FİLİZ BULUT

TIP TARİHİ VE ETİK ANABİLİM DALI DOKTORA TEZİ

2023

T.C.
BURSA ULUDAĞ ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ
ENSTİTÜSÜ
TIP FAKÜLTESİ
TIP TARİHİ VE ETİK
ANABİLİM DALI

SAĞLIKTA BÜYÜK VERİ: ULUSAL DÜZENLEMELER VE VERİ KAYIT SİSTEMLERİNİN TIP ETİĞİ AÇISINDAN İNCELENMESİ

FİLİZ BULUT

(DOKTORA)

BURSA-2023

T.C.
BURSA ULUDAĞ ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ
TIP FAKÜLTESİ
TIP TARİHİ VE ETİK
ANABİLİM DALI

SAĞLIKTA BÜYÜK VERİ: ULUSAL DÜZENLEMELER VE VERİ KAYIT SİSTEMLERİNİN TIP ETİĞİ AÇISINDAN İNCELENMESİ

FİLİZ BULUT

(DOKTORA TEZİ)

DANIŞMAN:

Prof. Dr. Mustafa Murat CİVANER

BURSA-2023

T.C.

BURSA ULUDAĞ ÜNİVERSİTESİ

SAĞLIK BİLİMLERİ ENSTİTÜSÜ

ETİK BEYANI

Doktora tezi olarak sunduğum

"Sağlıkta Büyük Veri: Ulusal Düzenlemeler ve Veri Kayıt Sistemlerinin Tıp Etiği Açısından İncelenmesi" adlı çalışmanın, proje safhasından sonuçlanmasına kadar geçen bütün süreçlerde bilimsel etik kurallarına uygun bir şekilde hazırlandığını ve yararlandığım eserlerin kaynaklar bölümünde gösterilenlerden oluştuğunu belirtir ve beyan ederim.

Filiz Bulut

Tarih ve İmza

TEZ KONTROL ve BEYAN FORMU

12/01/2023

Adı Soyadı: Filiz Bulut

Anabilim Dalı: Tıp Tarihi ve Etik Anabilim Dalı

Tez Konusu: Sağlıkta Büyük Veri: Ulusal Düzenlemeler ve Veri Kayıt Sistemlerinin Tıp Etiği Açıcından İncelenmesi

ÖZELLİKLER	UYGUNDUR	UYGUN DEĞİLDİR	AÇIKLAMA
Tezin Boyutları	■	❑	
Dış Kapak Sayfası	■	❑	
İç Kapak Sayfası	■	❑	
Kabul Onay Sayfası	■	❑	
Sayfa Düzeni	■	❑	
İçindekiler Sayfası	■	❑	
Yazı Karakteri	■	❑	
Satır Aralıkları	■	❑	
Başlıklar	■	❑	
Sayfa Numaraları	■	❑	
Eklerin Yerleştirilmesi	■	❑	
Tabloların Yerleştirilmesi	■	❑	
Kaynaklar	■	❑	

DANIŞMAN ONAYI

Unvanı Adı Soyadı: Prof. Dr. M. Murat Civaner

İmza:

İÇİNDEKİLER

TÜRKÇE ÖZET

Büyük Veri'nin itici gücünü sağlık verileri oluşturmaktadır. Bu verilerin çok büyük miktarlarda işlenebilir olması ve dijital alana aktarılması gibi nedenlerle bu veriler, çeşitli etik sorunları beraberinde getirmiştir. Bu sorunlar mahremiyete yönelik kaygıların ötesinde ahlaki değerlerin dönüşümü, kitlesel gözetim, toplum manipülasyonu ve insan hakları ihlalleri gibi başlıklarda tartışılmaktadır. Ek olarak bu sorunlar çerçevesinde sağlığa erişim, sağlık hakkı, hasta hakkı, sağlıkta mahremiyet ve özerklik, verilerin kötüye kullanılması, ifşa edilmesi ve sağlık hizmetlerinin geleceğinin nasıl şekilleneceği gibi başlıklar da sorgulanmaktadır. Bu tartışmalardan hareketle ülkemizde kişisel sağlık verilerinin korunmasını düzenleyen mevzuatı ve sağlık veri tabanlarını etik açısından inceleyerek bir durum saptamasında bulunmak, Büyük sağlık verisinin yaratabileceği değer sorunları karşısında önemli bir gereksinimdir. Tezin amacı bu gereksinime katkı sağlamak amacıyla kişisel sağlık verilerinin korunmasıyla ilgili ulusal düzenlemelerin ve sağlıkta kullanılan veri tabanlarının neden olduğu etik sorunları saptamak ve bu sorunları meslek ahlakı yükümlülükleri ve insan hakları temelinde önleyecek veya giderecek öneriler geliştirmektir.

Tezde iki aşamalı soyut bir analiz gerçekleştirilmiştir. uluslararası etik kılavuzlarda üzerinde uzlaşı sağlanmış olan toplum yararı, minimum veri, hassas veri, eşitlik ve adalet, özerklik, mahremiyet ve gizlilik ilkeleri bu analize temel oluşturmuştur. Bu bağlamda veriler altı başlık altında gruplandırılmış ve tanımlanmıştır.
Analizin birinci aşamasında Türkiye Anayasası başta olmak üzere kişisel verilerle ilgili kanun, tüzük, yönetmelik, yönerge ve Kişisel Verileri Koruma Kurulu'nun rehberleri olmak üzere toplam 44 düzenleme belirlenmiştir. İkinci aşamada sağlık hizmetleri basamaklarını temsil eden veri tabanları ve mobil sağlık uygulamaları seçilmiştir. Belirlenen bu düzenleme ve veri tabanlarının tanımlanan altı ilke ile ne kadar uyumlu olduğu sorgulanmıştır.

Bu tezde Türkiye'deki kişisel verileri korumayı amaç edinen temel düzenlemeler ve sağlık hizmetlerinde kullanılan veri tabanlarının uluslararası etik kılavuzlarda belirlenen toplum yararı, minimum veri, hassas veri, eşitlik ve adalet, özerklik ile mahremiyet ve gizlilik ilkesi ile uyumlu olmadığı saptanmıştır. Temel bir düzenleme olan Kişisel Verileri Koruma Kanunu'nun 6. maddesinin 3. fıkrası ve 28. madde, bu ilkelerden hiçbiri ile uyumlu olmadığı belirlenmiştir. Özerklik açısından düzenlemelerdeki ve veri tabanlarındaki ortak sorun aydınlatılmış onamla ilgilidir. Veri tabanları ve mobil uygulamalara işlenen hassas veriler ve bu programların uygulanma biçimleri açısından mahremiyet ve gizliliğe ilişkin risk yaratabilecekleri tespit edilmiştir.

Sağlık veri tabanlarına işlenen yarı yapılandırılmış bilgiler, bireyleri kategorilere ayırmak ve sınıflandırmak gibi temel bir işleve sahiptir. Bu işlev, bireyleri hedef olarak belirlemeyi kolaylaştırmaktadır. Dolayısıyla sağlıkta Büyük Veriyle, sağlık verilerinin mahremiyet ve gizliliğini korumak giderek güçleşmekte, ortaya çıkabilecek etik sorunlar çeşitlenmektedir. Bu sorunları önlemek ve gidermek amacıyla uluslararası etik kılavuzlarda altı ilke belirlenmiştir. Bu ilkeler geliştirilmeye ve tartışmaya açıktır. Bu tezde ülkemizde halihazırda veri işleme sürecine dair durumun bu ilkelerle uyumlu olmadığı gösterilmeye çalışılmış ve somut bir şekilde pratikte karşılığı bulunan bu ilkelere uygun yaklaşımların benimsenmesinin başta devletin bir ödevi olduğu vurgulanmıştır.

