin 3 tane temel hedefi vardır. Bunlar; kullanılabilirlik, gizlilik ve

bütünlüktür. Bu hedefler bilgi güvenliğinin uygulama alanını oldukça genişletmektedir. Bilgi birçok farklı formatta bulunabilir ve farklı yöntemlerle iletilebilir. Bu çeşitlilik dolayısıyla bilginin yalnızca çok yüksek korumayla saklanması anlaşılmamalıdır. Kurum bazı bilgileri kimsenin ulaşamayacağı şekilde de saklayabilir ama hasta kayıtlarının tamamen ulaşılmaz bir şekilde saklanılması da hedeflenmez. Kullanıma hazır bir şekil bilginin güvenle saklanması temel hedeftir. Özellikle sağlık hizmetleri çok yoğun bir enformasyon süreci içermektedir. Dolayısıyla bu bilgiler bir şekilde belgelendirilmeyi ve saklanmayı gerektirmektedir (Çiftlik vd., 2013).

Sağlık hizmetlerinde gizlilik ve mahremiyet hizmet sunucusuyla hasta arasında kurulan güven ve samimiyetten doğan bir ilişki olmalıdır. Sağlık hizmetlerinde mahremiyet üçüncü aracı kurumlar, yönetilen bakım hizmetleri ve diğer sağlık hizmeti organizasyonlarından dolayı erozyona uğrayan bir değerdir. Davis'in 1995 yılında yaptığı araştırmaya göre her üç sağlık profesyonelinden birinin çok sık olmasa da verileri yetkisiz kişilerle paylaştığını ortaya koymuştur. Mahremiyet için net bir politika belirlenememesinin nedenini mahremiyetin tam anlaşılmamasının sebebinin de mahremiyetin her kesim tarafından farklı anlaşıldığını savunmuştur. Mahremiyet aslında bakana göredir. Birisinin değerlendirdiği algılanan mahremiyet şiddeti diğeri büyük bir ihlal olarak görünebilir. Fakat sağlık hizmetlerinin kalitesinin geliştirilmesi ve toplumun güvenini sağlamak için gizliliğin korunması gerekmektedir. Bu gizlilik optimum hasta tedavisi, tıbbi araştırmalar ve halk sağlığı için genişletilebilmelidir (Barrow ve Clayton, 1996).

Hizmet Kalitesi: Sağlık hizmetlerinin kalitesi pek çok göstergenin bir arada değerlendirilmesiyle ölçülmelidir. Hizmet kalitesinde müşteri ve çalışan memnuniyetinin önemi her zaman vurgulanmıştır. Fakat sağlık sektöründe kalite ölçümü imalat sektörü kadar kolay olmamaktadır. Makro ve mikro perspektiflerde değerlendirildiği zaman kalitenin artışını etkileyen faktörlerin arasında bilgilendirme, güvence, gizlilik yer almaktadır. Güven ve gizlilik ile ilgili yapılan çalışmalarda hastaların bu iki faktöre olumlu yanıt vermelerinin kalitenin artışıyla orantılı olduğu görülmüştür (Zaim ve Tarım, 2010). Modern teknoloji ile kişisel sağlık bilgilerinde gizlilik, bütünlük ve erişilebilirlik sorunları artmaktadır. Bu risklerin belirlenmesi ve yok edilmesi artık bir zorunluluktur. Bu risklerin ortadan kalkması için çalışanların

aynı bilgi kültürüne sahip olması önemlidir. Kültürün var olup olmamasının da kurum içinde ölçülmüş olması gereklidir (Karadağ ve Abuhanoğu, 2015).

2. GEREÇ ve YÖNTEM

Bu bölümde araştırmanın amacı, evren ve örneklemi, veri toplama araçları, çalışmanın sınırlılıkları, varsayımlar ve hipotezleri ilgili başlıklar altında ele alınmış ve açıklanmıştır.

2.1. Araştırmanın Amacı

Bu araştırma sağlık çalışanlarının 6698 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında var olan hukukî sorumluluklarına ilişkin bilgi düzeylerini değerlendirmek, hastalara ait elektronik sağlık kayıtlarının güvenlik ve mahremiyeti konusundaki standartlara uyum düzeylerini incelemek, sağlık çalışanlarının bu konudaki hukukî sorumluluklarına ilişkin bilgi düzeyleri ve elektronik sağlık kayıtlarının güvenlik ve mahremiyeti konusundaki standartlara uyum düzeylerinin birbiriyle ilişkisini ortaya koymak amacıyla tasarlanmış, tanımlayıcı kesitsel nitelikte bir araştırmadır.

2.2. Araştırmanın Evreni ve Örneklemi

Araştırmanın evrenini Kırıkkale ilinde bulunan 700 yataklı bir kamu hastanesinde görev yapan ve hasta bilgilerine ulaşma yetkisi olan sağlık çalışanları (hekim, ebe-hemşire, sağlık teknikerleri ve teknisyenleri, diğer sağlık meslekleri (Eczacı, Fizyoterapist, Biyolog vb.) ve tıbbi sekreterler oluşturmaktadır. Araştırma öncesi ilgili hastanenin personel biriminden elde edilen ve araştırma evrenini oluşturan güncel sağlık çalışanı sayısı toplamda 1126 kişidir (01.06.2022). Araştırma için örneklem büyüklüğü evreni bilinen örneklem hesaplama formülü (Özdamar, 2003) ile hesaplanmıştır. Kullanılan formül aşağıda verilmiştir.

Örneklem Formülü:

$$n = \frac{Nt^2pq}{d^2(N-1) + t^2pq}$$

N: Evrendeki Birey Sayısı.

n: Örnekleme alınacak birey sayısı

p: İncelenecek olayın görülme sıklığı

q: İncelenecek olayın görülmeme sıklığı

t: Belirli bir serbestlik derecesinde ve saptanan yanılma düzeyinde t tablosunda bulunan teorik değer

d: Olayın görülme sıklığına göre yapılmak istenen +, - sapma olarak simgelenmiştir.

t: 1,96'dır.

$$n = \frac{n \times p \times p \times Z^2}{[(N-1) \times t^2] + (p \times q \times Z^2)} = \frac{1126 \times 0{,}5 \times 0{,}5 \times 1{,}96^2}{[(1126-1) \times 0{,}05^2] + (0{,}5 \times 0{,}5 \times 1{,}96^2)} = 287$$

Yapılan hesaplama neticesinde (%95 güven düzeyi ve %5 hata payı ile) ulaşılması gereken minimum örneklem sayısı 287 olarak hesaplanmıştır. Sonrasında meslek gruplarına göre tabakalandırma yapılarak, meslek gruplarına göre ulaşılması gereken minimum katılımcı sayıları belirlenmiş ve Çizelge 2.2.1'de gösterilmiştir.

Çizelge 2.2.1. Araştırmanın Gerçekleştirildiği Hastanede Görev Yapan Sağlık Çalışanlarının Unvanlarına Göre Dağılımı (Haziran, 2022)

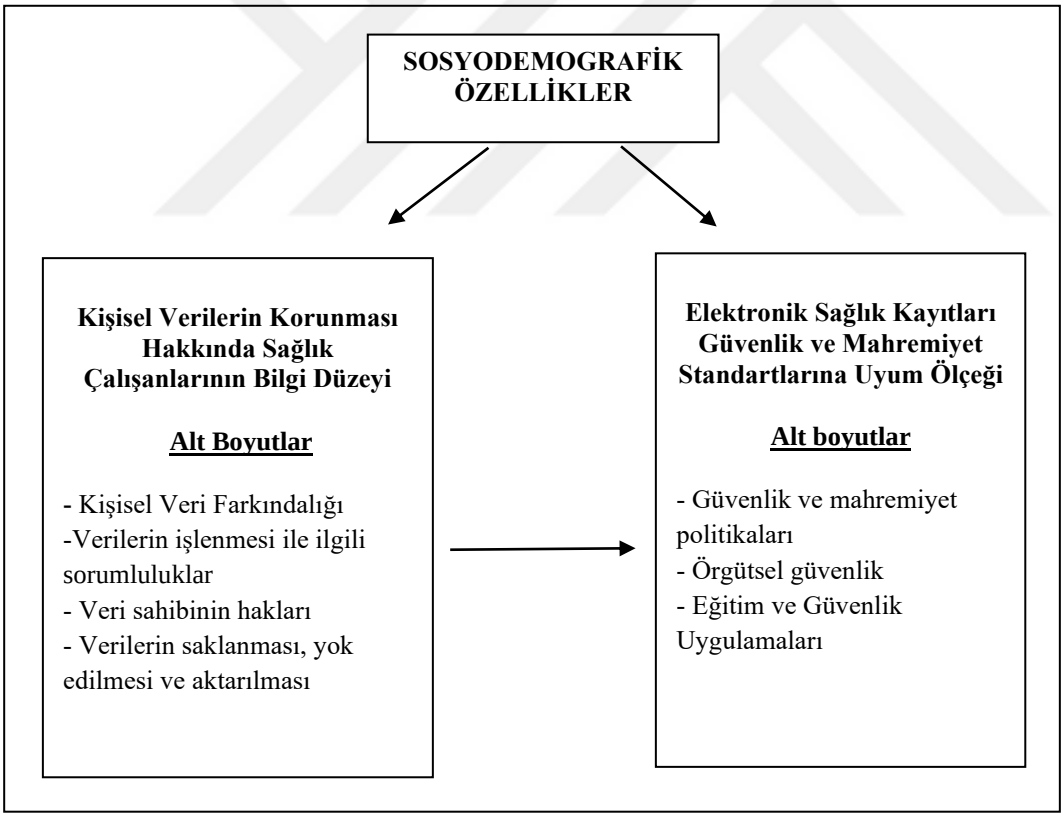
Unvan	Toplam sayı	Yüzde	Tabakalandırılmış Minimum Örneklem Sayısı
Hekim (Uzman+Pratisyen)	144	12,8	38
Hemşire +Ebe+Sağlık Memuru	651	57,8	166
Sağlık Tekn (Att, Lab. Tek., Radyoloji Tek. vb) +Tıbbi Sekreter	291	25,9	74
Diğer Sağlık Personeli (Eczacı, Biyolog, Sosyal Hizmet Uzmanı, Fizyoterapist vb)	40	3,5	10
Toplam	1126	100	288

Araştırmaya dahil olma kriterleri; araştırmanın yürütüldüğü hastanede hedef olarak belirlenen sağlık meslek gruplarından birinde, 657 sayılı devlet memurları kanunu kapsamında istihdam edilmiş olmak, en az bir yıldır bu hastanede görev yapıyor olmak ve araştırmaya gönüllü katılım sağlamak olarak belirlenmiştir. Araştırmanın verileri 2023 yılı Ocak-Nisan ayları arasında yüz yüze görüşme ile anket yöntemi kullanılarak elde edilmiştir. Kayıp veriler olma ihtimali göz önüne alınarak ve evren temsiliyetini artırmak adına araştırmaya minimum örneklem büyüklüğünden daha fazla sayıda katılımcı davet edilmiş ve araştırma gönüllü katılım sağlamayı kabul eden 366 sağlık çalışanı ile tamamlanmıştır.

2.3. Araştırmanın Modeli

Araştırma amacını gerçekleştirmek için tasarlanan araştırma modeli Şekil 2.3.'te verilmiştir.

Şekil 2.3 Araştırma Modeli



2.4. Araştırmanın Hipotezleri

Araştırmanın amacını gerçekleştirmek üzere aşağıdaki hipotezler oluşturulmuştur.

H1: Sağlık çalışanlarının KVK-HSBDÖ ve alt boyutlarına dair bilgi düzeyleri;

Sosyo-demografik özelliklerinden;

H1a1: Yaşa göre istatistiksel olarak anlamlı fark göstermektedir.

H1a2: Cinsiyete göre istatistiksel olarak anlamlı fark göstermektedir.

H1a3: Medeni duruma göre istatistiksel olarak anlamlı fark göstermektedir.

H1a4: Eğitim durumuna göre istatistiksel olarak anlamlı fark göstermektedir.

H1a5: Unvana göre istatistiksel olarak anlamlı fark göstermektedir.

H1a6: Meslekte çalışma yılına göre istatistiksel olarak anlamlı fark göstermektedir.

H1a7: Kurumda çalışma yılına göre istatistiksel olarak anlamlı fark göstermektedir.

H1a8: Elektronik sağlık kayıtlarını kullanma sürelerine göre istatistiksel olarak anlamlı fark göstermektedir.

Çalışanların eğitim alma özelliklerinden;

H1b1: Elektronik sağlık kayıtları, bilgi güvenliği ve mahremiyeti konularında eğitim almalarına göre istatistiksel olarak anlamlı fark göstermektedir.

H1b2: Kurumdaki elektronik sağlık kayıtları ile ilgili bilgi güvenliği ve mahremiyeti uygulamalarını değerlendirmelerine göre istatistiksel olarak anlamlı fark göstermektedir.

H1b3: Hasta hakları ve kişilik haklarında eğitim almalarına göre istatistiksel olarak anlamlı fark göstermektedir.

H1b4: KVKK hakkında daha önceden eğitim almalarına göre istatistiksel olarak anlamlı fark göstermektedir.

H2: Sağlık çalışanlarının elektronik sağlık kayıtlarının güvenlik ve mahremiyeti standartlarına uyumu toplam ölçek ve alt boyut puanları;

Sosyo-demografik özelliklerinden;

H2a1: Yaşa göre istatistiksel olarak anlamlı fark göstermektedir.

H2a2: Cinsiyete göre istatistiksel olarak anlamlı fark göstermektedir.

H2a3: Medeni duruma göre istatistiksel olarak anlamlı fark göstermektedir.

H2a4: Eğitim durumuna göre istatistiksel olarak anlamlı fark göstermektedir.

H2a5: Unvana göre istatistiksel olarak anlamlı fark göstermektedir.

H2a6: Meslekte çalışma yılına göre istatistiksel olarak anlamlı fark göstermektedir.

H2a7: Kurumda çalışma yılına göre istatistiksel olarak anlamlı fark göstermektedir.

H2a8: Elektronik sağlık kayıtlarını kullanma sürelerine göre istatistiksel olarak anlamlı fark göstermektedir.

Çalışanların eğitim alma özelliklerinden;

H2b1: Elektronik sağlık kayıtları, bilgi güvenliği ve mahremiyeti konularında eğitim almalarına göre istatistiksel olarak anlamlı fark göstermektedir.

H2b2: Kurumdaki elektronik sağlık kayıtları ile ilgili bilgi güvenliği ve mahremiyeti uygulamalarını değerlendirmelerine göre istatistiksel olarak anlamlı fark göstermektedir.

H2b3: Hasta hakları ve kişilik haklarında eğitim almalarına göre istatistiksel olarak anlamlı fark göstermektedir.

H2b4: KVKK hakkında daha önceden eğitim almalarına göre istatistiksel olarak anlamlı fark göstermektedir.

H3: Sağlık çalışanlarının KVK-HSBDÖ ve alt boyutları ile elektronik sağlık kayıtlarının güvenlik ve mahremiyeti standartlarına uyumu düzeyleri ölçeği ve alt boyutları arasında istatistiksel olarak anlamlı bir ilişki vardır.

2.5. Veri Toplama Araçları

Araştırma için kullanılan soru formu 3 kısımdan oluşmaktadır. Birinci kısımda sağlık çalışanlarının sosyo-demografik özelliklerini belirleyen sorular yer almıştır. Bu kısımda katılımcılara yaş, cinsiyet, medeni durum, unvanı, meslekte çalışma yılı, kurumda çalışma yılı, elektronik sağlık kayıtlarını kullanım süreleri gibi sorular

yanında katılımcıların elektronik sağlık kaydı ve veri güvenliği konusunda eğitim alma durumları ile ilgili sorular sorulmuştur.

İkinci kısımda KVK-HSBDÖ kullanılmıştır. Bu ölçek 4 boyuttan ve 20 maddeden oluşmaktadır. Değerlendirme Evet Hayır, Fikrim yok şeklinde yapılmaktadır. Ölçeğin güvenirlik katsayıları (Cronbach's Alpha) Kişisel Verilerin Farkındalığı boyutu için 0,810 Verilerin İşlenmesi Hakkında Şartlar ve Sorumluluklar boyutu için 0,724, Veri Sahibinin Hakları boyutu için 0,636 Verilerin saklanması, yok edilmesi ve aktarılmasına ilişkin politikalar boyutu için 0,690 ve toplamda 0,857 olarak hesaplanmıştır. 6698 Sayılı Kişisel Verilerin Korunması Kanunu çerçevesinde geliştirilen bu ölçeğe ilişkin süreç sonraki bölümde tanımlanmıştır.

Üçüncü ve son kısımda ise "Elektronik Sağlık Kayıtları Güvenlik ve Mahremiyeti Standartlarına Uyum Ölçeği" kullanılmıştır. Ölçeğe ilişkin bilgiler aşağıda verilmiştir.

Elektronik Sağlık Kayıtları Güvenlik ve Mahremiyeti Uyum Ölçeği

Mishra ve arkadaşları (2011) tarafından Health Insurance Portability and Accountability Act (HIPAA) standartlarını temel alınarak geliştirilen, Vedat Mehmet Paksoy (2019) tarafından Türkçe uyarlaması yapılmış Elektronik Sağlık Kayıtları Güvenlik ve Mahremiyet Standartlarına Uyum Ölçegi" 3 faktörden (Güvenlik ve Mahremiyet Politikaları, Örgütsel Güvenlik, Eğitim ve Güvenlik Uygulamaları) oluşan 20 maddelik bir ölçektir. Ölçeğin puanlaması orijinal ölçekte olduğu gibi 5'li Likert Skalası (1: Kesinlikle katılmıyorum, 2: Katılmıyorum, 3: ne atılıyorum ne katılmıyorum, 4: Katılıyorum, 5: Kesinlikle katılıyorum) ile değerlendirilmektedir. Paksoy (2019) tarafından araştırmada kullanılan ölçeğin güvenilirliği; Cronbach's Alpha güvenirlik katsayısı ile değerlendirilmiştir. İç tutarlılığı gösteren tüm maddeler için Cronbach's Alpha güvenirlik katsayısının Güvenlik ve Mahremiyet Politikaları boyutu (0,879), Örgütsel Güvenlik boyutu (0,871), Eğitim ve Güvenlik Uygulamaları boyutu (0,804) olduğu saptanmıştır.

Sağlık Çalışanlarının Kişisel Verilerin Korunması Kanunu Kapsamındaki Hukukî Sorumluluklarına İlişkin Bilgi Düzeyi Ölçeği

Türkiye'de sağlık çalışanlarının Kişisel Verilerin Korunması Kanunu kapsamındaki hukukî sorumluluklarına ilişkin bilgi düzeyini ölçen bir ölçek bulunmadığından, bu ölçek araştırmacılar tarafından 6698 Kişisel Verilerin Korunması Kanunu ve kişisel verilerin korunması kurumunun yayınları temelinde geliştirilmiştir. Bu ölçek ile sağlık çalışanlarının kişisel verilerin korunması kanunu çerçevesindeki hukukî sorumlulukları ile ilgili bilgi düzeylerini değerlendirmek hedeflenmektedir. Öncelikle 6698 Kişisel Verilerin Korunması Kanunu ve kişisel verilerin korunması kurumunun yayınları incelenerek 35 sorudan oluşan bir madde havuzu oluşturulmuştur. Sorular, hasta verilerine ulaşan ve onu kullanmaya yetkili olan sağlık çalışanlarını değerlendirecek şekilde ilgili kanun maddeleri temelinde oluşturulmuştur. Oluşturulan madde havuzu soruları akademisyen ve hukuk alanında çeşitli görevler yürüten 10 hukuk uzmanına değerlendirilmesi üzere sunulmuştur ve ifadelerin uygunluğuna dair görüşleri alınmıştır. Görüşlerine başvurulan uzmanlara ilişkin özellikler ve onay durumları Çizelge 3.8.1'de gösterilmektedir. Oluşturulan madde havuzundaki ifadelerin değerlendirme için uygun olduğuna karar verildikten sonra, havuzda yer alan 35 maddeyi içeren soru formu, 20 sağlık çalışanına uygulanarak dil açısından anlaşılabilir olup olmadığı kontrol edilmiştir. Sorulara verilecek cevaplar; "Evet, Hayır, Fikrim Yok" şeklindedir. Ölçekte doğru yanıtlar 1 puan, yanlış yanıtlar ve fikrim yok ifadeleri 0 puan olarak hesaplanmıştır.

2.6. Araştırmanın Etik Yönü

Araştırma Kırıkkale Üniversitesi Girişimsel Olmayan Araştırmalar Etik Kurulu'nun 29.06.2022 tarih 2022.06.08 sayılı onayı ile Kırıkkale İl Sağlık Müdürlüğü ve Kırıkkale Yüksek İhtisas Hastanesi Başhekimliğinin 12.10.2022 tarih ve E-46743357-799 sayılı izinleriyle gerçekleştirilmiştir (Ek1, Ek 2, Ek 3).

Araştırmanın yürütülmesinde gönüllülük esas alınmıştır. Katılımcılara uygulama öncesi araştırmacı tarafından bilgi verilerek gönüllü onam formu ile onamları alınmıştır

2.7. Araştırmanın Sınırlılıkları

Araştırmanın sonuçları, araştırmanın gerçekleştirildiği hastanede görev yapan 366 sağlık çalışanının vermiş olduğu cevaplar ile sınırlıdır, genellenemez.

2.8. Verilerin Analizi

Araştırma sonucunda elde edilen verilerin analizinde SPSS (Statistical Package for the Social Sciences) 21.0 paket programı kullanılmış ve %95 güven düzeyinde çalışılmıştır.

Öncelikle uzman görüşleri alınan 35 maddelik "KVK-HSBDÖ ile ilgili kapsam geçerlilik indeksi hesaplanmıştır. Sonrasında açımlayıcı faktör analizi (AFA) gerçekleştirilmiştir. Faktör analizi öncesinde ise; madde test korelasyonları incelenmiştir. Ölçeğin faktör analizine uygun olup olmadığını anlamak amacıyla KMO ve Bartlett testi yapılmıştır.

Ölçeğin faktör yapısının belirlenmesi amacıyla, açıklayıcı faktör analizi gerçekleştirilmiştir, faktör sayısının 1'den fazla olması durumunda "Oblimin with Kaiser Normalization" işlemi kullanılarak maddelerin ilgili faktörlere atanması işlemi yapılmıştır. Faktör analizi işleminde ölçek maddelerinin faktörlere atanması ya da ölçekten çıkarılması işlemlerinde faktör yükü değerlerine bakılmıştır.

Analizler sonrasında 4 boyutlu ve 20 maddeli "KVK-HSBDÖ"nin elde edilmesinin ardından kullanılan ölçeklere ilişkin normallik analizleri gerçekleştirilmiştir. Çalışmada ölçeklerin, güvenirlik düzeyinin belirlenmesi için Cronbach's Alpha katsayıları hesaplanmıştır Normallik analizleri sonrasında ölçek puanlarının normal dağılım göstermediği belirlenmiş ve hipotezleri test etmek üzere parametrik olmayan Mann Whitney U testi, Kruskal Wallis testi kullanılmıştır. Kruskal Wallis testinde fark çıkması durumunda çoklu karşılaştırma Bonferroni düzeltmeli Mann Whitney

testi ile analiz edilmiştir. Ölçek puanları arasındaki ilişki Spearman korelasyon testi ile analiz edilmiştir.

Kapsam Geçerliliği

Sağlık çalışanlarının Kişisel Verilerin Korunması Kanunu kapsamındaki hukukî sorumluluklarına ilişkin bilgi düzeyini değerlendirmek üzere oluşturulan maddeler ile ilgili kapsam geçerliliği çalışması, araştırmada kullanılacak sorular için 10 hukukçu uzmanın görüşü bizzat alınarak yapılmıştır. Görüşü alınan uzmanlar üniversite bünyesinde çalışan doçent öğretim üyesi, doktor öğretim üyesi, araştırma görevlileri, serbest avukatlar, Adalet Bakanlığı ve sağlık bakanlığı çalışanıdır. Görüş bildiriminde bulunan uzmanların hepsi hukuk fakültesi mezunudur. Sağlık çalışanlarının Kişisel Verilerin Korunması Kanunu kapsamındaki hukukî sorumluluklarına ilişkin bilgi düzeyini ölçmeye yönelik hazırlanan sorular uzmanlara yazılı olarak verilmiştir. Her göstergenin yanında uzmanlara "uygun, uygun değil ya da düzeltilmelidir" seçenekleri sunulmuştur. Ölçek soruları; sağlık çalışanlarının günlük rutin işlerini yürütürken kişisel verilerin korunması konusunda yaşanan durumların hukukî açıdan nasıl sonuç doğuracağı hakkında fikir sahibi olup olmadıklarını öğrenmek amacıyla oluşturulmuştur. Kapsam geçerliliği çerçevesinde danışılan uzmanlar listesi Çizelge 2.8.1 de verilmiştir.