Anahtar sözcükler: Kişisel sağlık verisi, hassas veri, tıp etiği, özerklik, mahremiyet

İNGİLİZCE ÖZET

Big Data in Health: An Examination of National Regulations and Electronic Health Systems in Terms of Medical Ethics

Health data is the driving force of Big Data. Due to the fact that these data can be processed in large quantities and transferred to the digital field, these data have brought along various ethical problems. These issues are discussed in topics such as transformation of moral values, mass surveillance, manipulation of society and violations of human rights beyond privacy concerns. In addition, within the framework of these problems, titles such as access to health, right to health, patient right, privacy and autonomy in health, misuse and disclosure of data and how the future of health services will be shaped are also questioned. Based on these discussions, it is an important requirement to determine the situation by examining the legislation regulating the protection of personal health data and health databases in terms of ethics in our country, in the face of the value problems that big health data can create. The aim of the thesis is to determine the ethical problems caused by the national regulations on the protection of personal health data and the databases used in health, and to develop suggestions to prevent or eliminate these problems on the basis of professional ethics obligations and human rights.

A two-stage abstract analysis was carried out in the thesis. The principles of community benefit, minimum data, sensitive data, equality and justice, autonomy, privacy and confidentiality, which have been agreed in international ethical guidelines, formed the basis of this analysis. In this context, the data are grouped and defined under six headings.
In the first stage of the analysis, a total of 44 regulations, including the Turkish Constitution, laws, statutes, regulations, directives, and the guides of the Personal Data Protection Board, were determined. In the second stage, databases and mobile health applications representing the health services steps were selected. It was questioned how compatible these regulations and databases were with the six principles defined.

In this thesis, it has been determined that the basic regulations aiming to protect personal data in Turkey and the databases used in health services are not compatible with the principles of community benefit, minimum data, sensitive data, equality and justice, autonomy and privacy and confidentiality determined in international ethical guidelines. It has been determined that paragraph 3 of article 6 and article 28 of the Personal Data Protection Law, which is a basic regulation, is not in compliance with any of these principles. In terms of autonomy, the common problem in regulations and databases concerns informed consent. It has been determined that sensitive data processed in databases and mobile applications and the way these programs are implemented may pose risks to privacy and confidentiality.

Semi-structured information processed into health databases has the basic function of categorizing and classifying individuals. This function makes it easy to set individuals as targets. Therefore, with big data in health, it is getting harder to protect the privacy and confidentiality of health data, and ethical problems that may arise are diversifying. In order to prevent and resolve these problems, six principles have been determined in international ethical guidelines. These principles are open to development and discussion. In this thesis, it has been tried to show that the current situation regarding the data processing process in our country is not compatible with these principles, and it has been emphasized that it is the duty of the state to adopt approaches in accordance with these principles, which have a concrete equivalent in practice.

Keywords: Personal health data, sensitive data, medical ethics, autonomy, privacy

1. GİRİŞ

Günümüz bilgi ve teknolojisi sayesinde önemli bir birikime ulaşılmıştır. İnsanlığın ulaştığı bu birikimin en önemli çıktılarından biri 21. yüzyılın Büyük Veri konusudur.

Bilgisayarların hayatımıza girmesi, teknolojinin her alanda kendini gösteren ilerleyişi beraberinde sosyal medyanın rolü, daima gelişen ve değişen dünyamızdaki ayak izlerimizi dijital alana taşımıştır. Bu alan birçok platform ile desteklenerek Büyük Veri havuzunun temel yapı taşlarını oluşturmuştur. Bu yapı taşları yarattığımız sanal dünyanın birikimi ile inşa edilmiş ve giderek anlamlı bir hal almaya başlamıştır.

Büyük Veri'nin uygulama alanında karşılığını en iyi, yeni bir ekonomi sistemi geliştirmeye başlayan Çin Halk Cumhuriyeti ile görmek mümkündür. Çin'in pilot proje olarak uygulamaya başladığı Sosyal Kredi Sistemi, Büyük Veri'nin bilimkurgu filmlerini aratmayan örneğini oluşturmaktadır. Ekonomide ve toplumda "güvenliği" teşvik etme girişimi olarak adlandırdığı bu sistem ile bireyler, toplum içindeki davranış kalıplarına göre belli puanlar almaktadırlar (Hussoloji, 2018). Sistem bireyleri, topladıkları puanlara göre toplum içinde sınıflandırmaktadır. Bu sınıflandırma ile belli bir krediye sahip olanlar sosyal imkanlardan daha fazla oranda yararlanabilmektedir. Kredisi düşük olanlar ise seyahat etme, kredi alma, bazı otel ve restoranlara girememe gibi kısıtlamalarla karşı karşıya kalacaklardır. Sistemin genel amacı kurum, kuruluşlar ve bireylerin hareketlerini kayıt altına alarak dijital bir havuz oluşturmak biçiminde belirtilebilir. Böylece elde edilen bilgilerle sosyal, politik ve ekonomik açıdan bir denetleme ve kontrol altına alma veya kontrol altında tutma söz konusu olabilecektir. Örneğin bağımsız bir gazeteci tarafından Pekin-Şangay hızlı treninden yapılan bir anonsta, "Sevgili yolcular! Biletsiz seyahat eden ya da uygunsuz davranan kişiler ya da halka açık alanlarda sigara içen kişiler, yasalara göre cezalandırılacaktırlar ve bu davranış, bireysel kredi bilgi sistemine kaydedilecektir. Negatif bir kişisel kredi kaydından kaçınmak için lütfen ilgili kurallara uyun ve trendeki ve istasyondaki düzene yardımcı olun." ifadelerine yer verilmektedir (Altan, 2018). Bu örnek hükümetin bu projeyi hayata geçirdiğinin bir işareti olarak gösterilebilir. Söz konusu proje çeşitli açılardan tartışmalar yaratmaktadır. Sosyolog Zhang Lifan,"Çin hükümeti sıradan insanları izlemek için Çin'i bir polis devletine, büyük bir hapishaneye

dönüştürmek için yüksek teknoloji kullanmaya eğilimlidir" ifadeleri ile sistemi ve hükümeti eleştirmiştir (Hussoloji, 2018).

Büyük Veriye dayalı bir başka uç örnek The Great Hack isimli belgeselin konusunu oluşturan Cambridge Analytica isimli veri analiz şirketinin başında olduğu Alamo Projesi'dir. Bu proje ile 2016 yılındaki ABD'deki başkanlık seçimlerinde Trump'ın seçilmesi için toplanan seçmen verileri kullanılarak insanlar manipüle edilmiştir. Bu örnek, şirketlerin bu verileri ve oluşturdukları psiko-grafikleri kullanarak önemli farklar yaratabildiklerini göstermektedir. Seçme özgürlüğünün gerçekten olup olmadığını tartışmaya açarak Büyük Veri'nin kötüye kullanımının korkunç boyutunu göstermektedir. İnsanların ticari bir ürün haline geldiği, insanların duygusal nabızlarına çok kolay ulaşılabildiği ve artık şirketlerin davranışlarımızı önceden isabetli bir biçimde tahmin edilebilmeyi sağlayan Büyük Veri oldukça önemli bir sorun alanını oluşturmaktadır. Günümüzün gücü Büyük Veriye sahip olmak ile ölçülebilecek düzeydedir. Bu ve kötüye kullanımlar, David Caroll'un savunuculuğunu yaptığı yeni bir insan hakkı olarak "veri hakkı" nın tanınması gerekliliğini ortaya koymuştur.

Konunun daha iyi anlaşılabilmesi için ilk önce Büyük Veri'nin ne olduğu, Sağlık alanında Büyük Veri ve Büyük Veri'nin ortaya çıkardığı etik sorunlarının neler olduğunu belirtmek gerekmektedir.

1.1.Büyük Veri Nedir?

Büyük Veri, literatürdeki bilgiler ışığında en genel tanımıyla dünyadaki bütün bilgilerin tek bir havuzda toplanması ve dijital olarak bu bilgilere ulaşılabilir olmayı ifade etmektedir. Büyük Veri, terim olarak ilk kez 1997'de NASA'da çalışan Michael Cox ve David Ellsworth isimli iki bilim adamı tarafından kullanılmıştır (Uçar & İlkılıç, 2020). Bu tarihten önce Büyük Veri'nin ilk kez 1854 yılında Londra'da ortaya çıktığı kabul edilmektedir. Buna göre 1854 yılında Londra'da yaşanan kolera salgınında Dr. John Snow, hastalığın ortaya çıktığı ve sık görüldüğü yerleri Londra şehir haritasında işaretlemiş ve hastalığın kaynağının Broad caddesindeki su pompası olduğunu keşfetmiştir. Böylece hastalığın kaynağı öğrenilmiş ve salgının yayılmasını önlemek için su pompası kırılmıştır. Dr. John Snow'un konuya yaklaşımı ve geliştirdiği çözüm,

bugün Büyük veri ve veri işlemenin ilk örneği olarak kabul edilmektedir (Dülger, 2020).

Literatürde Büyük Veri tartışmaları farklı boyutları ile karşımıza çıkmaktadır. Bunlardan biri de Büyük Veri'nin tanımına yönelik tartışmalardır. De Mauro ve arkadaşları, Büyük Veriye ilişkin tartışmalardan hareketle Büyük Veri kavramına açıklık getirmek amacıyla resmi bir tanım yaptıklarını duyurmuşlardır (De Mauro, Greco & Grimaldi, 2015). Önerilen bu tanım Büyük Veri'nin teorik altyapısını, bilginin değerini, teknolojiye olan ihtiyacını, veri işleme tekniklerini ve insanlar üzerindeki etkisini dikkate alması açılarından oldukça kapsamlıdır. Buna göre, Büyük Veri, "Değer'e dönüşmesi için özel teknoloji ve analitik yöntemler gerektiren, yüksek hacim, hız ve çeşitlilik gibi unsurlarla karakterize edilen bilgi varlığıdır." (De Mauro, Greco & Grimaldi, 2015). McKinsey Global Institute (MGI) tarafından 2011 yılında yayımlanan Büyük Veri Raporu'nda ise "boyutları geleneksel veri tabanı yazılım araçlarının tutma, depolama, yönetme ve analiz etme yeteneğini aşan veri setleri" şeklinde tanımlanmıştır (Manyika, Chui, Brown, Bughin, Dobbs, Roxburg & Byers, 2011). Büyük Veri'nin kamusal faydasını ön plana çıkaran bir başka tanımı ise "insanların mevcut üretim ve yaşam biçimlerini değiştiren ve yenilikleri yönlendiren kilit faktörü, dijital çağın stratejik kaynağı" biçimindedir (Shi, 2014).

Büyük Veriyi özel kılan, yapılandırılmış, yarı yapılandırılmış ve yapılandırılmamış bilgileri kendi bünyesinde barındırmasıdır (Rouse, 2017). Büyük Veri'nin birçok kaynağa sahip olduğu bilinmektedir. Her geçen gün kaynağı genişleyen Büyük Veriye bir yenisi Rusya'nın başkenti Moskova'da kullanılmaya başlayan Face Pay yöntemi olmuştur. Bu yönteme göre Moskova metrosunun tüm istasyonlarında dünyada ilk kez yüz tanıma yöntemiyle ödeme yapabilme hizmeti sunulmaya başlamıştır (Cumhuriyet, 2021). Dolayısıyla Büyük Veri, sosyal ağlardan tıbbi kayıtlara, mobil uygulamalardan nesnelerin internetine uzanan geniş bir kaynağa sahiptir. Literatürdeki teknik tanımlarının ötesinde Büyük Veri, her an sayısız toplanabilen, depolanabilen ve dijital verilere dönüştürülerek anlamlı hale getirilen bilgilerin, kurum, kuruluş ve bireylerin amaçlarına hizmet edecek bir çıktıya dönüşme sürecini ifade etmektedir.

Büyük Veriden elde edilen çıktıların değeri üzerinden yapılan bir tanım ise şu şekildedir; "yeni iç görüler çıkarmak ya da yeni değer biçimleri yaratmak amacıyla,

piyasaları, organizasyonları, vatandaşlar ile hükümetler arasındaki ilişkileri ve daha fazlasını değiştiren biçimlerde, insanın daha küçük ölçekte yapılamayacak ama büyük bir ölçekte yapabildiği şeyleri ifade eder." (Mayer-Schönberger & Cukier, 2013). Büyük Veriye duyulan ilgi her geçen gün artmakla birlikte bunun sadece bir başlangıç olduğu, Büyük Veri'nin yaşama ve dünyayla etkileşim kurma biçimimize meydan okuyan bir gerçekliğe sahip olduğu belirtilmektedir. Çünkü Büyük Veri insanlık tarihi açısından önemli bir dönüşümün başlangıcı olarak nitelendirilmektedir (Mayer-Schönberger ve ark., 2013).

Büyük Veri'nin en önemli özelliği, veri hacmi giderek büyürken, kapladığı alanın giderek küçülmesidir. Büyük Veri'nin başta gelen bu özelliği, Büyük Veriyi oldukça değerli kılmaktadır. Bu konuda örneğin ABD endüstri ve hükümet kuruluşları tarafından Büyük Veri'nin toplandığı bulut kaynaklarına (depolama, bilgi işlem, sosyal ağ vb.) sağlık verileri de dahil olmak üzere açık erişim sağlamak için yılda 200 milyar doların üzerinde harcama yapılmıştır (Dinov, 2016). Büyük Veriye sahip olmak, büyük bir güce sahip olmayı ifade etmektedir. Bu anlamda Büyük Veri, bir endüstri terimi olarak karşımıza çıkmaktadır.

1.1.1. Büyük Veri değer zinciri

Büyük Veri'nin giderek artan önemi, "değer zinciri" ifadesi ile daha iyi açıklanabilmektedir. Büyük Veri'nin özü, bilgi veya bilgi parçacıklarıdır. Bilginin elde ediliş süreci farklı adımlardan oluşmaktadır. Büyük Veri değer zinciri, veri toplama, depolama, saklama, korelasyon ve analiz ile analiz sonuçlarının kullanılması aşamalarından oluşmaktadır (International Working Group on Data Protection in Telecommunications, 2014a).

Büyük Veri'nin değer zincirindeki ilk adım veri toplamadır. Günümüzde veri çok yaygın olarak birçok kaynaktan elde edilebilmektedir. Cep telefonu uygulamaları, akıllı şebekeler, araçlardaki ücretli geçiş transponderleri, hasta kayıtları, konum verileri, sosyal web siteleri, hava trafik yolcu verileri, kamu kayıtları, müşteri sadakat programları, genom dizileme, satış geçmişi vb. gibi birçok veri kaynağı bulunmaktadır (International Working Group on Data Protection in Telecommunications, 2014a).