Çizelge 2.8.1. Geliştirilen Ölçek İçin Uzman Onayları Çizelgesi

	Uzmanlar	**Uzmanlık Alanı**	**Unvan**	**Onaylama**
1	FA** AS**	Medeni Hukuk	Akademisyen (Dr.)	Onaylandı
2	OZ** CA**	Ticaret Hukuku	Akademisyen (Prof.)	Onaylandı
3	AD** KÜ**	Anayasa Hukuku	Akademisyen (Dr.)	Onaylandı
4	BU** UR**	Anayasa Hukuku	Akademisyen (Arş. Gör)	Onaylandı
5	ÜL** ÖZ**	Medeni Hukuk	Akademisyen (Arş. Gör)	Onaylandı
6	Fİ** EK**	İdare Hukuku	Adalet Bakanlığı	Onaylandı
7	Sİ** EK**	-	Avukat	Onaylandı
8	BE** GÜ**	Ticaret Hukuku	Avukat	Onaylandı
9	PI** GÜ**	Ticaret Hukuku	Avukat	Onaylandı
10	GÜ** YÜ**	Bilişim Hukuku	Avukat	Onaylandı

Alınan uzman görüşleri sonrasında madde havuzunda yer alana her bir maddeye göre hesaplanan kapsam geçerlilik oranları Çizelge 2.8.2'de gösterilmiştir.

Çizelge 2.8.2. Maddelere Göre Kapsam Geçerlilik Oranları

Maddeler	Uygun Bulanlar	Değişim şartıyla uygun bulanlar	Uygunsuz Bulanlar	Kapsam Geçerlilik Oranı
Madde 1	9	1	0	0,8
Madde 2	10	0	0	1
Madde 3	10	0	0	1
Madde 4	10	0	0	1
Madde 5	10	0	0	1
Madde 6	10	0	0	1
Madde 7	10	0	0	1
Madde 8	10	0	0	1
Madde 9	10	0	0	1
Madde 10	10	0	0	1
Madde 11	10	0	0	1
Madde 12	10	0	0	1
Madde 13	10	0	0	1
Madde 14	10	0	0	1
Madde 15	10	0	0	1
Madde 16	10	0	0	1
Madde 17	10	0	0	1
Madde 18	10	0	0	1
Madde 19	7	0	3	0,4
Madde 20	10	0	0	1
Madde 21	10	0	0	1
Madde 22	8	2	0	0,6
Madde 23	10	0	0	1
Madde 24	10	0	0	1
Madde 25	10	0	0	1
Madde 26	10	0	0	1
Madde 27	10	0	0	1
Madde 28	10	0	0	1
Madde 29	8	0	0	0,6
Madde 30	10	0	0	1
Madde 31	8	0	0	0,6
Madde 32	10	0	0	1
Madde 33	10	0	0	1
Madde 34	10	0	0	1
Madde 35	10	0	0	1
Tüm Ölçeğin Kapsam Geçerlilik İndeksi				**0.943**

Kapsam geçerlilik indeksi hesaplamalarının ardından gerçekleştirilecek faktör analizi öncesinde ise; madde test korelasyonları incelenmiştir. Tavşancıl (2002)'a göre ölçekteki maddeler için madde test korelâsyonlarının 0,30 ve üstünde olması önerilmektedir (Tavşancıl, 2002).

Çizelge 2.8.3. Madde Toplam Korelasyonları 1

Maddeler	Silinen maddenin göre ölçek ortalaması	Kalan maddelerin ölçek ortalaması	Düzeltilmiş madde-toplam korelasyon	Silinen maddenin Cronbach's Alpha değeri
Madde 1	26,96	24,144	,341	,835
Madde 2	27,05	24,176	**,165**	,838
Madde 4	26,99	23,836	,360	,834
Madde 5	27,11	22,549	,567	,827
Madde 6	27,04	23,185	,500	,830
Madde 7	27,00	23,649	,419	,832
Madde 8	27,02	23,556	,402	,832
Madde 9	27,08	22,861	,515	,829
Madde 10	27,09	22,608	,581	,826
Madde 11	27,10	22,834	,504	,829
Madde 13	27,02	23,211	,538	,829
Madde 14	27,05	22,959	,540	,828
Madde 15	27,00	23,570	,458	,832
Madde 17	26,99	23,786	,395	,833
Madde 18	27,00	23,575	,440	,832
Madde 19	27,51	24,344	**,049**	,845
Madde 22	27,08	23,651	**,292**	,835
Madde 24	27,03	23,610	,363	,833
Madde 25	27,17	23,274	,328	,834
Madde 27	27,04	23,399	,429	,832
Madde 29	26,97	24,103	,308	,835
Madde 30	27,08	23,352	,375	,833
Madde 33	27,11	23,154	,397	,832
Madde 34	26,99	23,901	,348	,834
Madde 35	27,02	23,591	,395	,833
Madde 3	27,13	23,526	**,288**	,835
Madde 12	27,11	23,442	,322	,834
Madde 16	27,03	23,621	,359	,833
Madde 20	27,28	23,638	**,204**	,839
Madde 21	27,17	23,337	,309	,835
Madde 23	27,48	23,450	**,234**	,838
Madde 26	27,40	23,469	**,228**	,839
Madde 28	27,76	24,913	**-,061**	,845
Madde 31	27,14	23,424	,307	,835
Madde 32	27,30	24,101	**,102**	,843

Madde toplam korelasyonu 1 için korelasyon değeri 0,300'den küçük olan 2, 3, 19, 20, 22, 23, 26, 28 ve 32 numaralı maddeler çıkartılmıştır. Tekrarlanan madde toplam korelasyonu sonuçları çizelge 2.8.4'te gösterilmiştir.

Çizelge 2.8.4. Madde Toplam Korelasyonları 2

Maddeler	Silinen maddenin göre ölçek ortalaması	Kalan maddelerin ölçek ortalaması	Düzeltilmiş madde-toplam korelasyon	Silinen maddenin Cronbach's Alpha değeri
Madde 1	21,66	17,109	,345	,870
Madde 4	21,69	16,844	,364	,869
Madde 5	21,81	15,552	,640	,861
Madde 6	21,73	16,169	,555	,864
Madde 7	21,70	16,667	,432	,868
Madde 8	21,72	16,543	,432	,867
Madde 9	21,78	15,799	,597	,862
Madde 10	21,79	15,598	,659	,860
Madde 11	21,80	15,818	,568	,863
Madde 13	21,71	16,265	,565	,864
Madde 14	21,75	15,980	,592	,863
Madde 15	21,69	16,602	,471	,867
Madde 17	21,69	16,780	,411	,868
Madde 18	21,70	16,594	,458	,867
Madde 24	21,73	16,729	,335	,870
Madde 25	21,86	16,392	,320	,872
Madde 27	21,73	16,460	,437	,867
Madde 29	21,67	17,126	,282	,871
Madde 30	21,78	16,425	,380	,869
Madde 33	21,81	16,340	,374	,869
Madde 34	21,69	16,901	,351	,869
Madde 35	21,72	16,571	,426	,868
Madde 12	21,81	16,478	,332	,871
Madde 16	21,73	16,707	,344	,870
Madde 21	21,87	16,514	,281	,873
Madde 31	21,84	16,559	,286	,873

Madde toplam korelasyonu 2 için korelasyon değeri 0,300'den küçük olan 21, 29, 31 numaralı maddeler çıkarılmıştır ve madde toplam korelasyonu yeniden hesaplanarak Çizelge 2.8.5'de gösterilmiştir.

Çizelge 2.8.5. Madde Toplam Korelasyonları 3

Maddeler	Silinen maddenin göre ölçek ortalaması	Kalan maddelerin ölçek ortalaması	Düzeltilmiş madde-toplam korelasyon	Silinen maddenin Cronbach's Alpha değeri
Madde 1	19,18	14,377	,352	,872
Madde 4	19,21	14,135	,367	,871
Madde 5	19,33	12,934	,648	,862
Madde 6	19,25	13,505	,562	,865
Madde 7	19,22	13,974	,434	,869
Madde 8	19,24	13,849	,439	,869
Madde 9	19,30	13,149	,610	,863
Madde 10	19,31	12,954	,677	,861
Madde 11	19,32	13,132	,594	,864
Madde 13	19,23	13,599	,571	,866
Madde 14	19,27	13,316	,606	,864
Madde 15	19,22	13,945	,458	,869
Madde 17	19,21	14,088	,408	,870
Madde 18	19,22	13,910	,459	,869
Madde 24	19,25	14,074	,318	,873
Madde 25	19,39	13,657	,340	,874
Madde 27	19,25	13,839	,415	,870
Madde 30	19,30	13,778	,370	,872
Madde 33	19,33	13,631	,389	,871
Madde 34	19,21	14,187	,355	,871
Madde 35	19,24	13,902	,420	,870
Madde 12	19,33	13,844	,316	,874
Madde 16	19,25	14,112	,301	,873

Bu aşamada tüm ifadelerin madde toplam korelasyonu 0,300'den büyük olduğu için faktör analizine bu 20 madde dahil edilmiştir.

Sonrasında, ölçeğin faktör analizine uygun olup olmadığını incelemek amacıyla KMO ve Bartlett testi yapılmıştır. KMO katsayısı örneklemin büyüklüğünü test etmek için hesaplanırken, normal dağılım koşulu Bartlett testiyle incelenmektedir. Bu kapsamda KMO testi ölçüm sonucunun .50 ve daha üstü, Bartlett küresellik testi sonucunun da istatistiksel olarak anlamlı olması gerekmektedir. İlgili sonuçlar Çizelge 2.8.6'da verilmiştir.

Çizelge 2.8.6. Sağlık Çalışanlarının Kişisel Verilerin Korunması Kanunu Kapsamındaki Hukukî Sorumluluklarına İlişkin Bilgi Düzeyi Ölçeği KMO ve Bartlett Testi Sonuçları

Kaiser-Meyer-Olkin Örneklem Uygunluk Testi		0,845
Bartlett's testi	**Approx. Chi-Square**	2259,337
	sd	190
	p	0,000

Sağlık Çalışanlarının Kişisel Verilerin Korunması Kanunu Kapsamındaki Hukukî Sorumluluklarına İlişkin Bilgi Düzeyi Ölçeği için yapılan faktör analizinde KMO değeri 0,845 olarak hesaplanmıştır. Buna göre örneklem sayısı faktör analizi için uygundur (KMO>0,500). Bartlett testi kapsamında X^2 değeri 2259,337 ve istatistiksel olarak anlamlı bulunmuştur (p<0,05). KMO ve Bartlett testi sonucuna göre verilerin faktör analizi için uygun olduğu sonucuna ulaşılmıştır.

AFA birçok gizli değişkenin daha kontrol edilebilir faktörler haline getirilmesinde yani verilerin azaltılmasında ve özetlenmesinde kullanılmaktadır. Ölçeğin faktör yapısının belirlenmesi amacıyla faktör sayısının 1'den fazla olması durumunda Oblimin With Kaiser Normalization işlemi kullanılarak maddelerin ilgili faktörlere atanması işlemi yapılmıştır. Faktör analizi işleminde ölçek maddelerinin faktörlere atanması ya da ölçekten çıkarılması işlemlerinde faktör yükü değerlerine bakılmıştır.

Cronbach's alpha katsayısı ölçeğin güvenirlik düzeyini vermektedir ve katsayı 0 ile 1 arasında değişmektedir. Alpha (α) katsayısına bağlı olarak ölçeğin güvenilirliği şu şekilde yorumlanmaktadır (Alpar, 2003).

• ,00 ≤ α < ,40 ise ölçek güvenilir değildir,

• ,40 ≤ α < ,60 ise ölçeğin güvenirliği düşük,

• ,60 ≤ α < ,80 ise ölçek oldukça güvenilir,

• ,80 ≤ α < 1,00 ise ölçek yüksek derecede güvenilir bir ölçektir.

Çizelge 2.8.7. Sağlık Çalışanlarının Kişisel Verilerin Korunması Kanunu ile İlgili Hukukî Sorumluluklarına İlişkin Bilgi Düzeyi Ölçeği Faktör Analizi Sonuçları

Maddeler	Boyutlar				Açıklanan varyans oranı	Cronbach's Alpha
	1	2	3	4		
Madde 9	,814				28,650	,810
Madde 11	,813					
Madde 10	,777					
Madde 5	,633					
Madde 12	,567					
Madde 30	,432					
Madde 15		,834			8,634	,724
Madde 17		,745				
Madde 16		,631				
Madde 18		,528				
Madde 13		,446				
Madde 34			,843		7,372	,636
Madde 35			,727			
Madde 33			,637			
Madde 25			,545			
Madde 27			,320			
Madde 7				,847	6,522	,690
Madde 4				,714		
Madde 6				,555		
Madde 8				,513		

Extraction Method: Principal Component Analysis.

Rotation Method: Oblimin with Kaiser Normalization.

Yapılan açıklayıcı faktör analizi sonucuna göre Sağlık Çalışanlarında Kişisel Verilerin Korunması Kanunu ile İlgili Hukukî Sorumluluklarına İlişkin Bilgi Düzeyi Ölçeğinin 4 faktörden oluştuğu belirlenmiştir. Ölçeğin toplam varyansı açıklama oranı %51,177; güvenirlik katsayısı 0,857'dir. Buna göre boyutun güvenirlik düzeyi çok yüksektir.

Ölçeğin 1.boyutu faktör yükleri 0,432 ile 0,814 arasında değişen 6 maddeden (5, 9, 10, 11, 12 ve 30 numaralı madde) oluşmaktadır. Boyutun toplam varyansı açıklama

oranı %28,650; güvenirlik katsayısı 0,810'dur. Buna göre boyutun güvenirlik düzeyi çok yüksektir.

Ölçeğin 2.boyutu faktör yükleri 0,446 ile 0,834 arasında değişen 5 maddeden (13, 15, 16, 17. ve 18 numaralı madde) oluşmaktadır. Boyutun toplam varyansı açıklama oranı %8,634; güvenirlik katsayısı 0,724'tır. Buna göre boyutun güvenirlik düzeyi oldukça yüksektir.

Ölçeğin 3. boyutu faktör yükleri 0,320 ile 0,843 arasında değişen 5 maddeden (25, 27, 33, 34, 35 numaralı maddeler) oluşmaktadır. Boyutun toplam varyansı açıklama oranı %7,372; güvenirlik katsayısı 0,636'dir. Buna göre boyutun güvenirlik düzeyi yüksektir.

Ölçeğin 4. boyutu faktör yükleri 0,513 ile 0,847 arasında değişen 4 maddeden (4, 6, 7, 8 numaralı maddeler) oluşmaktadır. Boyutun toplam varyansı açıklama oranı %6,522; güvenirlik katsayısı 0,690'dir. Buna göre boyutun güvenirlik düzeyi yüksektir.

Çizelge 2.8.8. Ölçek Puanlarına Ait Betimsel İstatistikler ve Güvenirlik Analizi Sonuçları

Kullanılan Ölçekler ve Alt Boyutları	**Min**	**Max**	**x̄**	**ss**	**Cronbach's Alpha**
-Kişisel veri farkındalığı	0,00	1,00	,82	,273	0,810
-Verilerin işlenmesi ile ilgili sorumluluklar	0,00	1,00	,91	,194	0,724
-Veri sahibinin hakları	0,00	1,00	,86	,220	0,636
-Verilerin saklanması, yok edilmesi ve aktarılması	0,00	1,00	,91	,208	0,690
KVK-HSBD Ölçeği	0,20	1,00	,87	,173	0,857
-Güvenlik ve Mahremiyet Politikaları	1,88	5,00	4,00	0,69	0,922
-Örgütsel Güvenlik	1,80	5,00	3,97	0,65	0,838
-Eğitim ve Güvenlik Uygulamaları	1,17	5,00	3,99	0,70	0,877
ESK-GMSU Ölçeği	1,89	5,00	3,99	0,62	0,948

KVK-HSBDÖ ve alt boyutları ile Elektronik Sağlık Kayıtları Güvenlik ve Mahremiyet Standartlarına Uyum ve alt boyut puanları güvenirlik katsayıları 0,700 üstü olduğu için güvenirliğin yüksek olduğu görülmektedir.

2.9. Normallik Testi

Güvenirlik analizi sonrası, araştırma amacını gerçekleştirmek üzere kullanılacak ölçeklerin normal dağılım sağlayıp sağlamadığı analiz edilmiştir. Ölçek puanlarına ait normallik testi Çizelge 2.9.1'de verilmiştir.

Çizelge 2.9.1. Ölçek Puanlarına Ait Normallik Testi

	Kolmogorov-Smirnov Testi		
	İstatistik	**df**	**Sig.**
Kişisel veri farkındalığı	0,339	366	,000
Verilerin işlenmesi ile ilgili sorumluluklar	0,449	366	,000
Veri sahibinin hakları	0,326	366	,000
Verilerin saklanması, yok edilmesi ve aktarılması	0,463	366	,000
KVK-HSBD Ölçeği	0,249	366	,000
Güvenlik ve Mahremiyet Politikaları	0,173	366	,000
Örgütsel Güvenlik	0,214	366	,000
Eğitim ve Güvenlik Uygulamaları	0,19	366	,000
ESK-GMSU Ölçeği	0,146	366	,000

Yapılan normallik analizine göre ölçek puanlarının normal dağılım göstermediği belirlenmiştir ($p<0,05$). Buna göre araştırma hipotezlerini test etmek üzere yapılan analizlerde parametrik olmayan test teknikleri kullanılmıştır.

3. BULGULAR

Bu bölümde elde edilen verilere ilişkin gerçekleştirilen analizlerle elde edilen bulgular sunulmaktadır.

3.1. Araştırmaya Katılan Sağlık Çalışanlarının Sosyo-Demografik Özelliklerine İlişkin Tanımlayıcı Bulguları

Çizelge 3.1.1.'de araştırmaya katılan sağlık çalışanlarının sosyo-demografik özellikleri sunulmaktadır.

Çizelge 3.1.1. Katılımcıların Sosyodemografik Özellikleri

Sosyodemografik Özellikler		**n**	**%**
Cinsiyet	Kadın	247	67,5
	Erkek	119	32,5
Medeni durum	Evli	248	67,8
	Bekar	118	32,2
Yaş	30 yaş ve altı	143	39,1
	31-35 yaş	88	24,0
	36 yaş ve üstü	135	36,9
Eğitim düzeyi	Lise	48	13,1
	Ön lisans-Lisans	261	71,3
	Yüksek lisans-Doktora-Tıpta uzmanlık	57	15,6
Unvan	Hekim	59	16,1
	Hemşire/Ebe/Sağlık Memuru	212	57,9
	Sağlık Tek/Tıbbi Sekreter	74	20,3
	Diğer sağlık meslekleri	21	5,7
Meslekte çalışma yılı	5 yıl ve daha az	95	26,0
	6-15 yıl	182	49,7
	16 yıl ve daha fazla	89	24,3
Kurumda çalışma yılı	3 yıl ve daha az	128	35,0
	4-7 yıl	105	28,7
	8 yıl ve daha fazla	133	36,3

Çizelge 3.1.1. incelendiğinde sağlık çalışanlarının sosyo-demografik özelliklerine ilişkin tanımlayıcı bulguları şöyledir;

- Katılımcıların %67,5'i kadın %32.5'i erkeklerden oluşmaktadır.
- Katılımcıların %67,8'i evli, %32,2'si bekârlardan oluşmaktadır.

- Araştırmaya katılanların %13,1'i lise, %71,3'ü önlisans ve lisans, %15,6'i yüksek lisans ve doktora programlarından mezun olmuştur.
- Katılımcıların %39,1'i 30 yaş ve altında, %24'ü 31-35 yaş grubunda ve %36,9'u 36 yaş ve üstü yaş grubunda yer almaktadır.
- Katılımcıların %16,'ini hekimler, %57,9'unu hemşire/ebe/sağlık memuru olarak çalışanlar, %20,3'ünü sağlık teknikerleri ve tıbbi sekreterler oluşturmaktadır. Ayrıca %5,7 katılımcı ise diğer sağlık meslekleri (eczacı, biyolog, fizyoterapist vb.) grubunda yer almaktadır.
- Katılımcıların %26'sı mesleklerinde 5 yıl ve daha az süre deneyime sahipken, %49,7'si6-15 yıllık ve %24,3'ü ise 16 yıl ve daha fazla sürelik bir mesleki deneyime sahiptir. Katılımcıların ortalama mesleki deneyim süresi ise 11 yıldır.
- Katılımcıların araştırmanın gerçekleştirildiği kurumda görev yapma süreleri incelendiğinde ise; %35'inin bu kurumda 3 yıl ve daha az süredir görev yaptığı, %28,7'sinin 4-7 yıl aralığında ve %36,3'ünün 8 yıl ve daha uzun süredir görev yaptığı belirlenmiştir. Katılımcıların araştırmanın gerçekleştirildiği kurumda görev süresi ortalaması ise; 6,5 yıldır.

Çizelge 3.1.2. Katılımcıların Eğitim Alma Durumları ve ESK Kullanım Süresi

Sosyodemografik Özellikler		**n**	**%**
ESK kullanımı deneyimi süresi	3 yıl ve daha az	93	25,4
	4-7 yıl	100	27,3
	8 yıl ve daha fazla	173	47,3
ESK bilgi güvenliği ve mahremiyeti konularında eğitim alma durumu	Evet	265	72,8
	Hayır	99	27,2
Kurumunun ESK ile ilgili bilgi güvenliği ve mahremiyeti uygulamaları ile ilgili değerlendirme	Yeterli, bu konuda tüm kurallara uyulmaktadır	150	41,1
	Tamamen Yetersiz	33	9,0
	Kısmen yeterli, ESK ile ilgili güvenlik açıkları olduğunu düşünüyorum	182	49,9
Hasta hakları ve kişilik hakları konusunda eğitim alma durumu	Evet	234	63,9
	Hayır	132	36,1
KVKK kapsamındaki hukukî sorumluluklarla ilgili eğitim alma durumu	Evet	219	59,8
	Hayır	147	40,2

Çizelge 3.1.2 incelendiğinde sağlık çalışanlarının eğitim alma durumları ve esk kullanım sürelerine ilişkin tanımlayıcı bulguları şöyledir;

- Katılımcıların elektronik sağlık kayıtlarını kullanım süreleri ortalama 7,3 yıldır
- Katılımcılardan %27,2'si elektronik sağlık kayıtları, bilgi güvenliği ve mahremiyeti konularında eğitim almadığını ifade etmiştir. Eğitimi aldığını ifade edenler ise toplam katılımcıların %72,8'ini oluşturmaktadır.
- Katılımcılar arasında elektronik sağlık kayıtları ile ilgili bilgi güvenliği ve mahremiyeti uygulamalarını yeterli görenlerin oranı %41,1, eksiklerin olduğunu düşünlerin oranı 49,9 tamamen yetersiz olduğunu düşünenlerin oranı ise %9'dur.
- Katılımcıların %63,9'u hasta hakları ve kişilik hakları ile ilgili eğitim aldığını ifade ederken kalan %36,1'i eğitim almadığını belirtmiştir.
- Katılımcıların %59,8'i kişisel verilerin korunması kanunu kapsamındaki hukukî sorumluluklara ilişkin eğitim aldığını ifade ederken %40,2'si eğitim almadığını ifade etmiştir.

3.2. Sağlık Çalışanlarının Kişisel Verilerin Korunması Kanunu'na İlişkin Bilgi Düzeyi

Sağlık çalışanların Kişisel Verilerin Korunması Kanunu'na İlişkin Bilgi Düzeyini ölçek üzere oluşturulan ifadeleri katılım durumları Çizelge 3.2.1' de verilmiştir.