Sensör teknolojisinin yaygınlaşmasıyla veri kaynağı giderek genişlemektedir. Bugün kullanılan akıllı diş fırçaları, akıllı buzdolapları, akıllı ayakkabılar, akıllı TV'ler gibi birçok "akıllı" cihaz, her bireyin yaşam tarzı hakkında çok şey ortaya çıkarabilmektedir (International Working Group on Data Protection in Telecommunications, 2014a).

Toplanan verinin depolanması ve saklanması günümüz bulut teknolojisi sayesinde bir sorun olmaktan çıkmıştır. Büyük Veri'nin depolanmasını ve saklanmasını kolaylaştıran destekleyici yeni teknolojiler, Büyük Veri'nin değer zincirinin en önemli bileşenidir. Depolanan veriler daha çok yapılandırılmamış, ham verilerdir.

Ham ve yapılandırılmamış halde bulunan veri, bir yığından başka bir şey ifade etmez. Çeşitli kaynaklardan gelen verinin birleştirilmesi, birleştirilen verilerden yeni bilgiler oluşturulması verinin analizi yoluyla gerçekleşmektedir. Büyük Veri değer zincirinin en önemli aşaması verinin analizi ile ortaya çıkarılan korelasyonlardır. Örneğin tıp alanında Büyük Veri analizi yoluyla elde edilen korelasyonlardan biri taburcu edilen bir hastanın bir ay içinde geri dönme olasılığını artıran bütün koşulların listesinin çıkarılabilmesidir (Mayer-Schönberger ve ark., 2013).

Analiz tekniklerine ilişkin teknikler ise Veri Madenciliği, Makine Öğrenmesi, Sosyal Ağ Analizi, Öngörücü Analitik, Doğal Dil İşleme ve Görselleştirme gibi başlıca tekniklerden oluşmaktadır (International Working Group on Data Protection in Telecommunications, 2014a).

Büyük Veri değer zincirinin son aşaması analiz sonuçlarının kullanılmasıdır. Verinin analizinden elde edilen çıktılar çok önemlidir ve birçok amaç için kullanılabilir. Analiz sonuçlarından en çok bankalar, sigorta şirketleri, kredi derecelendirme kuruluşları, işverenler gibi birçok kurum daha iyi ve daha bilinçli kararlar verebilmek için yararlanmaktadırlar (International Working Group on Data Protection in Telecommunications, 2014a). Büyük Veriye sahip olan şirketler kendisini iyileştirmek, daha iyi müşteri memnuniyeti sağlamak, müşteri merkezli kişiselleştirilmiş pazarlama kampanyaları oluşturmak gibi karlılık odaklı amaçlarla Büyük Veriyi kullanmak istemektedirler (Rouse, 2017).

1.2. Sağlıkta Büyük Veri

Büyük Veri'nin başlıca kaynaklarından biri sağlık alanındaki veridir. Çünkü Büyük Veri'nin en çok değer ürettiği alan sağlıktır.

Büyük sağlık verisinin analizi yoluyla elde edilen çıktıların etkin bir şekilde kullanılması, sağlık hizmetlerinin sunum kalitesi ve etkinliğini iyileştirebilir. Gerek toplum sağlığı açısından bir bulaşıcı hastalığın varlığını önceden öngörebilmek, gerekse erken evrelerde risk altındaki hastaları saptamak gibi önemli yararları dile getirilmektedir.

Sağlık alanında Büyük Veri, sağlık ve sağlık sistemi performansını artırmak amacıyla elektronik olarak yakalanan ve saklanan, rutin veya otomatik olarak toplanan Büyük Veri kümeleri biçiminde tanımlanmaktadır (Habl, Theresa Renner, Bobek & Laschkolnig, 2016). Sağlık kuruluşlarında tutulan elektronik sağlık kayıtları, halk sağlığı verileri, sağlık sigortası ile ilgili veriler, klinik araştırmadan elde edilen bilgiler, diğer bilimsel araştırma sonuçlarından elde edilen bilgiler gibi birçok kaynaktan elde edilen verinin bütünü sağlık alanındaki Büyük Veriyi oluşturmaktadır. Gerçek zamanlı tıbbi sensörler, tıbbi cihazlar, web uygulamaları ve sosyal medyadan gelen yapılandırılmamış veriler de sağlık alanındaki Büyük Veriyi içermektedir (Ankaralı, 2020). Büyük Veri'nin sağlık alanındaki en kolay anlaşılır örneği, Google arama motorunda yapılan sağlıkla ilgili aramaları bölgesel olarak kümeleyerek, herhangi bir yerdeki salgın veya yaygın bir hastalığın varlığını ortaya çıkarabilme özelliğidir (Silahtaroğlu, 2018). Bu yöntemi, kolera salgınının yerini tespit eden Dr. John Snow, 1854 yılında haritada işaretleyerek yapmıştır. John Snow'un yapmış olduğu bu yöntem, hem Büyük Veri'nin hem de sağlıkta Büyük Veri'nin kullanımı açısından bir ilk olarak kabul edilmektedir. Sağlık alanında yapılan en eski Büyük Veri kaynağı, 1948 yılından beri süren Framingham Heart Study çalışmasıdır (Ankaralı, 2020). Bu çalışma ile üç nesil boyunca kalp hastalıkları incelenmiş ve kardiyovasküler hastalığın sigara, yüksek tansiyon, obezite, yüksek kolesterol seviyeleri ve fiziksel hareketsizlik gibi değiştirilebilir risk faktörlerinden kaynaklandığı ortaya konulmuştur (National Institutes of Health Office of Science Policy, 2021). Büyük Veri kullanılarak çeşitli veri kümeleri incelenmesiyle hastalıkların gizli kalıpları, bilinmeyen korelasyonları ve iç yüzü ortaya çıkarılabilmektedir (He, Ge & He, 2017). Örneğin güney Afrika'da

araştırmacılar Büyük Veriyi kullanarak B vitamini kullanımı ile AIDS hastalığının ve HIV pozitif ölümlerinin daha gecikmeli olması arasında anlamlı bir ilişki saptamışlardır (Tene, & Polonetsky, 2013). Bununla birlikte sağlık hizmetlerinin planlanması, geniş topluluklardaki sağlık harcaması eğilimleri, hastalıkların dağılımı, etkin tedaviye erişim oranları, yeni üretilen bir ilacın hedef kitle tahmini gibi birçok çıkarım yapmak mümkündür (Altınbaş, 2018). Literatür incelendiğinde Büyük Veri analizinin sağlık alanında oldukça yaygın bir şekilde kullanıldığı görülmektedir.

Sağlıkta Büyük Veri, veri toplama kaynaklarına bağlı olarak her geçen gün artmaktadır. Veri boyutu açısından değerlendirildiğinde sağlık hizmetlerindeki Büyük Veri'nin 2011'den sonra 150 eksabaytı aştığı, bir başka çalışmada sağlık hizmetlerindeki veri boyutunun 2020'de 40 zettabayt (ZB) civarında olduğunun tahmin edildiği aktarılmaktadır (Hong ve ark, 2018). Türkiye'deki Büyük sağlık verisi için Sağlık Bakanlığı'nın veri yönetimi için bir sistem altyapısı mevcuttur. Bakanlığın bu altyapısında İstanbul'da kullanılan 12 ve boş bulunan 13 olmak üzere 25 adet, Ankara'da kullanılan 30 ve 25 adet boş olmak üzere 55 adet veri merkezi kabini bulunmaktadır (Elmas, Gürel Gökçay, & Gül, 2020).

1.3.Büyük Veri ve Başlıca Etik Sorunları

Büyük Veri'nin özellikle kamu hizmetleri açısından önemli fırsatları bulunduğu belirtilmektedir (Kaya, 2020). Ancak bu fırsatların yanı sıra mahremiyet ve gizliliğin ihlali başta olmak üzere birçok risk ve kaygı verici etik sorun kümeleri bulunmaktadır. Bu sorun kümeleri *"Ethics of Big Data"* kitabında kimlik, mahremiyet, itibar ve mülkiyet şeklinde dört başlıkta sınıflandırılmaktadır (Davis & Patterson, 2012). Buna göre kimlik boyutunda başkalarının kolaylıkla çeşitli kimlik bilgilerine erişim sağlaması sorunu, bu erişimin mahremiyete olan etkisi, itibar boyutunda etkileşim içinde olmadığımız kişilere itibarımız hakkında bilgi verebilmesi ve mülkiyet boyutunda hangi bilgiler üzerinde kimin hak sahibi olacağı sorunu incelenmiştir.

Taylor Armerding bir makalesinde Büyük Veri ile bağlantılı beş büyük sorunu şu şekilde özetlemektedir (aktaran Lokke, 1980, s.65);

- Ayrımcılık: Veri analizleri belirli özellikleri (etnik köken, cinsiyet, din vb.) olan kişilerin, başkalarıyla aynı olanaklara sahip olması konusunda zorluk çıkarabilir.
- Güvenlik ihlali: Kişisel verileriniz sızdırılabilir, sonradan işlenmeleri için büyük fırsatlar doğar. Örneğin, şimdilerde, özellikle uyuyan çocukların web kamera resimlerini arayan arama motorları (Shodan) vardır.
- Anonimliğe veda: Büyük Veri setlerine bağlanarak anonim kişilerin kimliği yeniden tanımlanabilir.
- Devlete verilen geniş yetkiler: Büyük Veri ayrıca, izleme ve devletin organlarına hangi yetkilerin verileceği sorununu da gündeme getirir.
- Düzenlenmemiş bilgi işlem: Pek çok kişisel veriniz, bilgi işlemin doğru yapıldığı konusunda bir saydamlık ya da garanti sunulmadan işlenebilir.

Veri karmaşıklığının da önemli düzeyde arttığı içinde bulunduğumuz bilişim çağında Büyük Veri, dünyayı anlama, araştırma ve değiştirme biçimlerimizi etkilemekte ve hatta dönüştürmektedir (Dinov, 2016; Mayer-Schönberger & Cukier, 2013). Girişte belirtilen iki örnekte olduğu gibi Büyük Veriyi kullanan hükümet ve şirketler gibi karar vericiler, topluma önemli ölçüde müdahale edebilmekte ve toplumun yapısını değiştirebilmektedir. Bu durum özellikle toplumun psikolojik olarak manipülasyona uğratılabilmesini karşımıza çıkarmaktadır. Toplumun manipüle edilmesi insan hakkı ihlallerine yol açarken temelde bireysel özgürlüğümüzün ortadan kaldırabildiğine işaret etmektedir. Bireyler olarak gerçekten 'seçme' şansımızın olup olmadığını sorgulatmaktadır. Günümüzde özellikle Büyük sağlık verileri, şirketlerin ve devletlerin himayesi altına girmeye başlamıştır. Dolayısıyla toplanan bilgilerle tıp kurumu, şirketlerin ve devletlerin toplum üzerindeki söz konusu müdahalelerine ve manipülasyonlarına araç olabilmektedir. Giderek küreselleşen ve bu anlamda şirketleşen dünyada Büyük sağlık verilerinin toplanmasının yaratabileceği değer sorunları, insan hakları başta olmak üzere, sağlık hizmetlerine erişim, sağlık hakkı ve sağlık hizmetlerinin geleceği açılarından önemli etik sorunlar yaratmaktadır.

Büyük sağlık verisi, verinin ekonomik değeri üzerinden tanımlanmakta ve böylece verinin alınıp satılabilen bir meta olarak değerlendirilmesine sebep olmaktadır. Örneğin Türkiye'de Sağlık Bakanlığı ve Sosyal Güvenlik Kurumu (SGK) tarafından toplanan kişisel sağlık verileri, hastaların bilgisi olmadan satılmıştır (Birgün, 2014).

Bu durum tıp etiğinin çok önemli değerlerinden biri olan mahremiyetin harcandığına işaret etmekle birlikte genel olarak kişisel sağlık bilgilerinin ekonomik değeri olan ticari bir ürün olarak tanımlandığını göstermektedir. Sağlıkta Büyük Veri'nin yarattığı bu ve benzeri kaygılara, Avrupa Doktorları Daimi Komitesi (CPME) tarafından dikkat çekilmiş ve sağlık ve tıbbi veriler başta olmak üzere bireylerin verilerinin yüksek düzeyde korunması gerekliliği vurgulanmıştır (CPME, 2012). Gizliliğin daha fazla ihlal edilecek olmasına yönelik oluşan kaygılar, içinde bulunduğumuz yapay zeka çağının boyutları düşünüldüğünde giderek artmaktadır.

Kaygı verici bir başka senaryo, depolanan kişisel verilerin, kötü amaçlı şahıs veya örgütlerin eline geçebilecek olmasıdır. Bu durum kişisel veriye karşı en büyük tehdit unsuru olarak bildirilmektedir (Snoad, 2011). Snoad'ın bildirdiğine göre yapılan bir araştırmaya göre, tüketiciler kişisel mahremiyetin suiistimali konusunda terörizm veya iklim değişikliğinden daha fazla endişelidir. Bununla birlikte sosyal ağların giderek daha fazla kullanılması, internet üzerinden daha fazla alışveriş yapılması, daha fazla çevrimiçi olunması ile depolanan bilgilerden birçok kişiye ait yeni bilgilere tahmin edilerek ulaşılması çok daha kolay olacaktır (Snoad, 2011). Günümüz dünyası gerçeklik algısını sanal dünya üzerinden kurmaktadır. Bugün en çok kullanılan sosyal medya uygulamalarından Facebook, Instagram, TikTok gibi uygulamalar ücretsiz olarak kullanıcıya sunulmakta ve karşılığında kullanıcıya ait kişisel bilgileri işlemektedirler. Örneğin TikTok uygulamasının gizlilik politikası incelendiğinde kullanıcı adı, parola, doğum tarihi, e-posta adresi, telefon, fotoğraf veya video gibi profil bilgileri, kullanıcı içeriği ve davranışsal bilgiler, konum bilgisi, cihaz IP adresi, saat dilimi ayarları, cihaz modeli, cihaz sistemi, cihaz kimlikleri, ekran çözünürlüğü, işletim sistemi, aplikasyon ve dosya isimleri, tuş vuruşu düzen veya ritim bilgileri, pil durumu gibi kullanıcılar hakkında teknik bilgileri topladığını bildirmektedir. TikTok en son güncellediği gizlilik politikası ile biyometrik verileri de toplayacağını açıklamıştır (Haberler.com, 2021).