Çizelge 3.2.1. Sağlık Çalışanlarının Kişisel Verilerin Korunması Kanunu Kapsamındaki Hukukî Sorumluluklarına İlişkin Bilgi Düzeyi

İfadeler	Fikrim yok		Katılmıyorum		Katılıyorum	
	n	%	n	%	n	%
4. Hastaya ait sağlık verileri tümüyle kişisel veri kabul edilir.	22	6,0	5	1,4	339	92,6
5.Hastaların kişisel verileri bilimsel amaçlar için kullanılacaksa açık rıza alınmadan da kullanılabilir.	33	9,0	37	10,1	296	80,9
6. Hastanın hayatı, beden bütünlüğü söz konusu ise ve acil bir durum söz konusu rıza aranmaksızın kişisel veriler kullanılıp işlenebilir.	29	7,9	13	3,6	324	88,5

Çizelge 3.2.1. Sağlık Çalışanlarının Kişisel Verilerin Korunması Kanunu Kapsamındaki Hukukî Sorumluluklarına İlişkin Bilgi Düzeyi (Devamı)

İfadeler	Fikrim yok		Katılmıyorum		Katılıyorum	
	n	%	n	%	n	%
7. Öğrenildiği durumlarda kişinin mağdur olmasına ya da ayrımcılığa maruz kalmasına neden olan verilere Özel Nitelikli Kişisel Verilerdir. Bu halde sağlık verileri özel nitelikli verilerdir.	26	7,1	3	,8	337	92,1
8. Kişinin teşhis edilmesini sağlayan verilere Biyometrik veriler denir. Hastanın biyometrik verileri gereklilik kalksa bile muhafaza edilmelidir.	34	9,3	3	,8	329	89,9
9. Hastaların sağlık verileri; kamu sağlığı korunurken veya koruyucu hekimlik uygulamaları kapsamında kullanılacaksa, kişinin açık rızası olmaksızın yetkili kurum ve kuruluşlar tarafından işlenebilir ve aktarılabilir.	33	9,0	27	7,4	306	83,6
10.Sağlığa ilişkin veriler tıbbi teşhis ve tedavi hizmetlerinin yürütülmesi amacıyla izin aranmaksızın yetkili kurum ve kuruluşlar tarafından işlenebilir ve aktarılabilir.	49	13,4	13	3,6	304	83,1
11.Sağlığa ilişkin veriler; sağlık hizmetlerinin ve finansmanının planlanması ve yönetimi amacıyla ilgili kişinin açık rızası olmaksızın yetkili kurum ve kuruluşlar tarafından işlenebilir ve aktarılabilir.	40	10,9	25	6,8	301	82,2
*12. Sağlığa ilişkin veriler yurtdışına aktarılırken ülkede geçerli olan kişisel verilerin korunması prosedürlerine gerek kalmaz.	44	12,0	296	80,9	26	7,1
13. Hastalara ait kişisel veriler bilimsel çalışmalarda ancak ilgili kişilerin özel hayatın gizliliğini ve kişisel haklarını ihlâl etmemek şartıyla kullanılabilir.	21	5,7	14	3,8	331	90,4
14. Kamu kurumunda hastaya ait veriler disiplin soruşturmasında kullanılacaksa ilgili hastadan izin alınması gerekmez.	30	8,2	18	4,9	318	86,9
15. Hastane çalışanları hastalara ait verilerin saklanmasında her türlü önlemi almak ve alınan önlemi uygulamak zorundadır.	19	5,2	9	2,5	338	92,3
*16. Sağlık personeli hastaya ait bilgileri hastayla kan bağı olan herkese açıklayabilir.	24	6,6	325	88,8	17	4,6
17. Sağlık kurumlarında veri sorumluları ile verileri işleyen kişilerin, verilerin gizliliği ve paylaşımı konusundaki sorumlulukları görevden ayrıldıktan sonra da devam eder.	19	5,2	6	1,6	341	93,2
18. Hastaya ait veriler kullanılmadan önce yapılan aydınlatma yetersizse verilerin kullanılması hak ihlalidir.	25	6,8	5	1,4	336	91,8
25. Aydınlatmanın herhangi bir şekli zorunluluğu yoktur. Sözlü, yazılı vb. şekilde gerçekleştirilebilir.	42	11,5	48	13,1	276	75,4

Çizelge 3.2.1. Sağlık Çalışanlarının Kişisel Verilerin Korunması Kanunu Kapsamındaki Hukukî Sorumluluklarına İlişkin Bilgi Düzeyi (Devamı)

	Fikrim yok		Katılmıyorum		Katılıyorum	
İfadeler	**n**	**%**	**n**	**%**	**n**	**%**
27.Anonim veri herhangi bir kişi ile ilişkilendirilemeyecek verilere denir. Buna göre hastanın yüzü çekilmeden vücut parçasının fotoğrafını çekmek anonim veriyi oluşturur.	23	6,3	19	5,2	324	88,5
30. Beyaz kod veren sağlık çalışanları için güvenlik personelinin hasta bilgilerine hastane sisteminden ulaşılması hak ihlali değildir	31	8,5	28	7,7	307	83,9
33. Hastanın örtünme tercihleri gibi dışarıdan bakıldığında tespit edilebilen bilgileri kişisel veri sayılmaz.	26	7,1	45	12,3	295	80,6
34. İdare kişisel verileri korumak için tedbirler almak zorundadır. (aykırı kullanım, aykırı erişim, doğru muhafaza)	20	5,5	5	1,4	341	93,2
35. Kişisel veriler, kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından (sağlık bakanlığı, sağlık müdürlükleri, hastaneler…) yürütülen önleyici ve koruyucu faaliyetler kapsamında işlenebilir.	21	5,7	15	4,1	330	90,2

* Çizelgede yer alan, 12, 16 numaralı ifadeler KVKK'na göre kasıtlı olarak oluşturulan yanlış ifadelerdir.

Çizelge 3.2.1. ve devam çizelgelerinde araştırmaya katılan sağlık çalışanlarının KVK-HSBDÖ için oluşturulan madde havuzundaki tüm ifadelere ilişkin değerlendirmeler gösterilmiştir. Çizelgeler incelendiğinde katılım düzeyi en yüksek olan ifadelerin; 15, 17 ve 34 numaralı maddeler olduğu görülmektedir. Bu maddeler ve katılım yüzdeleri aşağıda verilmiştir.

- Madde 15-Hastane çalışanları hastalara ait verilerin saklanmasında her türlü önlemi almak ve alınan önlemi uygulamak zorundadır (%92,3).
- Madde 17-Sağlık kurumlarında veri sorumluları ile verileri işleyen kişilerin, verilerin gizliliği ve paylaşımı konusundaki sorumlulukları görevden ayrıldıktan sonra da devam eder (%93,2).
- Madde 34-İdare kişisel verileri korumak için tedbirler almak zorundadır (aykırı kullanım, aykırı erişim, doğru muhafaza) (%93,2).

  Katılım düzeyi en düşük olan ifadeler ise; 12ve 16 sayılı ifadelerdir.

- Madde 12- Sağlığa ilişkin veriler yurtdışına aktarılırken ülkede geçerli olan kişisel verilerin korunması prosedürlerine gerek kalmaz (%7,1).
- Madde 16- Sağlık personeli hastaya ait bilgileri hastayla kan bağı olan herkese açıklayabilir (%4,6).

Çizelge 3.2.4'te ise; sağlık çalışanlarının KVK-HSBDÖ verdiği cevapların doğru ve yanlış olma durumları incelenmektedir.

Çizelge 3.2.2. Çalışanların KVK-HSBD Ölçeğine Verdikleri Yanıtların Doğru-Yanlış Olma Durumları

İfadeler		**Boyutlar**				**Doğru yanıt Ort.**	**Standart Sapma**
		Doğru		**Yanlış**			
		n	%	n	%		
Kişisel veri farkındalığı	İfade 5	296	**80,9**	70	**19,1**	0,81	0,394
	İfade 9	306	83,6	60	16,4	0,84	0,371
	İfade 10	304	83,1	62	16,9	0,83	0,376
	İfade 11	301	82,2	65	17,8	0,82	0,383
	İfade12	296	**80,9**	70	**19,1**	0,81	0,394
	İfade 30	307	83,9	59	16,1	0,84	0,368
1. Boyut ort.			**82,4**		**17,6**		
Verilerin işlenmesi ile ilgili sorumluluklar	İfade 13	331	90,4	35	9,6	0,9	0,294
	İfade 15	338	92,3	28	7,7	0,92	0,266
	İfade 16	325	88,8	41	11,2	0,89	0,316
	İfade 17	341	93,2	25	6,8	0,93	0,253
	İfade 18	336	91,8	30	8,2	0,92	0,275
2. Boyut ort.			**91,3**		**8,7**		
Veri sahibinin hakları	İfade 25	276	**75,4**	90	**24,6**	0,75	0,431
	İfade 27	324	88,5	42	11,5	0,89	0,319
	İfade 33	295	**80,6**	71	**19,4**	0,81	0,396
	İfade 34	341	93,2	25	6,8	0,93	0,253
	İfade 35	330	90,2	36	9,8	0,9	0,298
3. Boyut ort.			85,6		14,4		
Verilerin saklanması, yok edilmesi ve aktarılması	İfade 4	339	92,6	27	7,4	0,93	0,262
	İfade 6	324	88,5	42	11,5	0,89	0,319
	İfade 7	337	92,1	29	7,9	0,92	0,27
	İfade 8	329	89,9	37	10,1	0,9	0,302
4. Boyut ort.			**90,8**		**9,2**		
Sağlık Çalışanlarının Kişisel Verilerin Korunması Kanunu Kapsamındaki Hukukî Sorumluluklarına İlişkin Bilgi Düzeyi Ölçeği						**0,87**	**0,173**

Çizelge 3.2.2. incelendiğinde; sağlık çalışanlarının ölçeğin, kişisel veri farkındalığı

alt boyutundaki ifadeleri %82 oranında doğru cevapladıkları, verilerin işlenmesi ile ilgili sorumluluklar alt boyutundaki ifadelerini ise %91,3 doğru yanıtladıkları, veri sahibinin hakları alt boyutundaki ifadelerin ise, %85 oranında doğru yanıtlandığı, son olarak verilerin saklanması, yok edilmesi ve aktarılması alt boyutunda yer alan ifadelere %90'ın üzerinde doğru cevap verildiği görülmektedir. Ölçeğin tamamı değerlendirildiğinde sağlık çalışanlarının Kişisel Verilerin Korunması Kanunu Kapsamındaki Hukukî Sorumluluklarına İlişkin Bilgi Düzeyi Ölçeği yer alan ifadeleri %87 oranında doğru yanıtladığı, yani sağlık çalışanlarının kişisel verilerin korunması kanunu kapsamındaki hukukî sorumluluklarına ilişkin bilgi düzeyinin ve farkındalıklarının oldukça yüksek olduğu görülmektedir.

Bu sonuçlar değerlendirildiğinde sağlık çalışanlarının KVKK kapsamında en iyi bildiği konuların verilerin işlenmesi ile ilgili sorumluluklar ve verilerin saklanması, yok edilmesi ve aktarılması konuları olduğu söylenebilir. Ancak kişisel veri farkındalığı (yanlış cevap %17,6) ve özellikle veri sahibinin hakları (yanlış cevap %14,4) konusunda bilgi eksikleri olduğu belirlenmiştir.

3.3. Elektronik Sağlık Kayıtları Güvenlik ve Mahremiyet Standartlarına Uyum Ölçeği

Bu bölümde araştırmaya katılan sağlık çalışanlarının ESK-GMSU Ölçeği ifadelerine ilişkin değerlendirmeleri incelenmiştir.

Çizelge 3.3.1.'de araştırmaya katılan sağlık çalışanlarının ESK-GMSUÖ ifadelerine ilişkin değerlendirmeleri yer almaktadır. Çizelgeler incelendiğinde katılım düzeyi en yüksek olan ifadelerin; 1, 4 ve 5 sayılı maddeler olduğu belirlenmiştir. Bu ifadeler ve katılım yüzdeleri aşağıda verilmiştir.

Madde 1- Çalıştığım kurumda elektronik sağlık kayıtlarının güvenlik ve mahremiyet kurallarına uyumu için önceden tanımlanmış ve kabul görmüş bir uygulama bulunmaktadır (%80,4).

Madde 4- Çalışılan kurumlarda elektronik sağlık kayıtlarının güvenliğini temin etmek amacıyla gözle görülür bir liderlik sağlanmalıdır (%79,3).

Çizelge 3.3.1. Elektronik Sağlık Kayıtları Güvenlik ve Mahremiyet Standartlarına Uyum Ölçeği İfadelerine İlişkin Değerlendirmeler

Elektronik Sağlık Kayıtları Güvenlik ve Mahremiyet Standartlarına Uyum Ölçeği İfadeleri	**Katılmıyorum**		**Kararsızım**		**Katılıyorum**	
	n	**%**	**n**	**%**	**n**	**%**
1-Çalıştığım kurumda elektronik sağlık kayıtlarının güvenlik ve mahremiyet kurallarına uyumu için önceden tanımlanmış ve kabul görmüş bir uygulama bulunmaktadır.	12	3,2	60	16,4	294	80,4
2-Çalıştığım kurumda birbirini gözeten ve koruyan bireylerden oluşan yaygın bir bilgi güvenliği kültürü mevcuttur.	22	6,0	65	17,8	279	76,2
3-Çalıştığım kurumda bilgi güvenliği oluşturmak devamlı bir süreçtir.	20	5,4	63	17,2	283	77,3
4-Çalışılan kurumlarda elektronik sağlık kayıtlarının güvenliğini temin etmek amacıyla gözle görülür bir liderlik sağlanmalıdır.	16	4,4	60	16,4	290	79,3
5-Çalıştığım kurumda elektronik sağlık kayıtlarının güvenlik ve mahremiyetini sağlamak için gerekli olan politika, prosedür, eğitim, şifreleme ve erişim sınırlamaları gibi iç kontrol mekanizmaları mevcuttur	32	8,7	40	10,9	294	80,3
6-Çalıştığım kurumda denetleme yapmak, bilgi güvenliği çalışmalarını geliştirmek için gerekli bir eylem olarak görülmektedir.	30	8,2	54	14,8	282	77,1
7-Çalıştığım kurumda bilgi güvenliği politikaları veya prosedürleri kolaylıkla anlaşılabilir ve erişilebilir durumdadır.	28	7,7	51	13,9	287	78,5
8-Çalıştığım kurumda bilgi güvenliği hakkında bireyler arası bilgi alışverişi yapmanın önemli olduğu ifade edilmektedir.	24	6,5	53	14,5	185	78,9
9-Çalıştığım kurumda personele düzenli aralıklarla bilgi güvenliği politikaları eğitimi verilmektedir.	23	6,3	59	16,1	284	77,6
10-Çalıştığım kurumda bilgi güvenliği politika ve prosedürleri, değişen örgütsel gereksinimleri karşıladığının değerlendirilmesi amacıyla periyodik olarak gözden geçirilir.	22	6,0	63	17,2	281	76,8
11-Çalıştığım kurumda bilgi güvenliği politikalarını sıklıkla okumaya gereksinim duyarım.	28	7,7	63	17,2	275	75,1
12-Çalıştığım kurumda insan zaaflarını kullanarak bilgi aşırma taktiği olarak adlandırılan "Sosyal Mühendislik" konusunda sıklıkla bilgilendirme söz konusudur ve bu taktiklerin sistemim için nasıl hassasiyet yaratabileceğinin farkındayım.	21	5,7	74	20,2	271	74,1
13-Çalıştığım kurumda hangi bilgilere, ne amaçla erişebileceğimin farkındayım.	28	7,6	57	15,6	281	76,7
14-Çalıştığım kurumda bilgisayarım üzerinde dışarıdan getirilen taşınabilir belleğin kullanımı için iznim vardır.	26	7,1	64	17,5	276	75,4
15-Çalıştığım kurumda sistem de kötü amaçlı yazılım bulunduğunda ne yapacağıma dair prosedürlerin farkındayım.	20	5,5	71	19,4	189	75,1
16-Çalıştığım kurumda benim sorumlu olduğum herhangi bir bilginin yanlış kullanımını veya uygunsuz erişimini bildirmek zorundayım.	19	5,2	62	16,9	275	77,8
17-Çalıştığım kurumda uymak zorunda olduğum şifreleme politikalarının farkındayım.	14	3,8	66	18,0	286	78,1
18-Çalıştığım kurumda kabul gören uygun bir bilgi güvenliği davranışı ve tutumu sıklıkla tebliğ edilmektedir.	23	6,3	61	16,7	282	77,1
19-Çalıştığım kurumda, bilgi güvenliği konularında çalışanların eğitimi için sürekliliği olan bir çaba söz konusudur.	24	6,6	53	14,5	289	79

Katılım düzeyi en düşük olan ifadeler ise 12, 14 ve 15 numaralı maddelerdir.

- Madde 12- Çalıştığım kurumda insan zaaflarını kullanarak bilgi aşırma taktiği olarak adlandırılan "Sosyal Mühendislik" konusunda sıklıkla bilgilendirme söz konusudur ve bu taktiklerin sistemim için nasıl hassasiyet yaratabileceğinin farkındayım. (%74,1).
- Madde 15- Çalıştığım kurumda sistem de kötü amaçlı yazılım bulunduğunda ne yapacağıma dair prosedürlerin farkındayım. (%75,1).
- Madde 14-Çalıştığım kurumda bilgisayarım üzerinde dışarıdan getirilen taşınabilir belleğin kullanımı için iznim vardır. (%75,4).

Çizelge 3.3.2. Sağlık Çalışanlarının Kişisel Verilerin Korunması Kanunu Kapsamındaki Hukukî Sorumluluklarına İlişkin Bilgi Düzeylerinin Sosyodemografik Değişkenler Açısından İncelenmesi

Sosyodemografik Değişkenler		Kişisel veri farkındalığı			Verilerin işlenmesi ile ilgili sorumluluklar			Veri sahibinin hakları			Verilerin saklanması, yok edilmesi ve aktarılması			KVK-HSBDÖ		
		x̄	ss	p	x̄	ss	p	x̄	ss	p	x̄	ss	p	x̄	ss	p
Cinsiyet	**Kadın**	,79	,29		,90	,20		,84	,22		,90	,21		,86	,17	
	Erkek	,87	,19	,115	,93	,17	,184	,88	,21	**,015***	,92	,20	,135	,88	,16	,135
Mann Whitney U		13376,0			13777,5			12652,0			13222,0			13322,0		
Medeni durum	**Evli**	,80	,29		,92	,16		,85	,21		,90	,20		,86	,17	
	Bekar	,86	,21	,232	,89	,20	,107	,85	,23	,564	,91	,21	,241	,88	,16	,619
Mann Whitney U		13633,0			13520,2			14148,0			13847,0			14175,0		
ESK bilgi güvenliği ve mahremiyeti konularında eğitim alma durumu	**Evet**	,83	,27		,92	,18		,85	,22		,91	,19		,88	,16	
	Hayır	,79	,27	,088	,88	,21	**,040***	,85	,22	,717	,88	,23	,160	,85	,18	,068
Mann Whitney U		11774,0			11792,0			12831,0			12232,5			11539,5		
Hasta hakları ve kişilik hakları konusunda eğitim alma durumu	**Evet**	,79	,29		,91	,19		,83	,24		,89	,21		,85	,18	
	Hayır	,86	,23	,056	,90	,19	,513	,89	,17	**,012***	,92	,18	,261	,89	,15	**,034***
Mann Whitney U		13802,2			14981,0			13288,5			14670,0			13447,0		
KVKK kapsamındaki hukukî sorumluluklar konusunda eğitim alma durumu	**Evet**	,79	,29		,91	,19		,82	,24		,85	,22		,85	,18	
	Hayır	,86	,23	**,041***	,90	,20	,423	,90	,16	**,002***	,92	,17	,232	,89	,15	,055
Mann Whitney U		14306,0			15517,0			13336,0			15256,05			14253,0		

***p<0,05**

Çizelge 3.3.2'de Sağlık Çalışanlarının KVK-HSBDÖ puanlarının araştırmada incelenen sosyo-demografik özelliklere göre istatistiksel olarak anlamlı fark gösterip göstermediği Man Whitney U testi ile incelenmiştir. Çizelge 3.3.2. incelendiğinde;

Katılımcıların Kişisel Verilerin Korunması Kanunu kapsamındaki hukukî sorumluluklarına ilişkin bilgi düzeyleri puan ortalamaları ile katılımcıların cinsiyetleri, ESK bilgi güvenliği ve mahremiyeti konularında eğitim alma durumları, hasta hakları ve kişilik hakları konusunda eğitim alma durumları ve KVKK Kapsamındaki hukukî sorumlulukları konusunda eğitim alma durumları arasında istatistiksel olarak anlamlı fark olduğu görülmektedir ($p<0,05$). Elde edilen sonuçlara göre; Araştırmaya katılım sağlayan sağlık çalışanlarının KVK-HSBD ölçeğinin "veri sahibinin hakları" alt boyutundan elde ettiği puanların, katılımcıların cinsiyetlerine göre istatistiksel anlamlı bir fark ($U=12652,0$; $p=0,015<0,05$) oluşturduğu belirlenmiştir. Ortalamalar incelendiğinde bu farkın cinsiyeti erkek (ort: $0,88 \pm 0,21$) olan sağlık çalışanlarından kaynaklandığı görülmektedir. Buna göre hipotez **H1a2** (Cinsiyete göre istatistiksel olarak anlamlı fark göstermektedir) kabul edilmiştir.

Araştırmaya katılım sağlayan sağlık çalışanlarının KVK-HSBD ölçeğinin "verilerin işlenmesi ile ilgili hukukî sorumluluklar" alt boyutundan elde ettiği puanların, katılımcıların "ESK, bilgi güvenliği ve mahremiyet hakkında eğitim alma" durumuna göre istatistiksel anlamlı bir fark ($U=11792,0$ $p=0,040<0,05$) oluşturduğu belirlenmiştir. Ortalamalar incelendiğinde bu farkın ESK, bilgi güvenliği ve mahremiyet hakkında eğitim alan (ort: $0,92 \pm 0,18$) sağlık çalışanlarından kaynaklandığı görülmektedir. Buna göre hipotez **H1b1** (Elektronik sağlık kayıtları, bilgi güvenliği ve mahremiyeti konularında eğitim almalarına göre istatistiksel olarak anlamlı fark göstermektedir) kabul edilmiştir. Araştırmaya katılım sağlayan sağlık çalışanlarının KVK-HSBD ölçeğinin "veri sahibinin hakları" alt boyutundan elde ettiği puanların, katılımcıların "hasta hakları ve kişilik hakları konusunda eğitim alma" durumuna göre istatistiksel anlamlı bir fark ($U=13288,5$ $p=0,012<0,05$) oluşturduğu belirlenmiştir. Ortalamalar incelendiğinde bu farkın "hasta hakları ve kişilik hakları konusunda eğitim almayan" alan (ort: $0,89 \pm 0,17$) sağlık çalışanlarından kaynaklandığı görülmektedir. Ayrıca, KVK-HSDB ölçeği toplam puanlarının katılımcıların "hasta hakları ve kişilik hakları konusunda eğitim alma" durumuna göre istatistiksel anlamlı bir fark ($U=13447,0$ $p=0,034<0,05$) oluşturduğu

belirlenmiştir. Yine ortalamalar incelendiğinde bu farkın "hasta hakları ve kişilik hakları konusunda eğitim almayan" alan (ort: 0,89 ± 0,15) sağlık çalışanlarından kaynaklandığı görülmektedir. Buna göre hipotez **H1b3** (Hasta hakları ve kişilik haklarında eğitim almalarına göre istatistiksel olarak anlamlı fark göstermektedir.) kabul edilmiştir.

Araştırmaya katılım sağlayan sağlık çalışanlarının KVK-HSBD ölçeğinin "kişisel veri farkındalığı" alt boyutundan elde ettiği puanların, katılımcıların "KVKK kapsamındaki hukukî sorumlulukları konusunda eğitim alma" durumuna göre istatistiksel anlamlı bir fark (U=14306,0 p=0,041<0,05) oluşturduğu belirlenmiştir. Ortalamalar incelendiğinde bu farkın "KVKK kapsamındaki hukukî sorumlulukları konusunda dair eğitim almayan" (ort: 0,86 ± 0,23) sağlık çalışanlarından kaynaklandığı görülmektedir. Ayrıca, katılımcıların ölçeğin "veri sahibinin hakları" alt boyutundan elde ettiği puanların, katılımcıların "KVKK Kapsamındaki hukukî sorumlulukları konusunda eğitim alma" durumuna göre istatistiksel anlamlı bir fark (U=13336,0 p=0,002<0,05) oluşturduğu belirlenmiştir. Yine ortalamalar incelendiğinde bu farkın "KVKK kapsamındaki hukukî sorumlulukları konusunda eğitim almayan" (ort: 0,90 ± 0,16) sağlık çalışanlarından kaynaklandığı görülmektedir. Bu sonuca göre **Hipotez H1b4** (KVKK hakkında daha önceden eğitim almalarına göre istatistiksel olarak anlamlı fark göstermektedir.) kabul edilmiştir. Katılımcıların KVK-HSBD ölçeği ve alt boyutlarından elde ettikleri puanlar ile medeni durumları arasında anlamlı bir farklılık bulunamamıştır. Bu nedenle hipotez **H1a3** (Medeni duruma göre istatistiksel olarak anlamlı fark göstermektedir.) reddedilmiştir

Çizelge 3.3.2. Sağlık Çalışanlarının Kişisel Verilerin Korunması Kanunu Kapsamındaki Hukukî Sorumluluklarına İlişkin Bilgi Düzeylerinin Sosyodemografik Değişkenler Açısından İncelenmesi (Devamı)

Sosyodemografik Değişkenler		Kişisel veri farkındalığı			Verilerin işlenmesi ile ilgili sorumluluklar			Veri sahibinin hakları			Verilerin saklanması, yok edilmesi ve aktarılması			KVK-HSBDÖ		
		x̄	ss	p	x̄	ss	p	x̄	ss	p	x̄	ss	p	x̄	ss	p
Yaş	**30 yaş ve altı**	,82	,26	,696	,89	,22	,224	,85	,23	,910	,90	,22	,985	,86	,18	,555
	31-35 yaş	,82	,29		,93	,18		,85	,23		,91	,21		,87	,19	
	36 yaş ve üstü	,83	,26		,93	,16		,86	,19		,92	,18		,88	,14	
Chi-Square (X)²		,724			2,991			,189			,030			1,178		
Eğitim düzeyi	**Lise**	,83	,27	,915	,90	,18	,157	,86	,19	,408	,91	,21	,259	,87	,15	,910
	Ön lisans-Lisans	,81	,29		,90	,21		,84	,23		,90	,21		,86	,16	
	Yük lisans-dokt-tıpta uzm.	,88	,15		,96	,09		,90	,17		,94	,157		,92	,07	
Chi-Square (X)²		,171			3,707			1,791			2,701			,189		
Unvan	**Hekim**	,88	,17	**,001***	,96	,11	**,030***	,87	,19	**,005***	,93	,18	,149	,91	,10	**,001***
	Hemşire/ebe/sağlık memuru	,77	,31		,88	,22		,83	,23		,89	,22		,84	,19	
	Sağlık Tek /Tıbbi Sekreter	,91	,18		,95	,15		,90	,19		,91	,21		,92	,12	
	Diğer sağlık meslekleri	,94	,13		,96	,10		,93	,14		,98	,10		,95	,09	
Chi-Square (X)²		16,413			8,919			12,868			5,330			15,580		
Çoklu karşılaştırma		2<1,3,4			2<1,3,4			2<1,3,4						2<1,3,4		
Meslekte çalışma yılı	**5 yıl ve daha az**	,84	,22	,625	,90	,20	,530	,83	,25	,232	,89	,23	,618	,86	,17	,649
	6-15 yıl	,83	,28		,91	,20		,88	,20		,92	,19		,88	,17	
	16 yıl ve daha fazla	,80	,29		,93	,16		,84	,21		,90	21		,86	,17	
Chi-Square (X)²		,939			1,270			2,923			,962			,863		

***p<0,05**

Çizelge 3.3.2.'te araştırmaya katılım sağlayan sağlık çalışanlarının KVK-HSBDÖ puanlarının araştırmada incelenen sosyodemografik özelliklere göre istatistiksel olarak anlamlı fark gösterip Kruskall Wallis testi ile incelenmiştir. Analiz sonuçları incelendiğinde;

Araştırmaya katılan sağlık çalışanlarının KVK-HSBD ölçeğinin tüm boyutları (Kişisel veri farkındalığı, Verilerin işlenmesi ile ilgili sorumluluklar, Veri sahibinin hakları, Verilerin saklanması, yok edilmesi ve aktarılması) ve ölçeğin toplam puanı ile unvanları arasında istatistiksel olarak anlamlı fark olduğu ($p<0,05$) ve gerçekleştirilen post-hoc (Games Howell) test sonuçlarına göre ise, tüm boyutlar ve ölçeğin tamamı için farkı oluşturan grubun "ebe, hemşire ve sağlık memurlarından" oluşan meslek grubu olduğu belirlenmiştir. Bu sonuçlara göre; Hipotez **H1a5** (Unvana göre istatistiksel olarak anlamlı fark göstermektedir) kabul edilmiştir. Bu durumda sonuç olarak araştırmanın gerçekleştirildiği hastanede görev yapan "ebe-hemşire-sağlık memuru" grubunun Kişisel Verilerin Korunması Kanunu kapsamındaki hukukî sorumluluklarına ilişkin bilgi düzeyinin hastanede görev yapan diğer sağlık meslek grubu çalışanlarına göre düşük olduğu söylenebilir. Çizelge 3.3.2. incelendiğinde araştırmaya katılan sağlık çalışanlarının KVK-HSBD ölçeğinin toplamı ve tüm boyutlarından elde ettikleri puan ortalamaları ile yaş, eğitim düzeyi ve meslekte çalışma yılı özellikleri arasında istatistiksel olarak anlamlı farklılık olmadığı belirlenmiştir ($p>0,05$). Elde edilen bu sonuçlara göre; Hipotez **H1a1, H1a4** reddedilmiştir.