Toplanan kişisel bilgilerin şirketler tarafından çok değerli olması nedeniyle saklanması önemli bir sorundur. Max Schrems'in Facebook'a yaptığı veri talep başvurusunda, kullanıcının sildiği halde akışta silinen ancak şirketin veri analiz ve satışının gerçekleştiği veri tabanlarından bilgilerin silinmediği ortaya çıkmıştır. Buna benzer bir

örnek ise Türkiye'de çevrimiçi kitlesel gözetimin yapılmasıdır. Buna göre Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yapıldığı belirtilen gözetimde, yaklaşık bir buçuk yıldır internet servis sağlayıcılarından tüm kullanıcıların internet trafiği kayıtlarının saat başı kendisine hangi formatta kayıt altına alınacağını ve kendisine nasıl gönderileceğini anlattığı teknik detay dokümanı ile istediği belirtilmektedir (Eroğlu, 2022). BTK bu verileri internet kullanıcılarının kimlikleriyle birlikte, hangi internet sitelerini ziyaret ettikleri ve hangi uygulamaları kullandıkları ile birlikte kaydettiği ifade edilmektedir (Eroğlu, 2022). Bütün bu süreçte gelecekte bizi ne gibi sorunların beklediğinin sorgulanması ve derinlemesine tartışılması gerektiği ileri sürülerek, Büyük Veriye yaklaşımımızı belirleyen bir etik alanına ihtiyacımız olduğu vurgulanmaktadır (Mullins, 2018).

Özellikle Büyük sağlık verileri, şirketlerin çok fazla dikkatini çekmektedir. Çünkü sağlık alanı, Büyük Veri'nin uygulama alanının çok geniş olduğu bir sektördür. Sağlık alanında toplanan kişisel sağlık bilgilerinin, özellikle teknoloji devleri için önemli bir değere sahip olduğu belirtilmekte ve bu bilgilerin şirketlerin eline bırakılmaması gerektiği vurgulanmaktadır (Boiten, 2020). Şirketler için çok değerli kişisel sağlık verilerine erişim giderek daha önemli hale gelmekte ve şirketler doğaları gereği kar amacı güderek bu verilerden elde edilen bilgileri diledikleri gibi kullanabilme olanağı bulmaktadırlar. Dijital alana aktarılan bilgilere erişim için güvenlik önlemleri alınsa bile her zaman yeterli olamamakta ve bu bilgilere erişim sağlamak bir biçimde mümkün hale olabilmektedir (Helm, 2020).

Büyük Veri'nin, sağlık alanında tek bir hastaya özgü kişiselleştirilmiş tedavi yöntemleri sunabilmesi, yapay zekanın sağlık alanında kendine önemli bir yer kazandırması ve böylece sağlık hizmetlerinin bambaşka bir boyut kazanması, koruyucu sağlık hizmetlerini geliştirebilme potansiyeli, tıpta hata payını azaltabilmesi ve kanıta dayalı tıpta daha kesin bilgiler üretilmesi gibi oldukça önemli yararları bulunmaktadır. Buna karşın yarattığı sorunlar incelendiğinde, mahremiyet ve gizliliğe dayalı etik sorunlar bulunmaktadır. Kişisel sağlık verilerinin dijital ortama aktarılması, daha çok veri ihlalleri yaşanması riskini ortaya çıkarmaktadır. Tarihin en büyük sağlık verisi hırsızlığı, 2015 yılında yaşanan ABD'deki bir sigorta şirketi olan Anthem Inc.'de gerçekleşen olaydır. Şirket, kendisine kayıtlı olan 80 milyon kişiye ait sosyal

güvenlik numaraları ile diğer kişisel sağlık bilgilerinin çalındığını duyurmuştur (Painter Randall, 2015). Bu bağlamda veri sızıntılarından en çok sağlık alanının etkilendiği ileri sürülebilir (Winally, 2018).

Ülkemizde de benzer veri sızıntı olayları yaşanmış ve hatta e-Nabız veri kayıt sistemi ile toplanan kişisel bileğiler kötü amaçlarla kullanılmıştır. Girişte aktarılan Cambridge Analytica'ya benzer bir olay, ülkemizde 31 Mart (2019) seçimlerinde yaşanmıştır. Buna göre muhalefet partilerin iktidar partisi olan bir siyasi partinin İstanbul yerel seçim sonuçlarına itiraz ederken YSK'ya sunduğu deliller arasında hukuka aykırı bir şekilde kişisel verilerin toplandığı iddiası bulunmaktadır. Bu iddianın savunmasında ise bu verilere ulaşmanın zor olmadığı yönünde olmuştur (Öztürk, 2019). Aynı seçimin iptal edilmesinin bir diğer gerekçesi, 41 bin 132 kısıtlı/engelli seçmenin oy kullandığı iddiası olmuştur. Psikiyatrik muayene olduktan sonra yazılan reçeteyle antidepresan kullanan bir kişinin adının, İstanbul seçimlerini iptal eden Yüksek Seçim Kurulu'nun (YSK) "kısıtlı seçmen" listesine eklendiği ortaya çıkmıştır (SOL, 2019). Yaşanan bu olay, Türkiye'de insanların sağlık verilerinin siyasi amaçlarla kullanılabildiği göstermektedir.

Sağlıkta Büyük Veri'nin getirmiş olduğu bir başka etik sorun iş sağlığı alanındadır. Buna göre bir şirket, kurumsal firmalara 20 yaş üzerindeki çalışanların sağlık kayıtlarını analiz etmiş ve çalışanların sağlık profillerini çıkarmıştır (Uçar & İlkılıç, 2020). Böylece işçilerin hangisi kalp krizi geçirecek, kim mesleki hastalık sınırında önceden tahmin etmek mümkündür. İşveren bu tahminlere göre hasta ihtimali olan kişileri işten çıkarabilir veya işçileri sağlık profillerine göre işe alım yapabilir. Dolayısıyla işveren kendi menfaatlerini koruyan ayrımcılığa dayalı bir sistemi inşa edebilir. Örneğin bu sistemin daha ileri aşaması genetik mühendisliğinin çok geliştiği bir dünyayı anlatan Gattaca filminde işlenmiştir. Bu filmde DNA testleri insanların kimliklerini oluşturmakta ve insanların toplum içerisindeki geçerliliğini belirlemektedir. DNA testleri yetersiz olarak görülen kişiler, toplum içerisinde bir alt sınıf olan "geçersizler" i oluşturmaktadır.

Sağlık alanında Büyük Veri analizlerine artık biyometrik veriler de girmeye başlamıştır. Türkiye'de Covid-19 pandemisini önleme kapsamında alınan tedbirlerden biri, avuç içi izi alınarak kimlik tespiti uygulamaları yapılmak istenmesidir. Diğer

bulaşıcı hastalıklar ve özellikle de Covid-19 virüsü nedeniyle önemli bir halk sağlığı sorununa neden olabilecek bir tehlike yaratması gerekçesiyle bu uygulamaya Türk Tabipleri Birliği (TTB) karşı çıkmış ve SGK'ya "sağlık kurumlarında avuç içi izi alınarak kimlik tespiti uygulamaları durdurulmalı" görüşünü bildirmiştir (TTB, 2021). Söz konusu bu uygulama ve benzerleri göstermektedir ki, genel olarak dünyada geleneksel kimlik doğrulamanın yerini avuç içi, parmak izi, yüz ve iris tanıma gibi biyometrik verilerle yapılacak doğrulama yöntemleri alacaktır.

Sağlık alanında Büyük Veri'nin bir diğer en önemli kaynağı, elektronik sağlık veri tabanlarının giderek artan kullanımıdır. Bu veri tabanları, e-Nabız gibi bireylerin kendilerine ait en hassas nitelikteki bilgiler olabildiği gibi hastanelerin kullandığı ve sağlık çalışanlarının da veri girişi için kullandığı uygulamalardan oluşmaktadır. Sağlık alanında kullanılan veri tabanlarının sağlık hizmetleri açısından önemli yararları bulunmaktadır. Sağlık hizmetlerine erişimi artırmak, bakım ve sağlık kalitesini iyileştirme ve maliyetleri düşürmek gibi başta gelen faydalar olarak bilinmektedir. Bazı araştırmalarda ise dezavantajlı gruplar için erişimi artırmadığı, veri kayıt sistemlerinin doğruluk, üretkenlik ve maliyeti düşürmek gibi olumlu etkilerinin bulunmadığının gösterildiği belirtilmektedir (Layman, 2020).