Çizelge 3.3.2. Sağlık Çalışanlarının Kişisel Verilerin Korunması Kanunu Kapsamındaki Hukukî Sorumluluklarına İlişkin Bilgi Düzeylerinin Sosyodemografik Değişkenler Açısından İncelenmesi (Devamı)

Sosyodemografik Değişkenler		**Kişisel veri farkındalığı**			**Verilerin işlenmesi ile ilgili sorumluluklar**			**Veri sahibinin hakları**			**Verilerin saklanması, yok edilmesi ve aktarılması**			**KVK-HSBDÖ**		
		x̄	**ss**	**p**	**x̄**	**ss**	**p**	**x̄**	**ss**	**p**	**x̄**	**ss**	**p**	**x̄**	**Ss**	**p**
Kurumda çalışma yılı	**3 yıl ve daha az**	,82	,26	,704	,91	,21	,202	,86	,21	,730	,89	,23	,087	,86	,18	,965
	4-7 yıl	,84	,27		,89	,21		,84	,25		,92	,20		,87	,18	
	8 yıl ve daha fazla	,81	,28		,94	,15		,86	,20		,93	,17		,88	,15	
Chi-Square (X^2)		,701			3,197			,630			4,879			,701		
ESK kullanım süresi	**3 yıl ve daha az**	,81	,25	,276	,86	,24	**,034***	,84	,23	,189	,85	,27	**,011***	,84	,20	,509
	4-7 yıl	,86	,26		,93	,17		,81	,26		,94	,19		,88	,17	
	8 yıl ve daha fazla	,81	,28		,93	,16		,89	,17		,92	,16		,88	,15	
Chi-Square (X^2)		2,572			6,772			3,33			9,098			1,350		
Çoklu karşılaştırma					1<2,3							1<2,3				
Kurumdaki ESK güvenliği ve mahremiyeti değerlendirmesi	**Yeterli**	,85	,25	,136	,92	,19	,809	,85	,22	**,002***	,92	,21	**,033***	,88	,16	,069
	Tamamen Yetersiz	,73	,33		,92	,15		,78	,22		,83	,25		,81	,20	
	Kısmen yeterli	,82	,27		,91	,20		,88	,21		,91	,19		,88	,17	
Chi-Square (X^2)		3,996			,423			12,819			6,841			5,347		
Çoklu karşılaştırma								2<1,3			2<1,3					

***p<0,05**

Çizelge 3.3.2'de araştırmaya katılım sağlayan sağlık çalışanlarının KVK-HSBDÖ puanlarının araştırmada incelenen sosyodemografik özelliklere göre istatistiksel olarak anlamlı fark gösterip Kruskall Wallis testi ile incelenmeye devam edilmektedir. Çizelge 3.3.2. incelendiğinde katılımcıların Kişisel Verilerin Korunması Kanunu Kapsamındaki Hukukî Sorumluluklarına ilişkin bilgi düzeylerinin; ESK kullanım süreleri, kurumdaki ESK ile ilgili bilgi güveliği mahremiyeti uygulamalarını değerlendirmelerine göre istatistiksel olarak farklılık göstermektedir ($p<0,05$). Analiz sonuçları incelendiğinde;

Araştırmaya katılım sağlayan sağlık çalışanlarının KVK-HSBD ölçeğinin "verilerin işlenmesi ile ilgili sorumluluklar" alt boyutundan elde ettiği puan ortalamalarının, katılımcıların "ESK kullanım süresine" göre istatistiksel anlamlı bir fark (X^2:6,772 $p=0,034<0,05$) oluşturduğu belirlenmiştir ve gerçekleştirilen post-hoc (Games Howell) test sonuçlarına göre ise bu farkın ESK kullanım deneyimi 3 yıl ve daha az olanlar ile 8 yıl ve daha fazla olan gruplardan kaynaklandığı belirlenmiştir. Bu sonuca göre **hipotez H2a7** (Elektronik sağlık kayıtlarını kullanma sürelerine göre istatistiksel olarak anlamlı fark göstermektedir.) kabul edilmiştir. Ayrıca, araştırmaya katılım sağlayan sağlık çalışanlarının KVK-HSBD ölçeğinin "Verilerin saklanması, yok edilmesi ve aktarılması" alt boyutundan elde ettikleri puan ortalamalarının katılımcıların "ESK kullanım süresine" göre istatistiksel anlamlı fark (X^2:9,098 $p=0,011<0,05$) oluşturduğu belirlenmiştir. Gerçekleştirilen post-hoc (Games Howell) test sonuçlarına göre ise bu farkın ESK kullanım deneyimi 4-7 yıl arasında olan sağlık çalışanlarından kaynaklandığı belirlenmiştir. Bu sonuca göre **H2a7 (**Elektronik sağlık kayıtlarını kullanma sürelerine göre istatistiksel olarak anlamlı fark göstermektedir.) kabul edilmiştir.

Çizelge 3.3.2.'de araştırmaya katılım sağlayan sağlık çalışanlarının KVK-HSBD ölçeğinin "veri sahibinin hakları" (X^2:12,819 $p=0,002$) ve "verilerin saklanması, yok edilmesi ve aktarılması" (X^2:6,841 $p=0,033$) alt boyutundan elde ettikleri puan ortalamalarının katılımcıların "Kurumdaki ESK ile ilgili bilgi güvenliği ve mahremie ti uygulamalarına ilişkin değerlendirmelerine" göre istatistiksel anlamlı fark oluştur- duğu belirlenmiştir ($p<0,05$).

Gerçekleştirilen post hoc test sonuçları ise; farkın kurumdaki ESK ile ilgili bilgi

güvenliği ve mahremiyeti uygulamalarını "tamamen yetersiz" olarak değerlendiren sağlık çalışanlarından kaynaklanmaktadır. Bu sonuçlara göre; "KVK-HSBD daha düşük olan sağlık çalışanları, kurumdaki uygulamaları tamamen yetersiz bulmaktadır" denilebilir. Bu sonuca göre hipotez H2b2 (Kurumdaki elektronik sağlık kayıtları ile ilgili bilgi güvenliği ve mahremiyeti uygulamalarını değerlendirmelerine göre istatistiksel olarak anlamlı fark göstermektedir.) kabul edilmiştir.

Çizelge 3.3.2'de yer alan sonuçlar incelendiğinde sağlık çalışanlarının KVK-HSBDÖ ve alt boyutlarından elde ettiği puan ortalamaları ile "kurumda çalışma yılı" özellikleri arasında istatistiksel olarak fark olmadığı görülmektedir ($p>0,05$). Böylece hipotez **H2a6** (Kurumda çalışma yılına göre istatistiksel olarak anlamlı fark göstermektedir.) reddedilmiştir.

Çizelge 3.3.3. Sağlık Çalışanlarının Elektronik Sağlık Kayıtları Güvenlik ve Mahremiyet Standartlarına Uyum Ölçeği'nin Sosyodemografik Değişkenler Açısından İncelenmesi

Sosyodemografik Değişkenler		Güvenlik ve Mahremiyet Politikaları			Örgütsel Güvenlik			Eğitim ve Güvenlik Uygulamaları			ESK-GMSUÖ		
		x̄	ss	p	x̄	ss	p	x̄	ss	p	x̄	ss	p
Unvan	**Hekim**	3,42	,79	**,000***	3,44	,78	**,000***	3,41	,86	**,000***	3,42	,71	**,000***
	Hemşire/Ebe/Sağlık memuru	4,06	,66		4,05	,57		4,06	,64		4,05	,56	
	Sağlık tek/Tıbbi sekreter	4,25	,46		4,15	,54		4,18	,48		4,20	,42	
	Diğer sağlık meslekleri	4,17	,58		4,18	,58		4,22	,69		4,19	,57	
Chi-Square (X^2)		38,973			37,217			37,275			43,012		
Çoklu karşılaştırma		1<2,3,4			1<2,3,4			1<2,3,4			1,2,3,4		
Meslekteki çalışma yılı	**5 yıl ve daha az**	4,13	,71	**0,040***	4,00	,71	,401	4,10	,74	**,020***	4,08	,65	**,026***
	6-15 yıl	3,98	,67		3,95	,62		3,95	,69		3,96	,61	
	16 yıl ve daha fazla	3,93	,72		3,97	,63		3,94	,68		3,94	,62	
Chi-Square (X^2)		6,416			1,825			7,856			7,286		
Çoklu karşılaştırma		2,3<1			2,3<1			2,3<1			2,3<1		
Bu kurumda çalışma yıl	**3 yıl ve daha az**	3,94	,74	,536	3,90	,68	,573	3,95	,72	,278	3,93	,66	,564
	4-7 yıl	4,04	,71		3,95	,69		4,04	,74		4,02	,65	
	8 yıl ve daha fazla	4,03	,64		4,04	,58		3,98	,65		4,02	,56	
		1,247			1,971			2,562			1,146		
ESK kullanım süresi.	**3 yıl ve daha az**	4,07	,68	,057	3,98	,66	,326	4,04	,69	,358	4,04	,62	,101
	4-7 yıl	4,07	,71		4,00	,68		4,02	,71		4,04	,63	
	8 yıl ve daha fazla	3,93	,69		3,94	,62		3,94	,71		3,94	,62	
Chi-Square (X^2)		5,727			2,243			2,052			4,580		
Çoklu karşılaştırma		3<1,2			1,3<2			3<1,2			3<1,2		

***p<0,05**

Çizelge 3.3.3.'de sağlık çalışanlarının ESK-GMSU ölçeği puanlarının araştırmada incelenen sosyodemografik özelliklere göre istatistiksel olarak anlamlı fark gösterip göstermediği Kruskal Wallis testi ile incelenmiştir. Çizelge 3.3.3. incelendiğinde katılımcıların Elektronik Sağlık Kayıtlarının Güvenlik ve Mahremiyet Standartlarına Uyumlarının puan ortalamaları ile katılımcıların unvanı ve meslekte çalışma yılları arasında anlamlı istatistiksel farklılık ($p<0,05$) olduğu görülmektedir. Elde edilen sonuçlara göre;

Araştırmaya katılım sağlayan sağlık çalışanlarının ESK-GMSU ölçeğinin tüm alt boyutları arasında (güvenlik ve mahremiyet politikaları, örgütsel güvenlik ve eğitim ve güvenlik uygulamaları) ve ölçek toplam puanı ile, katılımcıların unvanlarına göre farklılık ($p<0,05$) bulunmaktadır. Test sonuçlarına göre farklılığı oluşturan grup hekimlerdir. Bu sonuçlara göre, Hipotez **H2a5** "Unvana göre istatistiksel olarak anlamlı fark göstermektedir." kabul edilmiştir.

Bu durumda hastanede görev yapmakta olan hekimlerin elektronik sağlık kayıtlarının güvenlik ve mahremiyetleri standartlarına uyumları diğer görev yapan meslek gruplarına göre istatistiksel olarak daha düşük seviyededir. Bu çalışmaya katılım sağlayan sağlık çalışanlarının ESK-GMSU ölçeğinin tüm alt boyutları ve ölçek toplam puanlarında, katılımcıların kurumda çalışma yılı ile ESK kullanım süreleri arasında istatistiksel olarak anlamlı farklılık ($p>0,05$) bulunamamıştır. Bu sonuçlara göre **H2a7 (**Kurumda çalışma yılına göre istatistiksel olarak anlamlı fark göstermektedir.) ve **H2a8 (**Elektronik sağlık kayıtlarını kullanma sürelerine göre istatistiksel olarak anlamlı fark göstermektedir.) hipotezleri reddedilmiştir. Araştırmaya katılım sağlayan sağlık çalışanlarının ESK-GMSU ölçeğinin alt boyutu "güvenlik ve mahremiyet politikaları" ile katılımcıların meslekte çalışma yılları arasında istatistiksel olarak anlamlı farklılık ($p=0,04<0,05$) bulunmuştur. Araştırmaya katılım sağlayan sağlık çalışanlarının ESK-GMSU ölçeğinin alt boyutu "eğitim ve güvenlik uygulamaları" ile katılımcıların meslekte çalışma yılları arasında istatistiksel olarak anlamlı farklılık ($X^2=7,856$; $p=0,020<0,05$) bulunmuştur. Gerçekleştirilen post-hoc testlere göre farkı oluşturan grubun mesleğinde 5 yıldan daha az çalışma tecrübesine sahip sağlık çalışanlarından olduğu belirlenmiştir.
Bu sonuca göre hipotez **H2a6** Meslekte çalışma yılına göre istatistiksel olarak anlamlı fark göstermektedir.) kabul edilmiştir.

Çizelge 3.3.3. Sağlık Çalışanlarının Elektronik Sağlık Kayıtları Güvenlik ve Mahremiyet Standartlarına Uyum Ölçeği'nin Sosyodemografik Değişkenler Açısından İncelenmesi (Devamı)

Sosyodemografik Değişkenler		Güvenlik ve Mahremiyet Politikaları			Örgütsel Güvenlik			Eğitim ve Güvenlik Uygulamaları			ESK-GMSUÖ		
		x̄	ss	p	x̄	ss	p	x̄	ss	p	x̄	ss	p
Yaş	**30 yaş ve altı**	4,13	,66		3,99	,67		4,05	,67		4,07	,60	
	31-35 yaş	3,98	,62	**,012***	3,96	,62	,517	4,03	,65	,153	3,99	,58	,085
	36 yaş ve üstü	3,89	,76		3,95	,64		3,89	,76		3,90	,66	
Chi-Square ($X^{2)}$		8,792			1,319			3,751			4,936		
Çoklu karşılaştırma		1>2,3											
Eğitim Düzeyi	**Lise**	4,19	,62		4,16	,62		4,09	,63		4,15	,58	
	Ön lisans-Lisans	4,10	,62	**,000***	4,06	,56	**,000***	4,10	,62	**,000***	4,09	,53	**,000***
	Yüksek lisans-doktora-tıpta uzmanlık	3,38	,74		3,41	,77		3,41	,83		3,40	,70	
Chi-Square (X^2)		45,627			40,928			37,128			45,118		
Çoklu karşılaştırma		3-1,2			3-1,2			3-1,2			3-1,2		
Kurumdaki ESK güvenliği ve mahremiyeti değerlendirmesi	**Yeterli**	4,27	,51		4,35	,52		4,21	,55		4,22	,46	
	Tamamen Yetersiz	3,47	,82	**,000***	3,41	,76	**,000***	5,38	,86	**,000***	3,43	,74	**,000***
	Kısmen yeterli	3,89	,71		3,92	,66		3,92	,70		3,90	,62	
Chi-Square (X^2)		43,281			32,983			56,696			50,607		
Çoklu karşılaştırma		2,3<1			2,3<1			2,3<1			2,3<1		

***p<0,05**

Çizelge 3.3.3'te sağlık çalışanlarının ESK-GMSU ölçeği puanlarının araştırmada incelenen sosyodemografik özelliklere göre istatistiksel olarak anlamlı fark gösterip göstermediği Kruskal Wallis testi ile incelenmiştir. Çizelge 3.3.3. incelendiğinde katılımcıların Elektronik Sağlık Kayıtlarının Güvenlik ve Mahremiyet Standartlarına Uyumlarının puan ortalamaları ile yaş, eğitim düzeyi ve kurumdaki ESK güvenliği ve mahremiyeti değerlendirmesi arasında istatistiksel anlamlı farklılık($p<0,05$) bulunmuştur. Elde edilen sonuçlara göre;

Araştırmaya katılım sağlayan sağlık çalışanlarının, ESK-GMSU ölçeğinin alt boyutu "güvenlik ve mahremiyet politikaları" ile katılımcıların yaşları arasında istatistiksel olarak farklılık ($p<0,05$) bulunmuştur. Gerçekleştirilen post hoc test sonuçlarına göre; farkın yaşı 31-35 arası olan katılımcılardan oluştuğu bulunmuştur. Bu sonuca göre hipotez **H2a1** (Yaşa göre istatistiksel olarak anlamlı fark göstermektedir.) kabul edilmiştir. Araştırmaya katılım sağlayan sağlık çalışanlarının ESK-GMSU ölçeğinin tüm alt boyutları ve ölçek toplam puanları ile, katılımcıların eğitim düzeyleri arasında anlamlı istatistiksel farklılık ($p<0,05$) bulunmuştur. Gerçekleştirilen post hoc test sonuçlarına göre, farklılığın lisansüstü eğitim derecesine sahip katılımcılardan kaynaklandığı bulunmuştur. Böylece hipotez **H2a4** (Eğitim düzeyine göre istatistiksel olarak anlamlı fark göstermektedir.) kabul edilmiştir.

Araştırmaya katılım sağlayan sağlık çalışanlarının ESK-GMSU ölçeğinin tüm alt boyutları ve ölçek toplam puanları ile, katılımcıların kurumdaki ESK güvenliği ve mahremiyeti değerlendirmesi arasında anlamlı istatistik farklılık ($p<0,05$) bulunmuştur. Gerçekleştirilen post hoc test sonuçları ise; farkın kurumdaki ESK ile ilgili bilgi güvenliği ve mahremiyeti uygulamalarını "tamamen yetersiz" olarak değerlendiren sağlık çalışanlarından kaynaklanmaktadır. Bu sonuca göre hipotez **H2b2** (Kurumdaki elektronik sağlık kayıtları ile ilgili bilgi güvenliği ve mahremiyeti uygulamalarını değerlendirmelerine göre istatistiksel olarak anlamlı fark göstermektedir.) kabul edilmiştir.

Çizelge 3.3.3. Sağlık Çalışanlarının Elektronik Sağlık Kayıtları Güvenlik ve Mahremiyet Standartlarına Uyum Ölçeği'nin Sosyodemografik Değişkenler Açısından İncelenmesi (Devamı)

Sosyodemografik Değişkenler		**Güvenlik ve Mahremiyet Politikaları**			**Örgütsel Güvenlik**			**Eğitim ve Güvenlik Uygulamaları**			**ESK-GMSUÖ**		
		x̄	**ss**	**p**	**x̄**	**ss**	**p**	**x̄**	**ss**	**p**	**x̄**	**ss**	**p**
Cinsiyet	**Kadın**	3,98	,73		3,96	,64		3,96	,72		3,97	,64	
	Erkek	4,06	,61	,575	3,98	,68	,712	4,04	,65	**,**469	4,03	,59	,410
Mann Whitney U		14167,500			14350,500			14014,000			13916,500		
Medeni durum	**Evli**	3,95	,73		3,95	,66		3,96	,72		3,96	,64	
	Bekar	4,11	,60	,088	4,00	,62	,607	4,04	,67	,314	4,06	,57	,198
Mann Whitney U		13027,000			14150,500			13686,00			13416,000		
ESK bilgi güvenliği ve mahremiyeti konularında eğitim alma durumu	**Evet**	4,18	,59		4,07	,56		4,11	,60		4,13	,52	
	Hayır	3,55	,74	**,000***	3,69	,78	**,000***	3,65	,83	**,000***	3,62	,71	**,000***
Mann Whitney U		6535,000			9074,000			8477,000			7283,500		
Hasta hakları ve kişilik hakları konusunda eğitim alma durumu	**Evet**	4,16	,60		4,07	,56		4,11	,62		4,12	,54	
	Hayır	3,73	,76	**,000***	3,79	,74	**,001***	3,77	,78	**,000***	3,76	,68	**,000***
Mann Whitney U		10191,00			12133,500			11358,00			10166,50		
KVKK kapsamındaki hukukî sorumlulukları konusunda eğitim alma durumu	**Evet**	4,21	,56		4,11	,52		,415	,59		4,16	,50	
	Hayır	3,70	,77	**,000***	3,76	,75	**,000***	3,74	,78	**,000***	3,73	,69	**,000***
Mann Whitney U		9673,000			11749,000			11021,500			9747,000		

***p<0,05**

Çizelge 3.3.3'te Elektronik Sağlık Kayıtları Güvenlik ve Mahremiyet Standartlarına Uyum Ölçeği puanlarının araştırmada incelenen sosyodemografik özelliklere göre istatistiksel olarak anlamlı fark gösterip göstermediği incelenmiştir. Çizelge 3.3.3. incelendiğinde katılımcıların ESK-GMSU ölçeğinden elde ettikleri puan ortalamaları ile ESK bilgi güvenliği ve mahremiyeti konularında eğitim alma durumları, hasta hakları ve kişilik hakları konusunda eğitim alma durumları KVKK kapsamındaki hukukî sorumluluklara dair eğitim alma durumları arasında istatistiksel farklılık olduğu görülmektedir. Elde edilen sonuçlara göre;

Bu araştırmaya katılım sağlayan sağlık çalışanlarının ESK-GMSU ölçeğinin tüm alt boyutları ve ölçek toplam puanlarında, katılımcıların cinsiyetleri ve medeni durumları arasında anlamlı farklılık (p>0,05) bulunamamıştır. Bu nedenle **H2a2 (**Cinsiyete göre istatistiksel olarak anlamlı fark göstermektedir.) ve **H2a3 (**Medeni duruma göre istatistiksel olarak anlamlı fark göstermektedir.) hipotezleri reddedilmiştir. Araştırmaya katılım sağlayan sağlık çalışanlarının ESK-GMSU ölçeğinin tüm alt boyutları ve ölçek toplam puanlarında, katılımcıların ESK bilgi güvenliği ve mahremiyeti konularında eğitim alma durumlarına göre istatistiksel olarak anlamlı farklılık (p=0,000<0,05) olduğu belirlenmiştir. Gerçekleştirilen post hoc test sonuçlarına göre; farkı oluşturan grubun bu konuda eğitim alan sağlık çalışanlarından kaynaklandığı belirlenmiştir. Buna göre **H2b1 (**Elektronik sağlık kayıtları, bilgi güvenliği ve mahremiyeti konularında eğitim almalarına göre istatistiksel olarak anlamlı fark göstermektedir.) hipotezi kabul edilmiştir. Araştırmaya katılım gösteren sağlık çalışanlarının ESK-GMSU ölçeği ve tüm alt boyutları ile hasta hakları ve kişilik hakları konusunda eğitim alma durumu arasında istatistiksel olarak anlamlı farklılık (p=<0,05) bulunmuştur. Gerçekleştirilen post hoc testlere göre istatistiksel farklılığın hasta hakları ve kişilik hakları konularında eğitim alan sağlık çalışanlarından kaynaklandığı bulunmuştur. Bu sonuca göre hipotez **H2b3** (Hasta hakları ve kişilik haklarında eğitim almalarına göre istatistiksel olarak anlamlı fark göstermektedir.) kabul edilmiştir.

Ayrıca araştırmaya katılım gösteren sağlık çalışanlarının ESK-GMSU ölçeği ve tüm alt boyutları ile KVKK kapsamındaki hukukî sorumluluklara konusunda eğitim alma durumu arasında istatistiksel olarak anlamlı farklılık (p=<0,05) bulunmuştur. Yapılan

post hoc testlere göre gruplar arasındaki farklılığın KVKK kapsamındaki hukukî sorumluluklar konusunda eğitim alan sağlık çalışanlarından kaynaklandığı bulunmuştur. Bu sonuca göre hipotez **H2b4** (KVKK hakkında daha önceden eğitim almalarına göre istatistiksel olarak anlamlı fark göstermektedir.) kabul edilmiştir.