Özetle günümüz sağlık hizmetleri veri tabanlarına kaydedilen sağlık verileri ile yürütülmektedir. Veri tabanlarına işlenen bilgiler yarı yapılandırılmış veri kategorisinde değerlendirilmektedir. Veri tabanlarında toplanan sınırsız sayıda verinin sahibinin kim olduğu bu bağlamda kişisel verinin nasıl korunacağı, taşeron bilgi işlem şirketlerinin veri tabanlarına sahip olarak işlenen kişisel veriye de sahip olduğu iddiasından hareketle verileri yanında götürmek istemesi, işlenen verinin ticari amaçlarla kullanılarak suiistimal edilmesi gibi etik sorun başlıkları bulunmaktadır. Ayrımcılığa uğrama, sağlık hizmetlerine erişim sorunları, gizli kalması istenilen bilgilerin ortaya çıkmasıyla mahremiyetin ihlali ve aile içi mağduriyetlerin yaşanması ve bazı temel insan haklarının ihlali gibi diğer etik sorun başlıkları bulunmaktadır. Dolayısıyla Sağlıktaki Büyük Veri, büyük bir etik sorun alanı oluşturmaktadır.

1.4. Tezin Amacı

Büyük Veri grupların, toplulukların davranışlarını tahmin etmek ve belirlemek için çok büyük miktarlarda verinin işlenmesi ve analiz edilmesini mümkün kıldığı için, veri kullanımına ilişkin risklerin kolektif boyutu önemli hale gelmektedir. Büyük Veri bağlamında işlenen tüm sağlık bilgileri, kişisel verilerle ilgilidir. Kişisel sağlık verilerinin korunması, özel yaşamın gizliliği, mahremiyet, verinin kötüye kullanılması ve ifşa edilmesi gibi başlıca etik sorunlar dikkate alındığında, Büyük Veri'nin sağlık alanında kullanılması sürecinde bireylerin daha fazla korunması gerekliliği ortaya çıkmaktadır. Ekonomik Kalkınma ve İşbirliği Teşkilatı (OECD) ve Avrupa Veri Koruma Direktifi tarafından kişisel verilerin makul, doğru ve meşru bir şekilde nasıl işlenebileceğine ilişkin bazı temel ilkeler oluşturulmuştur. Yanı sıra kişisel sağlık verilerinin korunması için uluslararası düzeyde ilgili tarafları (hükümetler, şirketler, gerçek veya tüzel kişiler, karar vericiler vb.) kapsayan etik rehberler oluşturulmaya çalışılmaktadır.

Kamu otoriteleri Büyük Veri'nin potansiyel riskleri konusunda gerekli bilgi ve farkındalığa sahip olmalıdır. Bu bağlamda Türkiye'de de 7 Mayıs 2016 tarihinde çıkarılan Kişisel Verileri Koruma Kanunu, kişisel verinin korunması hakkının güvence altına alınması için genel bir çerçeve sağlamaktadır. Sağlık verileri konusunda ise Kişisel Sağlık Verileri Hakkında Yönetmelik (2019) yürürlüğe girmiştir. Bu iki düzenleme başta olmak üzere kişisel verinin korunmasıyla ilgili diğer düzenlemelerdeki eksiklikleri ve olası etik sorunları saptamak ve yasal düzenlemelerin Büyük sağlık verileri bağlamındaki etik sorunlar açısından incelenmesi önemlidir. Yanı sıra sağlık alanında giderek daha fazla kullanılan veri tabanlarındaki olası etik sorunlarını meslek ahlakı yükümlülükleri ve haklar temelinde saptamak gerekmektedir.

Tezin amacı; kişisel verinin korunmasıyla ilgili düzenlemeler ve sağlıkta kullanılan veri tabanlarındaki etik sorunları tanımlamak ve bu sorunları önlenemeye ve çözmeye yönelik, meslek ahlakı yükümlülükleri ve insan hakları temelinde öneriler geliştirmektir. Beraberinde alanda çalışan hekimlerin veri tabanlarını kullanırken dikkat etmesi gereken ilke ve kuralları oluşturmaktır. Bu bağlamda tez alanda önemli bir boşluğu doldurmayı hedeflemektedir. Ülkemizde kişisel veriyi koruyan düzenleme

metinlerinin ve sağlık hizmeti basamaklarında kullanılan veri tabanlarının birlikte incelenmesi çalışmaya özgünlük katmaktadır.

2. GENEL BİLGİLER

2.1. Büyük Veri ve Temel Kavramları

2.1.1. Büyük Veri'nin özelliklerine ilişkin kavramlar

Veri büyüklüğü olarak terabit veya petabitin yüzlerce katları olarak ifade edilen Büyük Veri'nin çokluğunu ifade eden birtakım temel kavramlar bulunmaktadır. Verinin büyüklüğü "terabyte", "petabyte", "exabyte", "zettabyte" ve "yottobyte" sözcükleri ile açıklanmaya çalışılır (Dalgalıdere, 2016);

- Terabyte: 200 bin fotoğraf veya MP3 şarkı, tek bir terabaytlık hard diske sığdırılabilmektedir.
- Petabyte: İki veri merkezi kabinine yerleştirilmiş 16 tane Backblaze saklama poduna sığdırılabilmektedir.
- Exabyte: Bir apartmanı doldurabilecek dört veri toplama merkezinde iki bin kabine sığdırılabilmektedir
- Zettabyte: Exabyte için tanımlanan apartmanların 1000 katı. Menhattan'ın yaklaşık %20'sini kaplayacak ölçüde.
- Yottobyte: Bir milyon veri merkeziyle Delaware ve Rhode Adasına sığdırılabilmektedir.

Geleneksel veriye kıyasla Büyük Veri'nin pratik açıdan oldukça önemli avantajları bulunmaktadır. Bu farkları inceleyen bir çalışma Büyük Veri ve geleneksel veri arasındaki farkları Tablo 1'deki gibi ifade etmiştir.

Tablo 1. Geleneksel veri ile Büyük Veri'nin karşılaştırması (Yavuz, 2019)

Kriter	**Geleneksel Veri**	**Büyük Veri**
Hacim	KB, MB, GB	TB, PB
Veri üretim oranı	Saatlik, günlük	Anlık, saniyelik, dakikalık
Veri yapısı	Yapısal	Yapısal, yapısal olmayan veya yarı yapısal
Veri kaynağı	Merkezi	Tamamen dağıtık
Veri entegrasyonu	Kolay	Zor
Veri depolama	İlişkisel veri tabanı	HDFS, NoSQL
Veri erişim	İnteraktif	Toplu veya yakın gerçek zamanlı

Veri büyüklüğünü ifade eden kavramların yanı sıra Büyük Veri'nin bileşenleri olarak ifade edilen kavramlar bulunmaktadır (Gürsakal, 2014);

- Hacim (Volume): Verinin bilgisayarda ya da sistemde ya da bulutta kapladığı alan
- Hız (Velocity): Büyük Veri'nin hızı ile kastedilen sürekli yeni verilerin üretilmesi ile veri setinin artan bir dinamizme sahip olması
- Çeşitlilik (Variety): Büyük Veri'nin çeşitliliği veri kaynaklarının farklılığından kaynaklanan, veri kaynaklarının artmasıyla elde edilen verilerin çeşitlenmesi
- Doğrulama / Geçerlik (Verification): Büyük Veri'nin güvenli olması durumu
- Değer (Value): Verinin ortaya çıkardığı maddi değer biçimlerinde ifade edilmektedir.