3.4. Ölçek Puanları Arasındaki İlişkinin İncelenmesi

Sağlık çalışanlarında KVK-HSBDÖ ile ESK Güvenlik ve Mahremiyet Standartlarına Uyum Ölçeği puanları arasındaki ilişkinin incelenmesi için yapılan Spearman korelasyon testi sonuçları Çizelge 3.4.1.'de verilmiştir.

Çizelge 3.4.1. Ölçek Puanları Arasındaki İlişkinin İncelenmesi

Korelasyon									
		1	2	3	4	5	6	7	8
1. Kişisel veri farkındalığı	**r**	1,000							
	p								
2. Verilerin işlenmesi ile ilgili sorumluluklar	**r**	,438**	1,000						
	p	,000							
3. Veri sahibinin hakları	**r**	,363**	,290**	1,000					
	p	,000	,000						
4. Verilerin saklanması, yok edilmesi ve aktarılması	**r**	,546**	,354**	,330**	1,000				
	p	,000	,000	,000					
5. KVK-HSBD Ölçeği		,827**	,599**	,679**	,630**	1,000			
	p	,000	,000	,000	,000				
6. Güvenlik ve Mahremiyet Politikaları	**r**	**,169****	,021	,075	**,213****	**,159****	1,000		
	p	,001	,687	,151	,000	,002			
7. Örgütsel Güvenlik	**r**	**,167****	-,015	,101	**,196****	**,148****	**,643****	1,000	
	p	,001	,777	,053	,000	,005	,000		
8. Eğitim ve Güvenlik Uygulamaları	**r**	**,231****	**,114***	**,137****	**,282****	**,240****	**,715****	**,702****	1,000
	p	,000	,029	,009	,000	,000	,000	,000	
9. ESK-GMSU Ölçeği	**r**	**,199****	,043	**,115***	**,240****	**,192****	**,903****	**,836****	**,890****
	p	,000	,410	,027	,000	,000	,000	,000	,000

*. Korelasyon 0.05 seviyesinde (2-tailed) anlamlıdır.
**. Korelasyon 0.01 seviyesinde (2-tailed) anlamlıdır.

Analiz sonuçlarına göre; Sağlık Çalışanlarının Kişisel Verilerin Korunması Kanunu Kapsamındaki Hukukî Sorumluluklarına İlişkin Bilgi Düzeyi Ölçeği toplam puanları

ile ESK Güvenlik ve Mahremiyet Standartlarına Uyum Ölçeği toplam puanları arasında istatistiksel olarak pozitif yönlü zayıf ilişki olduğu (r=0,192; p=0,000<0,01); yine KVK HSBD Ölçeği toplam puanları ile ESK-GMSU Ölçeği alt boyutlarından" Güvenlik ve Mahremiyet Politikaları" alt boyutu arasında pozitif yönlü zayıf ilişki olduğu (r=0,159; p=0,002<0,01); "Örgütsel Güvenlik" alt boyutu arasında pozitif yönlü zayıf ilişki olduğu (r=0,148; p=0,005<0,01); ve "Eğitim ve Güvenlik Uygulamaları" alt boyutu arasında pozitif yönlü zayıf ilişki olduğu (r=0,240; p=0,000<0,01) belirlenmiştir. Bu sonuçlar sağlık çalışanlarının Kişisel Verilerin Korunması Kanunu kapsamındaki hukukî sorumluluklarına ilişkin bilgi düzeylerinin artırılmasının kurumda ESK Güvenlik ve Mahremiyet Standartlarına Uyum düzeyini artıracağını göstermektedir.

Ayrıca, KVKK-HSBD Ölçeğinin alt boyutlarından "Verilerin Saklanması ve İşlenmesi" alt boyutu dışında (r=0,043; p=0,410>0,05) kalan diğer alt boyutların her biri sağlık çalışanlarının ESK Güvenlik ve Mahremiyet Standartlarına Uyum düzeyleri ile istatistiksel olarak anlamlı bir şekilde pozitif ilişkilidir. Analiz sonuçları KVKK-HSBD Ölçeğinin alt boyutlarından "Kişisel Veri Farkındalığı" alt boyutu ile ESK-GMSU Ölçeği toplam puanları arasında pozitif yönlü zayıf ilişki olduğunu (r=0,199; p=0,00<0,01); "Veri Sahibinin Hakları" alt boyutu ESK-GMSU Ölçeği toplam puanları arasında pozitif yönlü zayıf ilişki olduğunu (r=0,115; p=0,027<0,05); ve "Verilerin Saklanması ve Yok Edilmesi" alt boyutu ile ESK-GMSU Ölçeği toplam puanları arasında pozitif yönlü zayıf ilişki olduğunu (r=0,240; p=0,00<0,01) göstermektedir. Bu sonuçlara göre sağlık çalışanlarının Kişisel Verilerin Korunması Kanunu kapsamındaki hukukî sorumluluklarına ilişkin özellikle kişisel veri farkındalığı, veri sahibinin hakları ve verilerin saklanması, yok edilmesi konularında bilgi düzeyinin artırılmasının kurumda ESK Güvenlik ve Mahremiyet Standartlarına Uyum düzeylerini artıracağı söylenilebilir.

3.5. Hipotez Kabul ve Ret Çizelgesi

Araştırmada kullanılan ölçekler ve alt boyutları ile ilgili oluşturulan hipotezlere ait özet sonuçlar aşağıdaki gibidir;

Çizelge 3.5.1. Hipotezlere İlişkin Özet Sonuçlar

	HİPOTEZLER	**KABUL**	**RET**
H1	Sağlık çalışanlarının Kişisel Verilerin Korunması Kanunu kapsamındaki hukukî sorumlulukları ölçeği ve alt boyutlarına dair bilgi düzeyleri;	X	
	a. Sosyo-demografik özelliklerinden;		
H1a1	Yaşa göre istatistiksel olarak anlamlı fark göstermektedir.		X
H1a2	Cinsiyete göre istatistiksel olarak anlamlı fark göstermektedir.	X	
H1a3	Medeni duruma göre istatistiksel olarak anlamlı fark göstermektedir.		X
H1a4	Eğitim düzeyine göre istatistiksel olarak anlamlı fark göstermektedir.		X
H1a5	Unvana göre istatistiksel olarak anlamlı fark göstermektedir.	X	
H1a6	Meslekte çalışma yılına göre istatistiksel olarak anlamlı fark göstermektedir.		X
H1a7	Kurumda çalışma yılına göre istatistiksel olarak anlamlı fark göstermektedir.		X
H1a8	Elektronik sağlık kayıtlarını kullanma sürelerine göre istatistiksel olarak anlamlı fark göstermektedir.	X	
H1	Sağlık çalışanlarının Kişisel Verilerin Korunması Kanunu kapsamındaki hukukî sorumlulukları ölçeği ve alt boyutlarına dair bilgi düzeyleri;	X	
	b. Çalışanların eğitim alma özelliklerinden;		
H1b1	Elektronik sağlık kayıtları, bilgi güvenliği ve mahremiyeti konularında eğitim almalarına göre istatistiksel olarak anlamlı fark göstermektedir.	X	
H1b2	Kurumdaki elektronik sağlık kayıtları ile ilgili bilgi güvenliği ve mahremiyeti uygulamalarını değerlendirmelerine göre istatistiksel olarak anlamlı fark göstermektedir.	X	
H1b3	Hasta hakları ve kişilik haklarında eğitim almalarına göre istatistiksel olarak anlamlı fark göstermektedir.	X	
H1b4	KVKK hakkında daha önceden eğitim almalarına göre istatistiksel olarak anlamlı fark göstermektedir.	X	

Çizelge 3.5.1. Hipotezlere İlişkin Özet Sonuçlar (Devamı)

	HİPOTEZLER	KABUL	RET
H2	Sağlık çalışanlarının elektronik sağlık kayıtlarının güvenlik ve mahremiyeti standartlarına uyumu toplam ölçek ve alt boyut puanları;	X	
	a. Sosyo-demografik özelliklerinden;		
H2a1	Yaşa göre istatistiksel olarak anlamlı fark göstermektedir.	X	
H2a2	Cinsiyete göre istatistiksel olarak anlamlı fark göstermektedir.		X
H2a3	Medeni duruma göre istatistiksel olarak anlamlı fark göstermektedir.		X
H2a4	Eğitim düzeyine göre istatistiksel olarak anlamlı fark göstermektedir.	X	
H2a5	Unvana göre istatistiksel olarak anlamlı fark göstermektedir.	X	
H2a6	Meslekte çalışma yılına göre istatistiksel olarak anlamlı fark göstermektedir.	X	
H2a7	Kurumda çalışma yılına göre istatistiksel olarak anlamlı fark göstermektedir.		X
H2a8	Elektronik sağlık kayıtlarını kullanma sürelerine göre istatistiksel olarak anlamlı fark göstermektedir.		X
H2b1	Elektronik sağlık kayıtları, bilgi güvenliği ve mahremiyeti konularında eğitim almalarına göre istatistiksel olarak anlamlı fark göstermektedir.	X	
H2b2	Kurumdaki elektronik sağlık kayıtları ile ilgili bilgi güvenliği ve mahremiyeti uygulamalarını değerlendirmelerine göre istatistiksel olarak anlamlı fark göstermektedir.	X	
H2b3	Hasta hakları ve kişilik haklarında eğitim almalarına göre istatistiksel olarak anlamlı fark göstermektedir.	X	
H2b4	KVKK hakkında daha önceden eğitim almalarına göre istatistiksel olarak anlamlı fark göstermektedir.	X	
H3	Sağlık Çalışanlarının KVK-HSBDÖ ve alt boyutları ile elektronik sağlık kayıtlarının güvenlik ve mahremiyeti standartlarına uyumu düzeyleri ölçeği ve alt boyutları arasında istatistiksel olarak anlamlı bir ilişki vardır.	X	

4. TARTIŞMA ve SONUÇ

Hastanelerde hastaların tıbbi gereksinimleri karşılanırken bunların karşılanma sürecinde hasta haklarının gerektirdiği mahremiyet ve bilgilerinin gizliliği faktörünün ön plana çıktığı görülmektedir. Bu önemli faktörün korunmasını sağlayacak yegâne kişi sağlık personelidir. Sağlık personeli tedavi süreci boyunca hasta bilgilerine direkt olarak ulaşabilmektedir ve bunları gerektiğinde üçüncü kişilerle paylaşabilmektedir. Bu paylaşımlar ve hastanedeki bilgilerinin sistemsel olarak güvenliğinin incelenmesi hukukun da ilgi alanına girmektedir. Hasta bilgilerinin güvenliğinin sağlanması konusunda sağlık çalışanlarının farkındalığını ve elektronik sağlık kayıtlarının mahremiyeti hakkındaki tutumlarını değerlendirmek amacıyla gerçekleştirilen bu çalışma, hastaların bu gizli alanlarına dahil olan bilgilerinin neden korunması gerektiğine hukuk ve sağlık yönetimi perspektifinden bakılmasını sağlamıştır.

Bu tez çalışmasında Kişisel Verilerin Korunması Kanunu'nun yanı sıra anayasal düzenlemeler, kamu hukuku ve özel hukuk ayrımı ve uluslararası hukukî düzenlemeler de ele alınmıştır.

Bu araştırma, Kırıkkale ilinde hizmet vermekte olan 700 yataklı bir kamu hastanesinde görev yapan sağlık çalışanlarıyla yürütülmüştür. Araştırmaya katılan sağlık çalışanlarının yaş ortalaması 33,83; meslekte çalışma süresi ortalaması 11,25 yıl; bu kurumdaki çalışma süresi ortalaması 6,5 yıl; Elektronik sağlık kaydı kullanımı deneyim süresi ortalaması 7,31 yıldır. Araştırmada katılımcılar içinde, bilgi güvenliği ve mahremiyeti konularında eğitim almış olanların oranı %72,8; Kurumunun elektronik sağlık kayıtları ile ilgili bilgi güvenliği ve mahremiyeti uygulamalarını kısmen yeterli, elektronik sağlık kayıtları ile ilgili güvenlik açıkları olduğunu düşünenlerin oranı %49,9; hasta hakları ve kişilik hakları konusunda herhangi bir eğitim almış olanların oranı %63,9; Kişisel Verilerin Korunması Kanunu Kapsamındaki Hukukî Sorumluluklarına ilişkin herhangi bir eğitim almış olanların

oranı %59,8'dir. Bu tez çalışmasında 6698 sayılı Kişisel Verilerin Korunması Kanunundan oluşturulmuş ifadelerden oluşan anket formu geliştirilmiştir. Sağlık çalışanlarının bu ifadelere verdiği yanıtlara ilişkin değerlendirmeler ve tartışmalar aşağıda yer almaktadır.

Araştırmaya katılan sağlık çalışanlarının %86,8'i üniversite mezunudur. Çalışanların çoğunluğu, %63,9'u hasta haklarıyla ilgili eğitim aldığını doğrularken yine aynı, %59,8 oranında daha spesifik bir konu olan kişisel verilerin korunması hakkında herhangi bir eğitim almadığını ifade etmiştir. Araştırmaya katılan sağlık çalışanlarının %41'i kurum içerisinde de tıbbi bilgilerin korunması ve hasta verisi mahremiyetinin tamamıyla korunduğunu düşünmektedir.

Bu tez çalışmasında elektronik sağlık kayıtları ve bilgi güvenliği hakkında daha önceden eğitim alınması ile ilgili soru %72,8 oranında "evet aldım" cevabı verilmiştir. Bu soru genel bir soru olup kişinin gerek eğitim hayatında gerekse hizmet içi eğitimlerinde ele alınan bir konu olduğundan cevabın yüksek olduğu düşünülmektedir. Çalışmada özellikle kişilik hakları hakkında herhangi bir eğitim alınmasına ilişkin soruya verilen olumsuz yanıtın fazla olmasının nedeninin çalışanların bu konunun aslında bilgi gizliliği ve mahremiyeti ile ilişkili olduğunu bilmediğinden ya da ilişki kuramadığından kaynaklandığı düşünülmektedir. Çünkü mahremiyet ve bilgi güvenliği ile ilgili eğitim aldığını düşünen personel sayısı %72 den fazla iken kişilik hakları ile ilgili herhangi bir eğitim alınmasına ilişkin soruy evet yanıtı yalnızca %49,9'dur. Özkan 2018 yılındaki benzer çalışmasında özel hayata ve aile hayatına saygı konusu ile ilgili sağlık personelinin bilgi eksiği olduğunu, kişisel verilerin korunması ve gizliliğinde yetersiz olduğunu ortaya koyarak hizmet içi eğitimler ve çeşitle eğitimlerle bunun desteklenmesi gerektiğinin sonucuna ulaşmıştır (Özkan, 2018).

Bayındır 2019 yılındaki çalışmasını hasta mahremiyeti ve gizliliği açısından muayene esnasında hekimle beraber gözlem yapan hekimlerin, tıp fakültesi öğrencilerinin ve stajyerlerin ayrıca yakınlarının alınmaması gerektiğini ve konsültasyon notlarının gizlilik ile iletilmesi gerektiğini savunmaktadır, sağlık verisinin korunması ve gizlilik açısından önem arz ettiği düşünülmektedir (Bayındır, 2019).

2019 yılında Resmî Gazete'de yayınlanan Tıp Fakültesi Eğitim Öğretim ve Sınav Yönetmeliği'ne göre *"İntörn doktorluk dönemi, öğrencilik ile tıp doktorluğu arasındaki geçiş dönemi olup tıbbi bilgi ve beceriler, iletişim becerileri ve mesleksel değerleri kullanarak klinik sorunlara çözüm getirme becerisinin geliştirildiği bir süreçtir.*" şeklinde staj yapacak doktor adayları için bir tanımlama getirilmiştir. Sağlık kurumları sağlık hizmetinin yanında eğitim faaliyetlerinin de aktif olarak sürdürüldüğü birer hizmet kurumlarıdır. Hastanın hekime vereceği gizli bilgiler tedavinin ve teşhisin bir parçasıdır, bu nedenle hekimle beraber gözlem yapan stajyer hekimlerin hasta tarafından paylaşılan bilgileri duyması ihtimali her zaman olacaktır. Her ne kadar hastanın bilgilerinin korunması için yanındaki stajyer hekim ve diğer sağlık personelinin muayene esnasında odadan çıkartılması istenilse de hastalar yataklı servislerde koğuş düzeninde yan yana yatmaktadır ve hastalarla ilgili değerlendirmeleri diğer hastaların duyması da başlı başına bir sorundur. Hastanelerin fiziki şartları Türkiye standartlarında mahremiyetin korunması için yeterli izolasyon sağlaması mümkün değildir. Hasta temel hak ve hürriyetlerinin odada bulunan gözlemciler tarafından ihlal edildiğini fark ettiği anda kişilik hakkının ihlâl edilmesinin son bulmasını talep etme hakkı bulunmaktadır.

Bu tez çalışmasında "hastalar … kişilik haklarının ihlalinin son bulmasını talep edebilir" maddesine %62,8 oranında evet cevabı verilmiştir. Hastalar kişilik haklarının son bulmasını talep edebilir ama bu günümüz koşullarında her zaman mümkün olmayacaktır. Yukarıda da bahsedildiği gibi ihlaller her zaman ve her koşulda olmaya devam etmektedir. Örneğin hasta muayene esnasında bile kişilik hakları ihlaline uğruyor olabilir. Bu da hastaların yan yana yatmak zorunda kaldığı odalar da veya başka koşullarda gerçekleşebilir. Belki de poliklinikte muayene olurken kapının önünde bekleyen diğer hastalar tarafından da ihlale uğruyor olabilir. Bu önlemleri almak kurumun sorumluluğundadır fakat fiziki şartlardan ve çalışma koşullarından dolayı mutlak bir mahremiyetten bahsetmek mümkün değildir.

Bu tez çalışmasında "Kişinin e-nebız verilerine ulaşmasında hekime yetki vermesi tüm çalışanlara yetki vermesi anlamına gelir" ifadesinin doğru olduğunu düşünen sağlık çalışanları toplam örneklemin %78,1'ini oluşturmaktadır. Buradaki önemli ayrım tüm ekip derken tüm hastanenin kastedilmemesidir. Bu ifade "hekimle beraber

kişinin sağlık hizmetinin yürütülmesinde birebir görev alan sağlık personeli" olarak algılanmalıdır. Çünkü tüm hastanenin yetki alması ilgisiz kişilerin yetkisiz erişimini oluşturacaktır.

Araştırmamızda elde edilen sonuçlar; sağlık çalışanlarının yarıdan fazlasının (%53,6) "hastaya ait kişisel verilerin silinmesinin yalnızca kurumun ihtiyacının ortadan kalmasıyla olacağını" düşündüğünü göstermiştir. Kişilerin kurumlardan sağlık verisinin silinmesi ya da değiştirilmesi taleplerinin nasıl değerlendirileceği, 6698 sayılı kişisel verilerin korunması kanununun 7. maddesine göre açıkça düzenlemiştir.

Dolayısıyla her türlü kişisel verinin kurumdan silinmesi istenebilir ancak, kurum tarafından bu isteğin yerine getirilmesi özel şartlara bağlıdır. Diğer özel nitelikli kanunlarda ve yönetmeliklerde düzenlenen kurallarda göre silinme talebi değerlendirilmelidir. Dolayısıyla bir daha hatırlanmayacak şekilde silinme işle yalnızca kurumun ihtiyacının kalmasıyla değil kişinin talebi doğrultusunda da gerçekleşir. Bu tez çalışmasında sağlık çalışanlarının bu konudaki düşüncelerinin çoğunlukla "yanlış" olduğunu göstermiştir.

Bu tez çalışmasında hastalara ait sağlık verisinin korunmasıyla kişilik haklarının kısmen de olsa korunduğunu düşünen sağlık personeli sayısı %96,2 olduğu belirlenmiştir. Sağlık verileri nitelikleri dolayısıyla KVKK m.6'da bahsedilen özellere haiz olduğundan korunma gerçekleştiği halde kısmen de olsa kişilik haklarının korunacağından bahsedebilmektedir

Çalışanların %92,6'sı hastalara ait verilerin tümüyle kişisel verileri oluşturduğunu düşünmektedir. Özkan'ın 2020 yılında yaptığı çalışmada kişisel verilerin tanımlaması ile ilgili bir eleştirisi bulunmaktadır. Kişisel veri kavramının çok geniş yorumlandığı ve daha dar yoruma tabii tutulması gerektiğini ifade etmektedir. Kanunda hangi verilerin kişisel veri olacağı şekilde sınırlılığın getirilmemiş olmasının bu sorunun kaynağı olduğunu ifade etmektedir (Özkan, 2020). Bu hususta kişiye ait her türlü verinin belirli bir kişiyle ilişkilendirilebilir olması önem arz etmektedir. Çünkü kişisel veri bir kişiye ait olanı ifade eder. Hastalara ait hangi verilerin kişisel veri olduğunu belirlemek gerekmektedir.

Bu araştırmada hastanın örtünme tercihleri gibi dışarıdan bakıldığında tespit edilebilen bilgileri kişisel veri sayılmaz maddesine katılımcıların %80'i katılıyorum cevabını vermiştir. Kişiyle ilişkilendirebilecek veriler kişisel veri kategorisine girmektedir. Örtünme tercihlerinin hangi durumlarda kişiyle ilişkilendirilebileceği her durumda/olayda ayrıca değerlendirilmelidir. Burada dikkati çekmek istenen farklılık, örtünme tercihinin herkes tarafından dışarıdan görünebilir olmasıdır. Çünkü kişisel verilerin korunması kurumunun internet sitesi kaynağı tanımına göre kişinin giyinme tarzı hakkındaki veri, aleni veriyi oluşturur. Kurum aleni veri için " *ilgili kişinin kendisi tarafından alenileştirilmiş olması"* tanımını yapmıştır. Alenileştirme verinin kişinin kendisi tarafından kamuoyuna açıklanması olarak tanımlanırken bu amacı güden faaliyetlerini de alenileştirme olarak görülmesi gerekmektedir. Bu nedenden dolayı dışarıdan bakıldığında fark edilen bir örtünme ya da giyinme tercihi her zaman kişisel veri olarak kabul edilmemelidir. KVKK madde 5 kişinin kılık kıyafetinin de kişisel veri sayılabileceğini ifade etmiştir. Oğuz'un 2018 yılında yaptığı çalışmada kılık, kıyafet ve örtünme tercihlerinin doğası gereği dışarıya açık veri olmasından dolayı KVKK m.5 ile çelişkiler yaratabileceğini savunmuştur. (Oğuz, 2018). Bilir, aleni veri için kişinin alenileştirme iradesinin olmasının yeterli olacağını ifade etmiştir (Bilir, 2021). Bu karşıt görüşlerin doğrultusunda dışarıdan bakıldığında fark edilen bir örtünme tercihinin kişisel veri olarak her koşulda kabul edilmesi tartışma konusudur.

Katılımcıların %44,3'ü "hasta verilerinin saklanmasında süre kısıtı yoktur, süresiz arşivlenir" ifadesine "evet" yanıtı verirken, %29,8 fikrim yok yanıtını vermişlerdir. Kurumların verileri arşivleme süresi olmalıdır. Kurumlar verileri süresiz arşivlenemez. Makul bir süre olmalıdır ve bu durum kurumdan kuruma değişiklik göstermektedir. 6698 sayılı KVKK m. 4/2 de genel ilkeler kapsamında verinin amacına uygun sürede muhafaza edilmesinin silinmesinin ise 7. Maddedeki anonimleştirme ya da yok edilme ile yapılması gerektiğini hükmetmiştir.

Bu aşamada anonimleştirme problemi ortaya çıkmaktadır. Görülmektedir ki teknolojinin gelişimi ile verilerin anonimleşmesi oldukça güç hale gelmektedir. Kişilerin doğumundan itibaren gerek devlet kaynaklarında gerekse diğer kurumların arşivlerinde kişiler hakkında uçsuz bucaksız veriler kaydedilmektedir. Orak'ın

çalışmasına göre "anonimleştirmenin" olmadığı görülmektedir ve bu tez çalışmasında anonimleştirmenin sözde bir anonimleştirme olduğu, bunun da adını "pseudonymisation" olduğu vurgulanmaktadır (Orak, 2019). Bu tez çalışmasında bir verinin herhangi bir kişiyle ilişkilendirilemeyecek hale getirilmesinin verinin anonimleşmesi olduğu düşünen personel oranının %88,5 olduğu tespit edilmiştir ve bu oranın yüksek olduğu belirlenmiştir.

Bir başka anonimleştirme problemi ise anonimleştirelerek paylaşılan hasta verilerinden kaynaklanmaktadır. Hoşnut 2019 yılında yaptığı çalışmada hastalarıyla ilgili sosyal medya üzerinden hastanın ismi gibi tanımlayıcı bilgilerini paylaşmadan eğlendirici, güldürücü gönderi paylaşan sağlık personelinin hastalar için psiko-sosyal yıkıntı oluşturabileceklerini ifade etmiştir (Hoşnut, 2019). Hoşnut (2019)'un tarif ettiği durumda hastaya ait her türlü veri dış dünyadan gizlense bile, ilgili kişinin paylaşımı gördüğü an kendisinden bahsedildiğini anlaması kişisel verilerde mümkün olmayan bir tam anonimleşme sorununu doğurmaktadır.

Katılımcıların %88,8'i "Sağlık personeli hastaya ait bilgileri hastayla kan bağı olan herkese açıklayabilir" ifadesine katılmadığını belirtmiştir. Katılanların oranı ise %4,6'dır. Kişinin birisiyle kan bağı bulunması için aynı çekirdek ailesinden olması gerekmemektedir. Örneğin 3. dereceden akrabası olan amca, hala, teyze gibi yakınlıklarda da kan bağı bulunmaktadır. Kişilerle ilgili yapılacak açıklama da önceliğin kim olacağı iyi tespit edilmesi gerekecektir. Ayrıca bilgilendirme için kişisel verilerin korunması göz önünde bulundurulmalıdır. Örneğin cinsel yolla bulaşan bir hastalığa sahip bir kişinin, bu durumu kendisinden başka kimsenin bilmemesini istemesi normaldir. Kişiyi zora sokacak bilgiler kişinin onayı olmadan ya da kişi kendisi paylaşmadan asla paylaşılmamalıdır.

Araştırmada kullanılan bir diğer ifade ise; "hastanın hayatı, beden bütünlüğü söz konusu ise ve acil bir durum söz konusu rıza aranmaksızın kişisel veriler kullanılıp işlenebilir" ifadesidir. Katılımcıların %88,5'i bu ifadeye "katılıyorum" yanıtını vermiştir. Sağlık kurumları sunduğu hizmetin yapısı gereği birtakım olayların kendiliğinden gelişmesi ve aciliyeti karşısında hedef kitlesi hakkında karar almanın sıkça gerçekleştiği kurumlardır. Sağlık hizmetleri ertelenemeyecek kadar aciliyet gerektirebilir. Kişinin hayatı söz konusu olduğunda bilgilendirme yapacak kişi bir

değerlendirmede bulunmalıdır. Yapacağı bilgilendirmenin faydası kişiye vereceği zarardan daha fazla ise bilgilendirme yapılmalıdır. Bu durum için literatürde daha çok anayasa hukuku alanına giren "pratik uyuşum" kavramı kullanılmaktadır. Burada yarışan değerler söz konusudur, bunlarda birisi "bilgi edinme hakkı" diğeri de "özel hayatın gizliliği"dir. Bu değerlerden hangisinin kullanılması kişi açısından önem arz ediyorsa, gereğinin ona göre yapılması hukuka aykırılık teşkil etmeyecektir (Keskinsoy ve Kaya, 2021).

Araştırmaya katılan sağlık çalışanlarının %84'ü "ihtiyacı olmadığı halde hasta verisine erişen sağlık personeli hak ihlâli yapmıştır" ifadesine katıldığını belirtmiştir. Virginio ve Ricarte (2015)'te yaptıkları çalışmada hasta güvenliğini sağlamak için yetkisiz erişime karşı nasıl bir kontrol yöntemi geliştirileceğini araştırmışlardır. Alt yapı sorunlarının yanı sıra kullanıcıların eğitimi de bir eksiklik olarak fark edilmiştir. Bu nedenle hasta güvenliğinin sağlanması sadece teknik bir sorun değil sosyo-teknik bir gerçek olduğu görülmüştür (Virginio ve Ricarte, 2015). Sağlık çalışanlarının yanı sıra hastaların da kişisel verilerin korunması hakkında net bir bilgisi olmadığı düşünülmektedir.

KVKK ile ilgili bilgi düzeyinin ölçülmesinde kullanılan ifadelerden "hasta yanlış girilmiş verilerin düzeltilmesini talep ederlerken doğacak masrafları kendisi temin etmek zorundadır" ifadesi ters ifade edilmiştir. Katılımcıların %63,9'u bu ifadeye katılmadığını belirtmiştir. 6698 sayılı KVKK ilgili kişinin hakları bölümünde madde 11 içerisinde bu konuyu düzenlemiştir. KVKK m.11/1 d bendinde "*Herkes, veri sorumlusuna başvurarak kendisiyle ilgili kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme hakkına sahiptir"* ifadeleri geçmektedir. Kişi yanlış girilmiş kişisel verisinin düzeltilmesini talep ederse doğacak masrafları ödemeyecektir eğer ki masraf ödendiyse ödenen miktarın kişiye tazmin edilmesi gerekmektedir.

Bilgi düzeyini ölçekte kullanılan bir diğer ifade ise; "Hastaların kişisel verileri bilimsel amaçlar için kullanılacaksa açık rıza alınmadan da kullanılabilir" ifadesidir. Katılımcıların %80,2'si bu ifadeye "katılıyorum" cevabını vermiştir. 6698 sayılı KVKK madde 28 de Kanun hükümlerinin hangi koşullarda uygulanamayacağı bölümünde açıkça düzenlenmiştir. KVKK Madde 28/1 c bendi " … *Kişisel verilerin*

millî savunmayı, millî güvenliği, kamu güvenliğini, kamu düzenini, ekonomik güvenliği, özel hayatın gizliliğini veya kişilik haklarını ihlal etmemek ya da suç teşkil etmemek kaydıyla, sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında işlenmesi … kanun hükmü kapsamı dışındadır." şeklinde düzenlenmiştir. İncinin 2015 yılında çalıştığı bilimsel yayın etiğine göre etik olmadan bilimin olmayacağı vurgulanmıştır. Çünkü etik biliminin temel ilkeleri arasında başkalarının hayatına saygı önem arz etmektedir ve esastır. Ayrıca başkalarının hayatına saygı duymanın yanı sıra dürüstlük, açık, insan onurunun korunması, güven ve saygı bilim yaparken önemini korumaktadır (İnci, 2015).

Sağlık çalışanları kişisel verilerin korunması konusunda son derece dikkatli olmalıdır hasta-sağlıkçı arasındaki güvenin tam merkezinde bir konumdalardır. Yasal düzenlemelere rağmen usulsüz hasta verilerinin paylaşılması söz konusudur. Her ne kadar sağlık çalışanları sağlık verisinin üçüncü kişilerle paylaşılmaması gerektiği anket çalışmamızda %88,8 oranında doğru cevaplamış olsa da uygulamada hatalarla karşılaşılmaktadır. Bunun nedeni hastane ortamın kendisine has bir kaotik ve aciliyet gerektiren özelliğinin bulunması olabilir. Akçakoca'nın 2021 yılındaki çalışmasında hastaların diğer sağlık çalışanları ile paylaşmasını bile istemediği verilerin hekimle daha rahat paylaşabildiğini ve hekimin bunu diğer kişiler ve sağlık personeliyle usulsüz paylaşımının nitelikli hal olduğunu ve daha ağır cezalarla korunması gerektiğini savunmaktadır (Akçakoca, 2021).

Öğrenildiği durumlarda kişinin mağdur olmasına ya da ayrımcılığa maruz kalmasına neden olan verilere "Özel Nitelikli Kişisel Veriler"dir. Katılımcıların %92,1'i bu konuyu değerlendirmek üzere kullanılan "sağlık verileri özel nitelikli verilerdir" ifadesine katılıyorum yanıtı vermiştir. KVKK' da yer alan madde 6/1 "*Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi … gibi verileri özel nitelikli kişisel veridir."* ifadesi ile özel nitelikli verilere tanımsal bir açıklama yapmıştır. Hukuk kuralları emreci, yorumlayıcı ve tanımlayıcı şekilde yazılmaktadır. Kanun maddesinde terimlerinde açıklaması yapılmaktadır. Bununla beraber anonim veri, biyometrik veri gibi terimlerin de tanımları yapılmıştır. Anonim veri hakkında katılımcılara yöneltilen "Anonim veri herhangi bir kişi ile ilişkilendirilemeyecek verilere denir. Buna göre; hastanın yüzü çekilmeden vücut parçasının fotoğrafını

çekmek anonim veriyi oluşturur" ifadesine katılımcıların %88,5'i katılıyorum yanıtını vermiştir. Biyometrik veri hakkında bilgiyi ölçmek için yönetilen "Kişinin teşhis edilmesini sağlayan verilere Biyometrik veriler denir. Hastanın biyometrik verileri gereklilik kalksa bile muhafaza edilmelidir" ifadesine ise "katılıyorum" yanıtı veren sağlık çalışanları çoğunluktadır (%89,9).

Katılımcılar "Sağlığa ilişkin veriler yurtdışına aktarılırken ülkede geçerli olan kişisel verilerin korunması prosedürlerine gerek kalmaz" ifadesine %80,9 oranında "katılmıyorum" yanıtını vermiştir. 6698 Sayılı KVKK kişisel verilerin yurtdışına aktarılması bölümü madde 9 Hükümleri ile kişisel verilerin sadece yurtiçi değil yurtdışına çıkarılırken de tam bir koruma altına alınmasını hedeflemektedir.

Kurumlar kişisel verilerin korunması için bir takım fiziki ve teknik önlemleri almak zorundadır. KVKK kanun maddesi 12/1 c bendinde kuruma sorumluluk yüklemektedir. Burada veri sorumlusu ile veri işleyen kişiler arasındaki farkı belirlemek gerekmektedir. Her veri işleyen kişi veri sorumlusu olmamaktadır. Veri sorumlusu genellik kurumun idaresinden sorumlu kişilerden oluşmaktadır.

Bu çalışmada KVK-HSBDÖ katılımcıların katılım düzeyi en yüksek olan ifadeler aşağıdaki gibidir.

- *Çalışılan kurumlarda elektronik sağlık kayıtlarının güvenliğini temin etmek amacıyla gözle görülür bir liderlik sağlanmalıdır.*
- *Çalıştığım kurumda elektronik sağlık kayıtlarının güvenlik ve mahremiyetini sağlamak için gerekli olan politika, prosedür, eğitim, şifreleme ve erişim sınırlamaları gibi iç kontrol mekanizmaları mevcuttur*
- *Çalıştığım kurumda bilgi güvenliği politikaları veya prosedürleri kolaylıkla anlaşılabilir ve erişilebilir durumdadır.*

Bu ifadeler ile katılımcıların örgütte, kurum içerisinde bilgi güvenliğinin korunması ve sürdürebilirliği açısından çalışmaların varlığı ve kurum tarafınca birtakım değerlerin korunması için özen gösterildiğini düşündüklerini yansıtmaktadır. Kurum içerisinde bir farkındalık mevcuttur ve elektronik hasta kayıt sistemine girişler için

şifreleme olmak üzere birtakım önlemler alınmaktadır. Araştırmanın yürütüldüğü hastanenin kullandığı; Altiva yazılımı hastane bilgi yönetim sistemi IP adresi denetimiyle çalışmaktadır ve her kullanıcı kendi adı ve şifresiyle sisteme giriş yapabilmektedir. Kişiler sadece tanımlı bilgisayarlardan ve uygulamalardan giriş yapabilmektedir, dışarıdan erişimler ise denetime tabidir. Böylece yetkisiz ve ilgisiz kullanım ihtimali en düşüğe getirilmesi hedeflenmektedir. Literatürde elektronik sağlık kayıtlarını için kullanılan sistemlerde en çok ihtiyaç duyulan düzenlemenin kullanılabilirlik ve veri güvenliği olduğu vurgulanmaktadır (Hoerbst ve Ammanwerth, 2010). Güvenlik, gizlilik ve veri koruma açık ara en önemli gereksinimdir. Veriler yetkisiz ve ilgisiz kullanımların ifşasına karşı yeterince korunmalıdır. Bu yüzden kimlik doğrulama faaliyetleri bu açıdan önemli rol oynar (Hoerbst & Ammanwerth, 2010). Ancak yine de bazı çalışmalarda "acil durumlarda bilgi güvenliği politikalarının ihlâl edilmesinin, eğer hayati bir risk varsa aşılabilir şeyler olduğu belirtilmektedir. Fernàndeze vd. (2012)'ne göre söz konusu insan hayatıysa erişimle ilgili prosedürler atlanır, fakat bunun için de kurumun bir acil durum planı olmalıdır ve bu ihlâli haklı gösteren nedenleri önceden belirlemelidir (Fernández-Alemán, Señor, Lozoya, Toval, 2012).

Bu tez çalışmasının amaçlarından birisi sağlık çalışanlarının "Kişisel Verilerin Korunması" ile ilgili hukukî sorumluluklarına ilişkin bilgi düzeylerini ölçmektir. Analizlerden elde edilen sonuçlar; sağlık çalışanlarının kişisel verilerin korunması ile ilgili hukukî sorumluluklarına ilişkin bilgi düzeylerinin oldukça "yüksek" seviyede (ort: 0,87 ± 0,173; min:0,20-max:1,00) olduğunu göstermiştir. Araştırmaya katılan sağlık çalışanları, KSVK-HSBD Ölçeğin alt boyutlarından sırasıyla "verilerin işlenmesi ile ilgili sorumluluklar" (ort: 0,91 ± 0,194; min:0,00-max:1,00), "verilerin saklanması, yok edilmesi ve aktarılması" (ort: 0,91 ± 0,208; min:0,00-max:1,00), "veri sahibinin hakları" (ort: 0,86 ± 0,220; min:0,00-max:1,00) ve "kişisel sağlık verisi farkındalığı" (ort: 0,86 ± 0,220; min:0,00-max:1,00) puanlarını almışlardır. Boyutlar içinde en düşük ortalama "kişisel sağlık verisi farkındalığı" alt boyutundan elde edilmiştir. Araştırmaya katılan sağlık çalışanlarının KVK-HSBD ölçeğinden elde ettikleri puan ortalamalarının; unvan, cinsiyet, Elektronik Sağlık Kayıtları (ESK) kullanma deneyimleri ve kurumdaki ESK güvenlik ve mahremiyet uygulamaları konusundaki değerlendirme durumlarına göre istatistiksel olarak

anlamlı fark gösterdiği belirlenmiştir (p<0,05). Ayrıca KVK-HSBD ölçeği puan ortalamalarının, katılımcıların ESK bilgi güvenliği ve mahremiyeti; hasta hakları ve kişilik hakları ve KVKK kapsamındaki hukuki sorumlulukları konularında eğitim alma durumlarına göre anlamlı farklılıklar gösterdiği tespit edilmiştir (p<0,05).

Bu tez çalışmasında değerlendirilen bir diğer konu ise; elektronik sağlık kayıtlarının güvenliği ve mahremiyeti konusundur. Elektronik hasta kayıtları ile ilgili güvenlik endişeleri her zaman bulunmaktadır. Elektronik sağlık kayıtları öz nitelikleri itibariyle iyileştirmeye açık bir potansiyeli bulunmaktadır. Klinisyenlerin kullanımındaki sorunları gidermek, kurum kültürü oluşturmak ve iş akışlarındaki sorunları çözümlemek bunlardan bir kaçıdır. Bunu yapmak içinde kurumda liderlik faaliyetinin olması gerekmektedir. Çünkü kurum öncelikle güvenlik sorununun olduğunun farkına varıp bunu ortaya koymak için öz değerlendirme yapmalıdır (Sittig, Ash ve Sigh 2014).

Bu tez çalışmasının bir diğer amacı ise; sağlık çalışanlarının elektronik sağlık kayıtları güvenlik ve mahremiyeti standartlarına uyum düzeylerini değerlendirmektir. Analizlerden elde edilen sonuçlar; sağlık çalışanlarının Elektronik Sağlık Kayıtları Güvenlik ve Mahremiyeti Standartlarına Uyum Ölçeğinden yüksek düzeyde puanlar elde ettiğini göstermiştir (ort: 3,99 ± 0,220; min:1,89-max:5,00). Katılımcılar, ESK-GMSU Ölçeğinin alt boyutlarından sırasıyla "güvenlik ve mahremiyet politikaları" (ort: 4,00 ± 0,69; min:1,88-max:5,00), "örgütsel güvenlik" (ort: 3,97 ± 0,650; min:1,80-max:5,00), "eğitim ve güvenlik uygulamaları" (ort: 3,99 ± 0,70; min:1,80-max:5,00) puanlarını almışlardır. Araştırmaya katılan sağlık çalışanlarının ESK-GMSU ölçeğinden aldıkları puanların ise; onların yaş, eğitim düzeyi, unvan ve meslekte çalışma yılı özelliklerine göre istatistiksel olarak anlamlı farklılıklar gösterdiği belirlenmiştir (p<0,05). Yine katılımcıların ölçekten aldığı puan ortalamalarının; elektronik sağlık kayıtlarında bilgi güvenliği ve mahremiyeti konusunda, hasta hakları ve kişilik hakları konusunda ve KVKK kapsamındaki hukuki sorumlulukları konusunda eğitim alma durumlarına göre istatistiksel olarak anlamlı farklılıklar oluşturduğu tespit edilmiştir (p<0,05).

Elde edilen sonuçlar özellikler sağlık çalışanlarında ilgili konularda eğitim alma durumumun ESK Güvenlik ve mahremiyeti standartlarına uyum konusunda anlamlı farklılıklar oluşturduğu belirlenmiştir. Bu sonuçlara göre eğitimin önemini bir kere ön plana çıkmıştır. Konu ile ilgili olarak Karabayır (2022), tarafından Karabük'te sağlık bilimleri öğrencileri ile gerçekleştirilen "kişisel sağlık verileri ve mahremiyeti" araştırmasında; öğrencilerin yasal veri paylaşımı, kişisel veriler ve veri bilgisine dair tutumları "orta derecede" olduğu sonucuna ulaşmıştır. Sağlık personeli olmaya aday kişilerin ve sağlık personelinin mahremiyeti koruma konusunda kritik öneme sahip olurken, bu konudaki bilgi düzeylerinin yetersiz olduğu sonucuna ulaşmıştır. Katılımcıların özellikle yasal süreç ve prosedür hakkında bilgi sahibi olmadıklarını belirlemiştir (Karabayır, 2022). Türkiye'de gerçekleştirilen başka bir araştırmada ise; 1. ve 2. Basamak sağlık hizmetinin sunulduğu kurumlarda 45 yaşının üstündeki sağlık personelinin elektronik sağlık uygulamalarına kabul ve hazır olma durumlarının 3. Basamak sağlık kurumlarında çalışan diğer yaş gruplarına kıyasla düşük olduğunun sonucuna ulaşmıştır (Gündoğdu, 2022).

Sağlık Çalışanlarının Elektronik Sağlık Kayıtları Güvenlik ve Mahremiyet Standartlarına Uyum Ölçeği ve alt boyutlarında unvana göre değerlendirme yapıldığında özellikle hekim grubu; bilgi güvenliği anlayışı, mahremiyet politikalarına uyumu, örgütsel güvenlik bilinci ve mahremiyet standartlarına uyumları diğer meslek gruplarına göre daha düşük istatistiksel ortalama puanı elde etmiştir. Bunun sebebi hekimlerin birincil olarak mesleki kaygı güdüp diğer etkenleri göz ardı etmesinden kaynaklanıyor olabilir. Bu yüzden hekimlerin kişisel veri farkındalığı ve mahremiyet bilincinin gelişimi için bir takım koruyucu önlemler alınması gerekebilir. Bu önlemler yaptırım olarak değil durumun ciddiyetini anlamalarını sağlayacak eğitim faaliyetlerinden oluşabilir. Belki Tıp Fakültelerinin Tıp etiği dersinin içeriğine eklenecek konularla bu zenginleştirilebilir belki de direkt sağlık hukuku dersleri ile öğrencilikten farkındalık kazanılması için zemin oluşturulabilir.

Ayrıca elde edilen sonuçlar hemşire, sağlık memuru ve ebe unvanına sahip sağlık çalışanlarının ise KVK-HSBD Ölçeği alt boyutlarından "verilerin işlenmesi, kişisel verilerin farkındalığı ve veri sahibinin hakları" konusunda kurumdaki diğer sağlık

profesyonellerine göre daha düşük ortalamalara sahip olduklarını göstermiştir. Özellikle bu meslek gruplarında görev yapan sağlık çalışanları, hastanın kabulünden taburculuğuna kadar tedavi sürecinin içinde olduğu için KVK'nın getirdiği hukuki sorumluluklar konusundaki bilgi düzeyin düşük olması hem kurumsal hem de bireysel problemleri beraberinde getirecektir. Bu durum hemşirelerin ve ebelerin meslek eğitimi alırken hukukî sorumlulukları konusunda eğitim verilmemesi ya da yoğun iş hayatlarında bu hususları daha geri planlara atmak zorunda kalmalarından kaynaklanıyor olabilir. Literatürde benzer şekilde, sağlık çalışanlarının eğitim seviyesinin artıkça hukuki sorumluluklarını daha iyi bildiği ve dolayısıyla farkındalıkları da arttığı tespit edilmiştir (Karabakır ve Çetin, 2016). Ayrıca bahsedilen çalışmada hemşirelerin çoğunun yasal mevzuatı veya prosedürü bilmediği ya da yetersiz olduğu belirlenmiştir (Karabakır ve Çetin, 2016).

Bu tez çalışmasında 3 yıl ve daha az süreli ESK kullanma tecrübesi olan çalışanların; verilerin saklanması, aktarılması ve yok edilmesi açısından istatistiksel ortalaması diğer çalışanlara göre ortalamalarından düşük çıkmıştır. 3 yıldan daha fazla süredir elektronik sağlık kayıtlarını kullanma tecrübesi olan sağlık personeli yüksek çıkmasının sebebi hizmet içi eğitimlere denk gelme ihtimalinin daha yüksek olması veya çalışma esnasındaki sorunları birebir yaşayıp, tecrübe etmeleri dolayısıyla yaşayarak çözüm bulmalarıyla ilişkilendirilebilir. Keçeli'nin de çalışmasında bahsettiği gibi tecrübe bir bilgi birikimidir. Bilgi birikimleri aslında öğrenme sürecini şekillendiren ve tetikleyen temeldir. Sistematik olmayan istemeden öğrenme durumu kişiler konuları tecrübe edindikçe öğrenmeyi beraberinde getirecektir (Keçeli, 2018). Bu bilgi ışığında şu sonuca varılabilir. 3 yıldan daha fazla ESK kullanan sağlık çalışanları sürekli tekrarlayan günlük işlerinde öğrenme amacı gütmeden tecrübeyle bilgi sahibi olmaktadırlar

Paksoy'un 2019 yılında yaptığı araştırma da ESK-GMSUÖ kullanılmıştır. Ölçeği dal hastanesi ve genel hastane ayrımıyla uygulayan Paksoy iki hastane grubu arasında anlamlı farklılık ($p=0,002<0,05$) olduğu görmüştür. Yaş ortalamalarının yüksek olduğu gruplar ile ESK eğitimi alma durumuna göre bireylerde alt boyutlarda istatistiksel puan artışının olduğunun sonucuna ulaşmıştır. Ayrıca çalışmasında cinsiyete göre "örgütsel güvenlik" alt boyutunda anlamlı farklılık ($p=0,042<0,05$)

olduğunun sonucuna ulaşmıştır (Paksoy, 2019). Bu bulgular bu tez çalışmasından elde edilen sonuçlarla benzerlik göstermektedir.

Son olarak bu tez çalışmasında; sağlık çalışanlarının kişisel verilerin korunması ile ilgili hukukî sorumluluklarına ilişkin bilgi düzeyleri ile elektronik sağlık kayıtları güvenlik ve mahremiyeti standartlarına uyum düzeyleri arasında istatistiksel olarak anlamlı bir ilişki olup olmadığı incelenmiştir. Analizler sonucunda; sağlık çalışanlarının kişisel verilerin korunması ile ilgili hukukî sorumluluklarına ilişkin bilgi düzeyleri ile elektronik sağlık kayıtları güvenlik ve mahremiyeti standartlarına uyum düzeyleri arasında pozitif yönlü zayıf bir ilişki (r=0,192; p=0,000) belirlenmiştir. Kısacası, sağlık personelinin kişisel verilerin korunması kapsamındaki hukuki sorumluluklarına ilişkin bilgi düzeylerinin arttırılması, hastanelerdeki ESK bilgi güvenliği ve mahremiyeti standartlarına uyum sağlamalarını artıracaktır. Konu ile ilgili literatür incelendiğinde; hukuki bilgi düzeyleri yeterli seviyede olan sağlık çalışanlarının kişisel verilerin korunması, mahremiyet gibi özel yaşamın gizliliği ilgilendiren konularda daha dikkatli davrandıkları ve farkındalıklarının yüksek olduğu gösterilmiştir (Arslan ve Demir, 2017). Ayrıca Erdem ve Akgün'ün (2018), yapmış olduğu araştırmada hasta hakları yönetmeliğini konusunda bilgi düzeyi yüksek sağlık çalışanlarının, hukuki sorunlarla karşılaşma durumunun daha az olduğu ve mahremiyet ve bilgi güvenliği ile ilgili standartlara uyumlarını artırdığını belirtilmiştir (Erdem ve Akgün, 2018). Bu bulgulara göre sağlık personelinin hukuki metinleri okuması ve bireysel farkındalık oluşturmasıyla hem hedef kitlesi hem de kendisi için kişisel verilerin korunması konusu ile mahremiyet konuları için fark yaratabileceği sonucuna varılmaktadır. Son olarak güncel hukuki metinlerin takibi ve bu metinlere uyum, sağlık personelinin çalışırken kendisini ve hastaları hukuki olarak korumaya almasını sağlayabilecektir. Bağlayıcılığı bulunan hukuki düzenlemelerin takibi kişisel verilerin yoğun işlendiği sağlık kurumlarında önem arz etmektedir.

5. ÖNERİLER

İnsanlar maddi ve manevi varlığını koruma hakkına sahiptir bu nedenle sağlık hakkı yaşam hakkının gereğidir. Sağlıklı olmak sunulan sağlık hizmetine bağlıdır (Arslan ve Demir, 2017). Sağlık hakkından hareketle kişi sadece sağlık açısından değil ruhsal ve sosyal açıdan da tam bir iyilik halinde olmalıdır. Bu nedenle sağlıkla ilgili aldıkları haklardan ve korumalardan tam olarak yararlanmalarına özen gösterilmelidir (Öztürk, 2018). Hastaya ait olan sağlık verilerinin ilgili olmayan kişiler tarafından öğrenilmesi halinde hastanın karışılacağı sorunlar kaçınılmazdır. Çünkü mahremiyet şeref ve haysiyetle ilgidir. İnsan maddi haklara sahip olurken şeref ve haysiyet haklarına da sahiptir ve koruma altındadır. Mahremiyete özen göstermenin ahlaki bir yönü de bulunmaktadır. Hastanın mahremiyetini korurken hasta hakkında eleştiri, dedikodu yapmak da mahremiyete zarar verecektir (Şen, 2015).

Mahremiyetin sağlanması için mahremiyet hakkında eğitimler verilmesi gerekmektedir. Bu tür eğitimler yalnızca yetişkinlere değil çocukluktan itibaren verilmiş olması gerekmektedir. Çünkü mahremiyet eğitimi bir süreçtir. Toplumda haklarını bilen ve koruyan, öz denetimi yapabilen, başkalarının hayatında saygı duyan, düşüncelerini özgürce ifade edebilen bireyler için çocukluktan eğitimin temeli atılmalıdır (Özaslan ve Akduman, 2018). Akıllı sağlık uygulamalarında alınacak önlemlerde ise teknolojinin gereklerine uygun önlemlerin ilgili uzmanların alması gerekmektedir. Çünkü akıllı sağlık uygulamaları geleneksel tip sağlık hizmetlerinin yetişemediği alanlarda da hizmet vermektedir. Güvenlik ve mahremiyet her zaman öncelikli korunması gereken bir değer olmalıdır (Kopmaz ve Aslanoglı, 2018).

Sağlık mesleği mensupları kişisel verilerin korunması ve mahremiyeti açısından eğitilmeli ve eksiklikleri giderilmelidir. Tıp fakültelerine ve diğer sağlık meslekleri yetiştiren fakültelerin eğitim müfredatlarına Sağlık Hukuku dersleri eklenerek eğitim aşamasında farkındalık oluşturulabilir. Meslek etiğinin korunmaması sonucunda hem

maddi hem de manevi yönden zarar görüleceği mesleğin ilk başından anlatılmalıdır (Dülger, 2015). Bu araştırmada hemşire, ebe ve sağlık memuru grubunun kişisel veriler ve ilgili kanun hakkındaki bilgi eksikliği konusunda fark oluşturmaktadır. Özellikle hasta ile çok yakın temas halinde olan bu meslek grubunun yasal mevzuatı bilmesi önem arz etmektedir. Bu bilgilerin lisans eğitiminde verilmesi mezuniyet sonrası işe başlanıldığında çalışırken kolaylık ve güven sağlayacaktır. Sağlık hukuku dersleri verilirken ders veren kişilerin sağlıktaki problemlere ve hukukî boyuta aynı anda hâkim olması da önerilmektedir (Durmuş, 2020).

KAYNAKLAR

1. Acar, D. Ş. (2010). Kişilik Hakkı İhlâllerinde Cevap ve Düzeltme Hakkı, Doktora Tezi, *Marmara Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul
2. Ağıralan, E., & Yiğit, Y. (2015). Bilgi Güvenliği, Kişisel Verilerin Korunması ve Mahremiyet Etki Değerlendirmesi. Yüksek Lisans Tezi. *Polis Akademisi Güvenlik Bilimleri Enstitüsü*, Ankara
3. Akar Y., Özyurt, E., Erduran, S., Uğurlu, D., & Aydın, İ. (2019). Hasta Mahremiyetinin Değerlendirilmesi. *Sağlık Akademisyenleri Dergisi*, *6*(1), 18-24.
4. Akçakoca, M. (2021). Tıp Ceza Hukukunda Kişisel Sağlık Verilerinin Korunması, *Erciyes Üniversitesi Sosyal Bilimler Enstitüsü* Doktora Tezi. Kayseri
5. Akkurt, S. S. (2020). Kişisel Sağlık Verilerinin İşlenmesine ve Covid-19 Pandemisi Sürecinde Mobil Uygulamalarla Paylaşılmasına Hukukî Bir Bakış. *İstanbul Ticaret Üniversitesi Sosyal Bilimler* Dergisi, 19(38), 142-160.
6. Aktaş, D., & Baykara, Z. G. (2020). Stomalı Bireylerde Hassas Bir Konu: Mahremiyet. *Gazi Sağlık Bilimleri Dergisi*, *5*(3), 8-15.
7. Alçin, A. A. 2022, Türk Hukukunda Kişisel Sağlık Verileri ve İdarenin Kişisel Sağlık Verilerini Koruma Yükümlülüğü. *Türkiye Adalet Akademisi Dergisi*, (51), 365-410.
8. Ali, A. S., Zaaba, Z. F., & Singh, M. M. (2023). Privacy During Epidemic Of Covıd-19: A Bibliometric Analysis. *Bulletin Of Electrical Engineering And Informatics*, *12*(1), 587-596.
9. Ali, M., Naeem, F., Tariq, M., & Kaddoum, G. (2022). Federated

Learning For Privacy Preservation İn Smart Healthcare Systems: A Comprehensive Survey. *IEEE Journal of Biomedical and Health İnformatics*.

10. Alpar, R. (2003). Uygulamalı Çok Değişkenli İstatistik Yöntemler, Detay Yayıncılık Dördüncü Baskı.
11. Akıncı, A. N. (2017). *Avrupa Birliği Genel Veri Koruma Tüzüğü'nün getirdiği yenilikler ve Türk hukuku bakımından değerlendirilmesi: Çalışma raporu-6*. T.C. Kalkınma Bakanlığı.
12. Arslan, E. T., & Demir, H. (2017). Sağlık Çalışanlarının Hasta Mahremiyetine İlişkin Tutumu: Nitel Bir Araştırma. *Bolu Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *17*(4), 191-220.
13. Aslanyürek, M. (2016). İnternet ve Sosyal Medya Kullanıcılarının İnternet Güvenliği ve Çevrimiçi Gizlilik ile İlgili Kanaatleri ve Farkındalıkları. *Maltepe Üniversitesi İletişim Fakültesi Dergisi*, *3*(1), 80-106.
14. Aşıkoğlu, Ş. İ. (2019). Veri Sorumlularının Aydınlatma Yükümlülüğü-Avrupa Birliği ve Türk Hukukunda. *Kişisel Verileri Koruma Dergisi,* 1(2), 41-65.
15. Atalay, H. N. (2021). Mahremiyet Kapsamında Kişisel Sağlık Verilerinin Korunması ve Depolanması. *Journal of Academic Perspective on Social Studies*, (1), 1-20.
16. Aydin, A. G. V. (1998). 1982 Anayasası Çerçevesinde Özel Hayatin Gizliliğinin Korunması. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 3*(3). 185-198
17. Baran, S., & Şener, E. (2018). Hastanelerde Bilgi Güvenliği Yönetimi: Nitel Bir Araştirma. *Süleyman Demirel Üniversitesi Vizyoner Dergisi*, *10*(23), 108-125.
18. Barrows Jr, R. C., & Clayton, P. D. (1996). Privacy, Confidentiality, And Electronic Medical Records. *Journal of The American Medical Informatics Association*, *3*(2), 139-148.

19. Başara, G. T. (2020). Kişisel Veri İşleme Sözleşmesi. *Uyuşmazlık Mahkemesi Dergisi*, (16), 57-90.

20. Bayindir, H., (2019) Özel Sağlık Kurumları Kapsamında Kişisel Sağlık Verilerinin İşlenmesi ve Korunması. Yüksek Lisans Tezi. *İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.* İstanbul

21. Bayraklı, V., & Güvenoğlu, E. (2013). Medikal Görüntülerde Doktor-Hasta Bilgi Gizliliğinin Sağlanması. *Akademik Bilişim 2013 – XV. Akademik Bilişim Konferansı Bildirileri* 23-25.

22. Bayraktar, M. (2022). Kişisel Sağlık Verilerinin İşlenmesi ve Korunması Doktora Tezi, *Marmara Universitesi Sosyal Bilimler Enstitüsü*. İstanbul

23. Bezirgan Gözmener, S. (2019). Kişisel Sağlık Verilerinin Kayıt ve Korunmasında Hemşirelerin Cezai Sorumluluğu, Yüksek Lisans Tezi, *Dokuz Eylül Üniversitesi Sağlık Hukuku Program*ı İzmir

24. Bilir, F. (2021). Kişisel Verilerin Korunması Kişinin Kendisinin Korunmasıdır. *TRT Akademi Dergisi*, *6*(11), 172-181.

25. Braun, Ö.Ü.C.A. (2021). Kişisel Verilerin Korunmasında Hukukî Sorunlar. *Yeditepe Üniversitesi Hukuk Fakültesi Yayını.* 139-140

26. Büken, N. Ö., & Ünsal, Ç. Z. Kişisel Verilerin Korunması Kanununun Biyomedikal Alana Yansımaları Açısından Değerlendirilmesi. *Hacettepe Hukuk Fakültesi Dergisi*, 7(2), 33-54.

27. Büyükay, Y. (2004). Hekimin Sır Saklama Yükümlülüğü. *Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi*, 8(1-2),

28. Campanella, P., Lovato, E., Marone, C., Fallacara, L., Mancuso, A., Ricciardi, W., & Specchia, M. L. (2016). The Impact of Electronic Health Records On Healthcare Quality: A Systematic Review and Meta-Analysis. *The European Journal of Public Health*, *26*(1), 60-64.

29. Candan, M., & Bilgili, N. (2018). Hemşire ve Ebelerin Hasta Mahremiyetine İlişkin Görüşlerinin Değerlendirilmesi. *Gazi Sağlık Bilimleri Dergisi*, *3*(3), 34-43.

30. Çelikçöp Ç. Yarar, O. (2019). Kalite Yönetim Direktörlerinin Bilgi

Güvenliği Farkındalığı: İstanbul İli Örneği. *Sağlıkta Performans ve Kalite Dergisi*, *17*(2), 29-48.

31. Çiftlik, E. E., Ünal, E., Özkan, S., Kesgin, V., Durmuş, M. K., Dinç, H., &, Ö. (2013) *Bir Eğitim ve Araştırma Hastanesinde Bilgi Güvenliği Politikaları. IV Uluslararası Sağlıkta Performans ve Kalite Kongresi Sözel Bildiriler* 233. Nisan
32. Çobansoy, G. (2020). İnsan Hakları Açısından Kişisel Verilerin Korunması Sorunu Yüksek Lisans Tezi. *Maltepe Üniversitesi, Sosyal Bilimler Enstitüsü.* İstanbul
33. Deniz, M. Ö. (2022). Sağlık Verilerinin İşlenmesinde Aydınlatma Yükümlülüğü. *Erciyes Akademi,* 36(3), 1424-1445.
34. Döner, A. (2022). Bilgi Edinme Hakkının Sınırı Olarak Özel Hayatın Gizliliği ve Kişisel Veriler. *Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi*, 26(1), 23-60.
35. Durmuş, V. (2021). Kişisel Sağlık Verilerinin Korunmasında İdarenin Hukukî Sorumluluğu. *Dokuz Eylül Üniversitesi Hemşirelik Fakültesi Elektronik Dergisi*, 14(1), 67-76
36. Dülger, M. V. (2015). Sağlik Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti (Protection Of Personal Data In Health Law And Patient Privacy). *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi* 1 (2), 43-80.
37. 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), 101-167.
38. Dülger, M. V. (2018). İnsan Hakları ve Temel Hak ve Özgürlükler Bağlamında Kişisel Verilerin Korunması. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 5*(1),71-144.
39. Elbir, N. (2020). Kişiliğinin Korunması Bağlamında İşçiye Ait Kişisel Verilerin Korunması. Doktora Tezi, *Ankara Üniversitesi Sosyal Bilimler*

Enstitüsü, Ankara

40. Erdem, Ö., & Akgün, H. S. (2018). Hasta ve sağlık çalışanlarının, hasta hakları konusunda bilgi düzeyleri: bir müdahale çalışması. *Sakarya Tıp Dergisi*, *8*(3), 518-524.
41. Erdinç, G. H. (2020). Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi. *Kişisel Verileri Koruma Dergisi,* 2(1), 1-19.
42. Ergüden, A. Ç. (2020). Kişisel Sağlık Verilerinin İşlenmesi. İstanbul Barosu.
43. Ergül, O. (2015). Sporda Zorunlu Tahkim-Bireysel Başvuru İlişkisi:' Yargı Denetimi Dışında Birakilan İşlemleri'dar Yorumlamak Mümkün Değil Mi?. *Anayasa Yargisi,* 31(1), 67-78.
44. Eriş, H., Havlioğlu, S., & Doni, N. (2017). Kalite Sistemi ve Bilgi Güvenliği Sistemlerinin Hasta Güvenliği Üzerine Etkisi: Bir Üniversite Hastanesi Uygulaması. *Sağlık Akademisyenleri Dergisi, 4*(3), 207-215.
45. Eroğlu, T. (2011). Özel Hayatın Gizliliğini İhlal Suçu (Tck m.134) Doktora Tezi. *Marmara Üniversitesi Sosyal Bilimler Enstitüsü.* İstanbul
46. Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security And Privacy In Electronic Health Records: A Systematic Literature Review. *Journal of Biomedical Informatics, 46*(3), 541-562.
47. Frakt, A. B., & Carroll, A. E. (2013). The Quality Imperative: A Commentary On The Us Healthcare System. *American Journal of Preventive Medicine, 44*(1), 22-26.
48. Godard, B., Hurlimann, T., Letendre, M., & Egalité, N. (2006). INHERIT BRCAs. *Guidelines For Disclosing Genetic İnformation To Family Members: From Development To Use. Fam Cancer, 5*, 103-116.
49. Gostin, L. O., Halabi, S. F., & Wilson, K. (2018). Health Data And Privacy in The Digital Era. *JAMA*, 320(3), 233-234.

50. Gökçay, B., & Arda, B. (2019). Kişisel Sağlık Verilerinin Korunması Kapsamında Sağlık Araştırmalarında Etik Bakış. *Türk Kardiyoloji Derneği Arşivi*, 47(3), 218-227.

51. Göktaş, B., Ömer, R. Ö., Duran, M., Şakar, S., Yılmaz, M., Güler, S. & Özdemir, G. (2017). Türkiye'de Sağlık Bilgi Sistemleri Üzerine Bir Araştırma. *Ankara Sağlık Bilimleri Dergisi,* 6(1), 125-138.

52. Gül, Ş, Kuzuca, İ. G., & Arda, B. (2019). Sınırlı Bir Çalışma: Hekim ve Hemşirelerin Gözünden Psikiyatri ve Etik. *Sürekli Tıp Eğitimi Dergisi*, *28*(4), 281-289.

53. Gülhan, O. (2022). Kişisel Sağlık Verileri Kapsamında Veri Öznesinin Erişim Hakkı. *Uluslararasi Akademik Birikim Dergisi, 5*(5). 279-280

54. Gülmüş, M. (2011). Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği. Yüksek Lisans Tezi. *Yıldız Teknik Üniversitesi.* İstanbul

55. Gündoğdu, G. (2022). Türkiye'nin E-Sağlığa Hazırbulunuşluk Düzeyinin Belirlenmesi Doktora Tezi. *Fırat Üniversitesi Sağlık Bilimleri Enstitüsü.* Elazığ.

56. Gündüz, F. E., & Yazicioğlu, İ. (2021). Bilgi Edinme Hakkı Çerçevesinde Kişisel Verilerin Korunması. *Anayasa Yargisi*, 38(1), 171-204.

57. Gündüz, N., & Altıntaş, S. Hasta Mahremiyetine Yönelik Sağlıkta Kalite Standartlarının Hastane Çalışanları Üzerinde Algılarının Ölçülmesi. *Sağlıkta Performans ve Kalite Dergisi*, *16*(1), 11-30.

58. Gür, B. A. (2018). Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması. *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştirmaları Dergisi*, *25*(2), 850-872.

59. Gürbüz, M. (2015). Kişilik Hakki Açısından Tıbbi Genetik Analizler Yüksek Lisans Tezi. *Anadolu Üniversitesi Sosyal Bilimler Enstitüsü.* Eskişehir

60. Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N., & Müller, G. (2011). Aspects Of Privacy For Electronic Health Records. *International*

Journal of Medical Informatics, 80(2), 26-31.

61. Habip, Oğuz. (2013). Elektronik Ortamda Kişisel Verilerin Korunması, Bazı Ülke Uygulamaları ve Ülkemizdeki Durum. *Uyuşmazlik Mahkemesi Dergisi*, (3), 1-38.
62. Hoerbst, A., & Ammenwerth, E. (2010). Electronic Health Records. *Methods of Information In Medicine*, *49*(04), 320-336.
63. Hoşnut, Y. (2019) Mahremiyet Bağlamında Kişisel Sağlık Verilerinin Korunması: Çorum İli Kamu Hastaneleri Örneği Yüksek Lisans Tezi. *Gazi Üniversitesi Sosyal Bilimler Enstitüsü,* Ankara
64. İleri, Y. Y., & Uludağ, A. (2017). E-Nabız Uygulamasının Yönetim Bilişim Sistemleri ve Hasta Mahremiyeti Açısından Değerlendirilmesi. *Uluslararası Sağlık Yönetimi ve Stratejileri Araştırma Dergisi*, *3*(3), 318-325.
65. İmançlı C. (2019) Kişisel Sağlık Verilerinin Korunamamasından Doğan Özel Hukuk Sorumluluğu Yüksek Lisans Tezi. *İstanbul Üniversitesi Sosyal Bilimler Enstitüsü* İstanbul.
66. İnci, O. (2015) Bilimsel Yayın Etiği. *Türk Kütüphaneciliği Dergisi* 29, 2 , 282-295.
67. İstek, A. (2016). Hasta Mahremiyeti Kapsamında Kişisel Veri. *Akademik Teklif Hukuk ve İdari Bilimler Dergisi*, 3(5), 182-215.
68. Kaissis, G. A., Makowski, M. R., Rückert, D., & Braren, R. F. (2020). Secure, Privacy-Preserving and Federated Machine Learning In Medical Imaging. *Nature Machine Intelligence*, *2*(6), 305-311.
69. Kandilli, E. (2019). Sağlik Hukukunda Etik Açisindan Kişisel Veriler ve Mahremiyet Hakkı Yüksek Lisans Tezi , *İstanbul Üniversitesi Sosyal Bilimler Enstitüsü).* İstanbul
70. Karaarslan, E., Ergin, A. M., Turğut, N., & Kılıç, Ö. (2015). Elektronik Sağlık Kayıtlarının Gizlilik ve Mahremiyeti. *20. Türkiye İnternet Konferansı* 7-8
71. Karabayır Demir, E. (2022). Karabük Üngversitesi Sağlık Bilimleri

Fakültesi Öğrencilerinin Kişisel Sağlık Verilerinin Kayıt ve Korunmasına İlişkin Tutumlarının Belirlenmesi, Yüksek Lisans Tezi. *Karabük Üniversitesi Sağlık Bilimleri Enstitüsü.* Karabük.

72. Karaca-Dedeoğlu, A. (2019). Uluslararası Sağlık Turizminde Hastanın Özel Hayatının Gizliliği ve Mahremiyetinin Korunması Hakkı. *Opus International Journal of Society Researches*, 10(17), 1875-1910.

73. Karadağ, M. & Abuhanoğlu, U. H. (2015). Sosyo-Kültürel Özelliklerin Bilgi Güvenliği Farkındalığı Üzerine Etkisi: Gülhane Askeri Tıp Fakültesi Eğitim Hastanesinde Bir Çalışma. *The Journal of Academic Social Science Studies 379-386*

74. Karabakır, B., & Çetin, G. (2016). Hemşirelerin tabi oldukları mevzuat ve hukuki sorumlulukları konusundaki farkındalıkları. *Adli Tıp Bülteni, 21*(2), 78-85.

75. Karadaş, N. (2019). Tıp Hukukunda Kişisel Verilerin Açıklanması Suçu, Yüksek Lisans Tezi. *İnönü Üniversitesi Sosyal Bilimleri Enstitüsü*. Malatya

76. Kaya, C. (2011). Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi. *Journal of Istanbul University Law Faculty*, 69(1-2), 317-334.

77. Keçeli, S. (2018). Çalışan Perspektifinden Örgütsel Öğrenme Yeteneğinin Görev ve Bağlamsal Performansa Etkisi: Sağlık Sektöründe Bir Uygulama. Doktora Tezi. *Haliç Üniversitesi Sosyal Bilimler Enstitüsü*. İstanbul

78. Keshta, I., & Odeh, A. (2021). Security and Privacy of Electronic Health Records: Concerns and Challenges. *Egyptian Informatics Journal*, *22*(2), 177-183.

79. Keskinsoy, Ö., & Kaya, S. B. (2021) Anayasa Mahkemesi Kararlarını Biçimlendirme Çabası Olarak Yorum. *Hacettepe Hukuk Fakültesi Dergisi, 11*(1), 63-105.

80. Kılıçarslan, N., Yılmaz, F. T., & Tarım, M. (2012). Hasta Haklarının

Sağlık Çalışanları Tarafından Algılanması. *Sağlıkta Performans ve Kalite Dergisi*, *3*(1), 47-62.

81. Kılınç, D. (2012). Anayasal Bir Hak Olarak Kişisel Verilerin Korunması. *Ankara Üniversitesi Hukuk Fakültesi Dergisi*, 61(3), 1089-1172.

82. Koç, F. (2021). İş İlişkisinde Kişisel Sağlık Verilerinin Işlenmesi. Yüksek Lisans Tezi. *Marmara Universitesi Sosyal Bilimler Enstitüsü.* İstanbul.

83. Koçak, H., & Memiş, K. (2018). Bilgi Toplumunda Korku: Bilgi Güvenliği ve Risk Toplumu. *Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi*, 20(3), 1-10.

84. Konca, N. K., & Badur, E. Avukatın Müvekkilinin Kişisel Sağlık Verilerine Erişimine İlişkin Değerlendirmeler. *Selçuk Üniversitesi Hukuk Fakültesi Dergisi,* 31(1), 195-230.

85. Kopmaz, B., & Arslanoğlu, A. (2018). Mobil Sağlık ve Akıllı Sağlık Uygulamaları. *Sağlık Akademisyenleri Dergisi*, *5*(4), 251-255.

86. Korkmaz, A. (2014). İnsan Hakları Bağlamında Özel Hayatın Gizliliği ve Korunması. *Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomik Araştirmalar Dergisi* (3), 99-103.

87. Kutlu, Ö., & Kahraman, S. (2017). Türkiye'de Kişisel Verilerin Korunması Politikasının Analizi. *Siyaset, Ekonomi ve Yönetim Araştırmaları Dergisi*, *5*(4), 45-62.

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

89. Küzeci, E., & Kılıç, Ş. (2019). 6698 Sayılı Kişisel Verilerin Korunması Kanunu'nun İş Sözleşmesi Çerçevesinde Değerlendirilmesi: Veri Sorumlusu, Veri İşleyen ve Diğer Aktörler. *Legal İş Hukuku ve Sosyal Güvenlik Hukuku Dergisi*, 16(63), 947-992.

90. Mandl, K. D., & Perakslis, E. D. (2021). HIPAA and the Leak of" Deidentified" EHR Data. *The New England Journal of Medicine*,

384(23), 2171-2173.

91. Mannhardt, F., Koschmider, A., Baracaldo, N., Weidlich, M., & Michael, J. (2019). Privacy-Preserving Process Mining: Differential Privacy For Event Logs. *Business & Information Systems Engineering*, *61*, 595-614.

92. Marşap, A., Akalp, G., & Yeniman, E. (2010). Sağlık İşletmelerinde İnsan Kaynağının Kurumsal Bilgi Güvenliği Kültürü Gelişimi. *Bilişim Teknolojileri Dergisi*, *3*(1). 31-35

93. Mcgraw, D., & Mandl, K. D. (2021). Privacy Protections To Encourage Use Of Health-Relevant Digital Data in A Learning Health System. *Npj Digital Medicine*, *4*(1), 2.

94. Menachemi, N., & Collum, T. H. (2011). Benefits and Drawbacks Of Electronic Health Record Systems. *Risk Management and Healthcare Policy*, 47-55.

95. Oğuz, S. (2018). Kişisel Verilerin Korunması Hukukunun Genel İlkeleri. *Bilgi Ekonomisi ve Yönetimi Dergisi*, 13(2), 121-138.

96. Ong, R. Y. C., & Sabapathy, S. (2020). Enhancing Patient Privacy Protection Under Hong Kong's Electronic Health Record Sharing System. *Common Law World Review*, *49*(1), 4-30.

97. Orak, B. (2019). Kişisel Sağlık Verilerinin Korunması, Yüksek Lisans Tezi. *Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü.* Ankara.

98. Orman, H. (2019). Doğum Sürecinde Mahremiyet Algısının Anne Memnuniyetine Etkisi Doktora Tezi *Sağlık Bilimleri Enstitüsü Marmara Üniversitesi* İstanbul

99. Öget, A. M. (2020). Kişisel Sağlık Verilerinin Korunmasında Özel Sağlık Kuruluşlarının Sorumluluğu. *İzmir Barosu Dergisi,* 85(3), 189-260.

100. Öğüz, T. & Dural, M. 2021. Filiz Kitabevi, *Türk Özel Hukuku Cilt II Kişiler Hukuku*

101. Özaslan, G. (2019). *Bilgi Güvenliği ve Mahremiyetin Korunmasına Yönelik Eğitimin Etkilerinin Değerlendirilmesi: Bir Özel Hastane Uygulaması* Doktora Tezi,

102. Özaslan, H., & Akduman G, G,. (2018,). Ailelerin Mahremiyet Eğitimine İlişkin Görüşlerinin İncelenmesi. In Set Conference Index In System (3), 1363-1369

103. Özata, M., & Özer, K. (2017). Sağlık Çalışanlarının Hasta Mahremiyeti Konusundaki Tutumlarının İncelenmesi. *Hacettepe Sağlık İdaresi Dergisi*, *20*(1), 81-92.

104. Özcan, S. (2018). Sigorta Hukuku Bağlamında Kişisel Sağlık Verilerinin Korunması. Yüksek Lisans Tezi *Kadir Has Üniversitesi Sosyal Bilimler Enstitüsü*, İstanbul

105. Özdamar, Kazım. *Modern Bilimsel Araştırma Yöntemleri: Araştırma Planlama, Toplum ve Örnek Seçimi, Güç Analizi, Proje Hazırlama, Veri Toplama, Veri Analizi, Bilimsel Rapor Yazımı*. Kaan Kitabevi, 2003.

106. Özdemir, H. (2009). Haberleşmenin Gizliliği ve Kişisel Veriler. *Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi*, 13(1-2), 285-303.

107. Özdemir, H. (2010). Hadim Etme ve Hekimin Sir Saklama Yükümlülüğü. *Ankara Haci Bayram Veli Üniversitesi Hukuk Fakültesi Dergisi*, 14(1), 125-164.

108. Özdemir, M., Yılmaz, M., & Hakan, Kaya (2022). Kişisel Sağlık Verilerinin 6698 Sayılı Kanun Çerçevesinde Korunması. *19 Mayıs Sosyal Bilimler Dergisi*, *3*(1), 85-96.

109. Özdemir, Y. M. (2014). Anayasa Mahkemesi Kararlari Işığında 1982 Anayasasi'nda Sınırlama Kaydı İçermeyen Temel Hak ve Özgürlüklerin Sınırlanması. *Anayasa Hukuku Dergisi*, 3(5), 413-442.

110. Özer, K. (2015). Sağlık Kuruluşlarında Hasta Mahremiyeti Uygulamalarının ve Sağlık Çalışanlarının Hasta Mahremiyetine Yönelik Tutumlarının İncelenmesi (Konya Örneği), Yüksek Lisans Tezi, *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü,* Konya.

111. Özkan, F. (2018). Kişisel Sağlık Verilerinin Korunmasının Pozitif Temelleri ve AİHM Kararlarından Örnekler. Yüksek Lisans Tezi *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü*. İzmir

112. Özkan, O. (2020). Kişisel Verilerin Korunması. Doktora Tezi *Sosyal Bilimler Enstitüsü. Ankara Sosyal Bilimler Üniversitesi* Ankara

113. Özlü, T. (2010). Hasta Hakları Bağlamında Sağlık Finansmanı. *Sağlıkta Performans ve Kalite Dergisi*, *2*(2), 9-20.

114. Öztürk, E. (2018). Cinsel Sağlık ve Üreme Sağlığında Haklar Yüksek Lisans. *İstanbul Medipol Üniversitesi Sosyal Bilimler Enstitüsü.* İstanbul

115. Öztürk, H., Özçelik, S. K., & Bahçecik, N. (2014). Hemşirelerin Hasta Mahremiyetine Özen Gösterme Durumu. *Ege Üniversitesi Hemşirelik Fakültesi Dergisi*, *30*(3), 19-31.

116. Pai, M. M., Ganiga, R., Pai, R. M., & Sinha, R. K. (2021). Standard Electronic Health Record (EHR) Framework For Indian Healthcare System. *Health Services And Outcomes Research Methodology*, *21*(3), 339-362.

117. Paksoy, V. M. (2019). Elektronik Sağlık Kayıtlarının Güvenlik ve Mahremiyet Uygulamalarının Özel Hastanelerde Değerlendirilmesi: Kayseri İli Örneği, Doktora Tezi. *Marmara Üniversitesi Sağlık Bilimleri Enstitüsü.* İstanbul.

118. Price, W. N., & Cohen, I. G. (2019). Privacy In The Age of Medical Big Data. *Nature Medicine*, *25*(1), 37-43.

119. Sabancığulları, S., Açıl, A. A., & Hallaç, S. (2014). Akut Psikiyatrik Bakımda Bir Profesyonel Kontrol Yöntemi: Hemşirelik Gözlemleri. *Psikiyatride Güncel Yaklaşımlar*, *6*(1), 79-91.

120. Sangchul, P. J. (2020). Gina Jeehyun Choi. Information Technology-Based Tracing Strategy In Response To Covıd-19 in South Korea-Privacy Controversies.

121. Sarpatwari, A., Kesselheim, A. S., Malin, B. A., Gagne, J. J., & Schneeweiss, S. (2014). Ensuring Patient Privacy In Data Sharing For

Postapproval Research. *New England Journal of Medicine*, *371*(17), 1644-1649.

122. Selek, O. (2019). Genel Veri Koruma Tüzüğü Işığında Kişisel Verilerin İşlenmesinde Rıza Açıklaması. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi,* 21(2), 911-951.

123. Serengil, Ş. K. (2012). KKTC'de Hasta Hakları. *Ankara Üniversitesi Hukuk Fakültesi Dergisi,* 61(2), 73

124. Sharma, Y., & Balamurugan, B. (2020). Preserving The Privacy Of Electronic Health Records Using Blockchain. *Procedia Computer Science*, *173,* 171-180.

125. Sittig, D. F., Ash, J. S., & Singh, H. (2014). The Safer Guides: Empowering Organizations To Improve The Safety And Effectiveness of Electronic Health Records. *The American Journal of Managed Care*, *20*(5), 418-423.

126. Sultanlı, İ. (2021). Anayasal Bir Hak Olan Kişisel Verilerin Korunması Hakkı ve Mahremiyet ile İlişkisi. *Selçuk Üniversitesi Adalet Meslek Yüksekokulu Dergisi*, *4*(1), 23-34.

127. Şimşek Küçükbasmacı, G. (2022). Sağlık Hukukunda Kişisel Verilerin Korunması ve AB Mevzuatı ile Karşılaştırmalı Olarak Değerlendirilmesi. Yüksek Lisans Tezi. *Ankara Üniversitesi Sağlık Bilimleri Enstitüsü*. Ankara

128. T.C. Sağlık Bakanlığı, (2016). Sağlıkta Kalite Standartları (Diyaliz). *Sağlıkta Kalite ve Akreditasyon Başkanlığı Dergisi*. (1) Ankara

129. Tankül, M., & Ergün, M. A. *Hastane Bilgi Yönetim Sistemlerinin Kişisel Verileri Koruma Kanunu Uyumluluğu'nun Bir Özel Hastanede Değerlendirilmesi: Anket Çalişması. 6. Geleceğin Mühendisleri Sempozyumu* 2-3. Temmuz

130. Taştan, F. G. (2017). Türk Sözleşme Hukukunda Kişisel Verilerin Korunmasi. *On İki Levha. (1)* 11

131. Tavşancıl, E., & Keser, H. (2002). Development of a Likert Type Attitude Scale towards Internet Usage. *Journal of Educational Sciences & Practices*, *1*(1). 80-100

132. Terry, N. P. (2012). Protecting Patient Privacy In The Age of Big Data. *Umkc L. Rev.*, *81*, 385.

133. Turaç, İ. S. (2022). Hemşirelerin Kanıta Dayalı Hemşireliğe Yönelik Tutumları ve Bilgi Güvenliğinin Hasta Güvenliği Kültürü Üzerine Etkisi. Doktora Tezi, *Hacettepe Üniversitesi Sağlık Blimleri Enstitüsü.* Ankara

134. Tyson, P. (2001). The Hippocratic Oath Today. *Nova*, 21(5). 1-2

135. Uysal, B., & Yorulmaz, M. (2018). Sağlıkta Kalite Standartları ve Bilişsel Mahremiyet. *Selçuk Üniversitesi Sosyal ve Teknik Araştirmalar Dergisi*, (16), 24-33.

136. Virginio Jr, L. A., & Ricarte, I. L. M. (2015). Identification of Patient Safety Risks Associated With Electronic Health Records: A Software Quality Perspective. *Medinfo*, 55-59.

137. Wang, T., Pizziferri, L., Volk, L. A., Mikels, D. A., Grant, K. G., Wald, J. S., & Bates, D. W. (2004). Implementing Patient Access To Electronic Health Records Under HIPAA: Lessons Learned. *Perspectives In Health İnformation Management/Ahıma, American Health Information Management Association*, *1*.

138. Xiang, D., & Cai, W. (2021). Privacy Protection and Secondary Use of Health Data: Strategies and Methods. *Biomed Research International*, *2021*, Article Id 6967166.

139. Yıldırım, F.N. (2019). Avrupa Birliği ve Türk Hukukunda Kişisel Verilerin Korunması. Yüksek Lisans Tezi. *Dokuz Eylül Üniversitesi Sağlık Bilimleri Enstitüsü.* İzmir.

140. Yusuf, Şen. (2015). İslâm Hukûkuna Göre Sağlık Hizmetlerinde Mahremiyet Hakkı. *Ekev Akademi Dergisi*, (61), 425-450.

141. Yücedağ, N. (2019). Kişisel Verilerin Korunması Kanunu

Kapsamında Genel İlkeler. *Kişisel Verileri Koruma Dergisi,* 1(1), 47-63.

142. Zaim, H. & Tarım, M. (2011). Hasta Memnuniyeti: Kamu Hastaneleri Üzerine Bir Alan Araştırması. In *Journal of Social Policy Conferences* (59) 1-24.

EK-4. ARAŞTIRMADA KULLANILAN ANKET FORMU

Anket No:

Sayın Katılımcı,

Bu anket formu, Kırıkkale Üniversitesi, Sağlık Bilimleri Enstitüsü, Sağlık Yönetimi Yüksek Lisans programında yürütülen **"Sağlık Çalışanlarının Kişisel Verilerin Korunması Kanunu Kapsamındaki Hukuki Sorumluluklarına İlişkin Bilgi Düzeyleri ve Elektronik Sağlık Kayıtlarının Güvenlik ve Mahremiyet Standartlarına Uyumlarının Değerlendirilmesi"** başlıklı adlı tez çalışmasında kullanılmak üzere hazırlanmıştır. Anket sonucunda elde edilen veriler sadece akademik amaçlar için kullanılacaktır. Kişisel bilgileriniz ile çalıştığınız kuruma ait bilgiler üçüncü taraflar ile paylaşılmayacaktır. Bu nedenle tüm **ifadeleri dikkatle okuyup** sizin için en uygun olanı işaretlemenizi ve yanıtsız soru bırakmamanızı rica ederim. Tamamen gönüllük esasına dayanan bu çalışmaya gösterdiğiniz ilgi ve yardımlarınızdan dolayı teşekkür ederiz. Araştırma esnasında veya araştırma bittikten soma, araştırma hakkında ek bilgiler almak, çalışma ile ilgili herhangi bir sorun ya da diğer rahatsızlıklarınız için 0(554) [redacted] numaralı telefondan veya faikcanyilan@gmail.com e-mail adresinden Faikcan Yılan ile iletişim kurabilirsiniz.

Doç. Dr. Meltem SAYGILI
Kırıkkale Üniversitesi Sağlık Bilimleri Enstitüsü
Sağlık Yönetimi Bölüm Öğretim Üyesi

Faikcan YILAN
Kırıkkale Üniversitesi Sağlık Bilimleri Enstitüsü
Sağlık Yönetimi Yüksek Lisans Öğrencisi

BÖLÜM 1: Kişisel Bilgiler

Lütfen size uygun olan seçeneği kutucuklara 'X' ya da ✓ işareti koyarak belirtiniz.

1. Cinsiyetiniz nedir? ( ) Kadın ( ) Erkek

2. Medeni durumunuz nedir? ( ) Evli ( ) Bekar

3. Yaşınız nedir? (Belirtiniz) ……

4. Eğitim düzeyiniz? Lise ( ) Önlisans ( ) Lisans ( ) Yüksek Lisans ( ) Doktora ( ) Diğer ( )

5. Unvanınız Uzm. Hekim ( ) Prt. Hekim ( ) Hemşire- Ebe-Sağlık Mem. ( ) Sağlık Tekn.(ATT, Lab Tek. Rönt. Tek. vs) ( )

Diğer (Eczacı, Diyetisyen, FTR vs) Tıbbi sekreter ( )

6. Mesleğinizde kaç yıldır çalışıyorsunuz?.....

7. Bu kurumda kaç yıldır çalışıyorsunuz?.....

8. Çalıştığınız birim nedir?.....

9. Elektronik sağlık kaydı kullanımı deneyim süreniz : …….yıl …….ay

10. Elektronik sağlık kayıtları, bilgi güvenliği ve mahremiyeti konularında eğitim aldınız mı? (Hizmetiçi eğitim, sertifika prog…) Evet ( ) Hayır ( )

11. Kurumunuzun elektronik sağlık kayıtları ile ilgili bilgi güvenliği ve mahremiyeti uygulamalarını nasıl değerlendirirsiniz?

Yeterli, bu konuda tüm kurallara uyulmaktadır ( ) Tamamen Yetersiz ( )

Kısmen yeterli, elektronik sağlık kayıtları ile ilgili güvenlik açıkları olduğunu düşünüyorum ( )

12. Hasta hakları ve kişilik hakları konusunda herhangi bir eğitim aldınız mı? (Hizmetiçi eğitim, sertifika prog…) Evet ( ) Hayır ( )

13. Kişisel Verilerin Korunması Kanunu Kapsamındaki Hukuki Sorumluluklarınıza ilişkin herhangi bir eğitim aldınız mı? (Hizmetiçi eğitim, sertifika prog…) Evet ( ) Hayır ( )

Bölüm 2. Sağlık Çalışanlarının Kişisel Verilerin Korunması Kanunu'na İlişkin Bilgi Düzeyi Anketi

	Sağlık Çalışanlarının Kişisel Verilerin Korunması Kanunu'na İlişkin Bilgi Düzeyi Anketi Aşağıda yer alan sorular Kişisel Verilerin Korunması Kanunu'na İlişkin Bilgi Düzeyinizi ölçmeye yöneliktir. Lütfen günlük uygulamalarınız düşünerek bu ifadelere katılım düzeyinizi size en uygun olan seçeneği (X) şeklinde işaretleyerek belirtiniz.	**Katılıyorum**	**Katılmıyorum**	**Fikrim Yok**
1.	Hastalara ait verilerin korunmasıyla hastanın temel hak ve hürriyetleri kısmen korunmuş olur.	1	2	3
2.	Hastaya ait kişisel verilerin korunması kişinin özel hayatının gizliliği ile ilgilidir.	1	2	3
3.	Hastaların ruh sağlığına ilişkin veriler kişisel veriler iken sunulan sağlık hizmetleri ile ilgili bilgiler kişisel verileri oluşturmaz.	1	2	3
4.	Hastaya ait sağlık verileri tümüyle kişisel veri kabul edilir.	1	2	3
5.	Hastaların kişisel verileri bilimsel amaçlar için kullanılacaksa açık rıza alınmadan da kullanılabilir.	1	2	3
6.	Hastanın hayatı, beden bütünlüğü söz konusu ise ve acil bir durum söz konusu rıza aranmaksızın kişisel veriler kullanılıp işlenebilir.	1	2	3
7.	Öğrenildiği durumlarda kişinin mağdur olmasına ya da ayrımcılığa maruz kalmasına neden olan verilere Özel Nitelikli Kişisel Verilerdir. Bu halde sağlık verileri özel nitelikli verilerdir.	1	2	3
8.	Kişinin teşhis edilmesini sağlayan verilere Biyometrik veriler denir. Hastanın biyometrik verileri gereklilik kalksa bile muhafaza edilmelidir.	1	2	3
9.	Hastaların sağlık verileri; kamu sağlığı korunurken veya koruyucu hekimlik uygulamaları kapsamında kullanılacaksa, kişinin açık rızası olmaksızın yetkili kurum ve kuruluşlar tarafından işlenebilir ve aktarılabilir.	1	2	3
10.	Sağlığa ilişkin veriler tıbbi teşhis ve tedavi hizmetlerinin yürütülmesi amacıyla izin aranmaksızın yetkili kurum ve kuruluşlar tarafından işlenebilir ve aktarılabilir.	1	2	3
11.	Sağlığa ilişkin veriler; sağlık hizmetlerinin ve finansmanının planlanması ve yönetimi amacıyla ilgili kişinin açık rızası olmaksızın yetkili kurum ve kuruluşlar tarafından işlenebilir ve aktarılabilir.	1	2	3
12.	Sağlığa ilişkin veriler yurtdışına aktarılırken ülkede geçerli olan kişisel verilerin korunması prosedürlerine gerek kalmaz.	1	2	3
13.	Hastalara ait kişisel veriler bilimsel çalışmalarda ancak ilgili kişilerin özel hayatın gizliliğini ve kişisel haklarını ihlal etmemek şartıyla kullanılabilir.	1	2	3
14.	Kamu kurumunda hastaya ait veriler disiplin soruşturmasında kullanılacaksa ilgili hastadan izin alınması gerekmez.	1	2	3
15.	Hastane çalışanları hastalara ait verilerin saklanmasında her türlü önlemi almak ve alınan önlemi uygulamak zorundadır.	1	2	3
16.	Sağlık personeli hastaya ait bilgileri hastayla kan bağı olan herkese açıklayabilir.	1	2	3
17.	Sağlık kurumlarında veri sorumluları ile verileri işleyen kişilerin, verilerin gizliliği ve paylaşımı konusundaki sorumlulukları görevden ayrıldıktan sonra da devam eder.	1	2	3
18.	Hastaya ait veriler kullanılmadan önce yapılan aydınlatma yetersizse verilerin kullanılması hak ihlalidir.	1	2	3

	Sağlık Çalışanlarının Kişisel Verilerin Korunması Kanunu'na İlişkin Bilgi Düzeyi Anketi (Devam)	**Katılıyorum**	**Katılmıyorum**	**Fikrim Yok**
19.	Aydınlatma yükümlülüğünü yerine getirmeyen veri sorumlusu hakkında para cezası verilebilir.	1	2	3
20.	Hasta yanlış girilmiş verilerin düzeltilmesini talep ederlerken doğacak masrafları kendisi temin etmek zorundadır.	1	2	3
21.	Hasta verilerinin elde edilmesi belirli prosedürlere bağlıyken veriler imha edilirken herhangi bir prosedüre gerek yoktur.	1	2	3
22.	Hasta verilerine ihtiyacı olmadığı halde erişen sağlık personeli hak ihlali yapmıştır.	1	2	3
23.	Hastaların kişisel verilerinin saklanmasında süre kısıtı yoktur süresiz arşivlenir.	1	2	3
24.	Kişisel verilerin kullanılmasında aydınlatma yükümlülüğü fiili imkansızlıklardan dolayı yerine getirilemiyorsa makul süre içerisinde mutlaka yapılması gerekir.	1	2	3
25.	Aydınlatmanın herhangi bir şekli zorunluluğu yoktur. Sözlü, yazılı vb. şekilde gerçekleştirilebilir.	1	2	3
26.	Cinsel sağlık verileri kamu sağlığı korumak için de olsa izin alınmaksızın işlenemez.	1	2	3
27.	Anonim veri herhangi bir kişi ile ilişkilendirilemeyecek verilere denir. Buna göre hastanın yüzü çekilmeden vücut parçasının fotoğrafını çekmek anonim veriyi oluşturur.	1	2	3
28.	Hastaya ait kişisel verinin silinmesi yalnızca kurumun ihtiyacının ortadan kalkmasıyla mümkündür. Kişinin talep etmesi verinin silinmesi için yeterli değildir.	1	2	3
29.	Hastalara ait bilgilerin saklandığı arşivlere yetkisiz giriŞ çıkışların engellenmesi kurumun sorumluluğundadır.	1	2	3
30.	Beyaz kod veren sağlık çalışanları için güvenlik personellerinin hasta bilgilerine hastane sisteminden ulaşılması hak ihlali değildir	1	2	3
31.	Hastanın e-nabız verilerine erişmesi için hekime yetki vermesi hekimle çalışan tüm ekibe yetki vermesi anlamına gelir.	1	2	3
32.	Kişilik hakları ihlal edilen kişi tazminat isteyemez sadece ihlalin son bulmasını talep edebilir.	1	2	3
33.	Hastanın örtünme tercihleri gibi dışarıdan bakıldığında tespit edilebilen bilgileri kişisel veri sayılmaz.	1	2	3
34.	İdare kişisel verileri korumak için tedbirler almak zorundadır. (aykırı kullanım, aykırı erişim, doğru muhafaza)	1	2	3
35.	Kişisel veriler, kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları tarafından (sağlık bakanlığı, sağlık müdürlükleri, hastaneler…) yürütülen önleyici ve koruyucu faaliyetler kapsamında işlenebilir.	1	2	3

Lütfen Bölüm 3'e geçiniz…

Bölüm 3. Elektronik Sağlık Kayıtları Güvenlik ve Mahremiyet Standartlarına Uyum Ölçeği

	Aşağıda yer alan sorular Elektronik Sağlık Kayıtları Güvenlik ve Mahremiyet Standartlarına Uyum Düzeyinizi ölçmeye yöneliktir. Lütfen günlük uygulamalarınız düşünerek bu ifadelere katılım düzeyinizi size en uygun olan seçeneği (X) şeklinde işaretleyerek belirtiniz.	**Kesinlikle Katılıyorum**	**Katılıyorum**	**Kararsızım**	**Katılmıyorum**	**Kesinlikle Katılmıyorum**
1	Çalıştığım kurumda elektronik sağlık kayıtlarının güvenlik ve mahremiyet kurallarına uyumu için önceden tanımlanmış ve kabul görmüş bir uygulama bulunmaktadır.					
2	Çalıştığım kurumda birbirini gözeten ve koruyan bireylerden oluşan yaygın bir bilgi güvenliği kültürü mevcuttur.					
3	Çalıştığım kurumda bilgi güvenliği oluşturmak devamlı bir süreçtir.					
4	Çalışılan kurumlarda elektronik sağlık kayıtlarının güvenliğini temin etmek amacıyla gözle görülür bir liderlik sağlanmalıdır.					
5	Çalıştığım kurumda elektronik sağlık kayıtlarının güvenlik ve mahremiyetini sağlamak için gerekli olan politika, prosedür, eğitim, şifreleme ve erişim sınırlamaları gibi iç kontrol mekanizmaları mevcuttur					
6	Çalıştığım kurumda denetleme yapmak, bilgi güvenliği çalışmalarını geliştirmek için gerekli bir eylem olarak görülmektedir.					
7	Çalıştığım kurumda bilgi güvenliği politikaları veya prosedürleri kolaylıkla anlaşılabilir ve erişilebilir durumdadır.					
8	Çalıştığım kurumda bilgi güvenliği hakkında bireyler arası bilgi alışverişi yapmanın önemli olduğu ifade edilmektedir.					
9	Çalıştığım kurumda personele düzenli aralıklarla bilgi güvenliği politikaları eğitimi verilmektedir.					
10	Çalıştığım kurumda bilgi güvenliği politika ve prosedürleri, değişen örgütsel gereksinimleri karşıladığının değerlendirilmesi amacıyla periyodik olarak gözden geçirilir.					
11	Çalıştığım kurumda bilgi güvenliği politikalarını sıklıkla okumaya gereksinim duyarım.					
12	Çalıştığım kurumda insan zaaflarını kullanarak bilgi aşırma taktiği olarak adlandırılan "Sosyal Mühendislik" konusunda sıklıkla bilgilendirme söz konusudur ve bu taktiklerin sistemim için nasıl hassasiyet yaratabileceğinin farkındayım.					
13	Çalıştığım kurumda hangi bilgilere, ne amaçla erişebileceğimin farkındayım.					
14	Çalıştığım kurumda bilgisayarım üzerinde dışarıdan getirilen taşınabilir belleğin kullanımı için iznim vardır.					
15	Çalıştığım kurumda sistem de kötü amaçlı yazılım bulunduğunda ne yapacağıma dair prosedürlerin farkındayım.					
16	Çalıştığım kurumda benim sorumlu olduğum herhangi bir bilginin yanlış kullanımını veya uygunsuz erişimini bildirmek zorundayım.					
17	Çalıştığım kurumda uymak zorunda olduğum şifreleme politikalarının farkındayım.					
18	Çalıştığım kurumda kabul gören uygun bir bilgi güvenliği davranışı ve tutumu sıklıkla tebliğ edilmektedir.					
19	Çalıştığım kurumda, bilgi güvenliği konularında çalışanların eğitimi için sürekliliği olan bir çaba söz konusudur.					

Sorularımız bitmiştir. Değerli katkılarınız için çok teşekkür ederiz.