Büyük Veri'nin bileşenlerini 5V'si olarak açıklayan çalışmaların yanı sıra 9V olarak açıklayan çalışmalar da vardır (Wu, Buyya & Ramamohanarao, 2016).

2.1.2. Veri kavramı ve ilişkili diğer kavramlar

Büyük Veriye kaynaklık eden ve İngilizce karşılığı *"data"* kelimesi, Latince *"datum"* sözcüğünün çoğulu olarak İngilizceye geçtiği belirtilmektedir. Latincedeki anlamı ise "vermek, dağıtmak, bir şey adamak" biçiminde tanımlanmaktadır (Rosenberg, 2013).

Terimin ilk kullanımı 1646 yılında "bir veri yığını" anlamında teolojik bir kaynakta geçtiği ve Oxford İngilizce Sözlüğü tarafından keşfedildiği bildirilmektedir (Rosenberg, 2013). İnsanların veri elde etme ve bu veriyi kaydetme özelliği çağlar öncesine dayanmaktadır. Buna göre ilk veri, Üst Paleolitik çağa tarihlenen, İshango isimli bir kemiğe yazıldığı aktarılmaktadır (Gürsakal, 2019). Veri sözcüğünün bir başka en eski kullanımlarından biri İskenderiyeli matematikçi Öklid'in "Veri" adlı kitabında gerçekleştiği belirtilmektedir (Gürsakal, 2019). Verinin bugünkü anlamıyla kullanımı ise 18. yüzyılın sonlarına tarihlenmektedir. On sekizinci yüzyıl boyunca bilimsel bağlamlarda *veri* sözcüğünün nasıl değiştiğini gözlemleyen Daniel Rosenberg (2013), yüzyılın başında verinin özellikle argümanın temeli olarak kabul edilen ilkelere ya da sorgulamaya açık olmayan kutsal metinlerden derlenen alıntılara atıfta bulunmak amacıyla kullanıldığı, yüzyılın sonuna gelindiğinde *veri* sözcüğü yaygın olarak deney, deneyim veya belirlenen kanıtlardaki gerçekleri anlatmak için

kullanıldığı belirtilmektedir. 19. yüzyıl boyunca ampirik araştırma ve gözlemin bir sonu olarak veri sözcüğü, istatistik ve ekonomi bilimlerinin gelişmesine zemin hazırlayarak ortak bir kullanım alanı oluşturduğu açıklanmaktadır (Rosenberg, 2013).

Veri, dijital çağ olarak da adlandırabileceğimiz içinde bulunduğumuz yüzyılda bilginin hammaddesi olarak görülmektedir. Günümüzde verinin elde edilebileceği çok çeşitli kaynak bulunmaktadır. İnsanın parmak uçlarının gezindiği çeşitli internet tabanlı uygulamalar aracılığıyla birçok bilgimiz "veri" statüsü kazanmaktadır. GPS uyduları, cep telefonu kayıtları, medya, çevrimiçi hizmetler, sipariş gönderim verileri, finansal kayıtlar (Bitcoin, hisse senedi alım satımları vs.), güvenlik kamera kayıtları, seyahat ile ilgili veriler, sosyal ağlar, e-posta ve sohbet verileri gibi birçok veri kaynağı bulunmaktadır ve bu kaynaklar aktif olarak kullanılmaktadır. Bunların yanı sıra günümüzde sağlık hizmetlerinde kullanılan geleneksel kayıt sistemi yerini elektronik kayıt sistemine bırakmıştır. Böylece elektronik sağlık kayıtları da önemli bir veri kaynağı oluşturmaktadır.

2.1.2.1.Veri türleri ve metaveri

Çok çeşitli şekillerde gruplandırılan veri türleri, yapılandırılmış, yarı yapılandırılmış ve yapılandırılmamış olmak üzere üç başlıkta sınıflandırılmaktadır (Gürsakal, 2014). Gürsakal'a göre verinin bir kayıtta veya dosyada sabit bir alanda bulunması söz konusu ise yapılandırılmış veridir. Verinin yapılandırılmış olması için belirlenebilir bir yapıda olması gerekmektedir. Yarı yapılandırılmış veriler, "yapı" ve "etiket" sözcüklerinin arasında olan veriler biçiminde tanımlanmaktadır. Eğer verilerin bir yapısı varsa ancak toplanan bütün enformasyon aynı yapıya sahip değilse bu tür veriler yarı yapılandırılmış veriler olarak gruplandırılmaktadır. Bunlar önceden belirlenmiş bir şemaya sahip olmayan, kendi kendini tanımlayan verilerdir. Bu grup verilere örnek olarak, bir doktorun hastasına ilişkin gözlemlerini belirli metin alanlarında yazması verilmektedir. Bu yolla "yapılandırılmış" meta veri alanları ilişkili içeriği tanımlamaktadır. "Hastanın geçirdiği hastalıklar", "ailesinin geçirdiği hastalıklar", "klinik bulgular" ve "teşhis" gibi alanlar doldurularak yarı yapılandırılmış veri grubunun oluşturulduğu ifade edilmektedir. Son olarak yapılandırılmamış veri, etiket kavramı ile açıklanmaktadır. Buna göre herhangi bir türde, herhangi bir format,

dizi veya kural izlemeyen verilerdir. Örneğin metin, video, ses, görüntü, pdf ve html dosyaları yapılandırılmamış veri olarak ifade edilmektedir (Gürsakal, 2014).

Bu veri türleri dışında ayrıca iç veri, (bir şirketin veri deposunda toplanan alışverişe ilişkin verileri), bağlamsal veri (dış kaynaklardan alınan mekan, nüfus, demografi gibi veriye hikaye ekleyen bağlama ilişkin veriler) ve entegre veri modeli (sonraki analizleri de destekleyecek olan her şeyi birbirine bağlayan meta veri) biçiminde ifade edilen farklı türler bulunmaktadır (Gürsakal, 2014).

Üst veri biçiminde de tanımlanan metaveri, başka bilgileri anlatan ya da açıklayan bilgiler şeklinde tanımlayan Lokke, bunu bir arkadaşa yazılan mektup ile örneklendirmektedir (Lokke, 1980, s.40). Buna göre bir kişiye yollanmış olan mektupta, zarfın üzerindeki bilgi *meta* (hakkında), mektubun kendisi ise *data'*dır (veri). Gray ve arkadaşlarına göre ise metaveri, verinin nasıl elde edildiği, nasıl hesaplandığı, nitelikleri, adları, birimleri, kesinliği ve veri düzenini açıklayan tanımlayıcı bilgilerdir (Gray ve ark., 2005). Yapılandırılmamış verileri bilgisayarın okuyacağı şekilde yapılandırılmış hale dönüştürmek ve bir düzen vermek için metaveriden yararlanılmaktadır (Gürsakal, 2019).

2.1.2.2. Veri seti ve veri tabanları

Veri seti, verilerin toplanması ve raporlanmasında tek bir biçimi destekleyen verileri ifade etmektedir (Tekin & Köksal, 2018). Örneğin Sağlık Net ile toplanması istenen kişisel sağlık bilgilerinin tanımlandığı ve bu verilerin toplanma yöntemlerini tarif eden "Ulusal Sağlık Veri Sözlüğü" veri setlerini göstermektedir (Tekin & Köksal, 2018).

Veri tabanı, bilgilerin toplandığı, depolandığı, yönetildiği ve kullanıldığı veri kaynaklarını ifade etmektedir. Buna göre veri tabanları, belirli bir konudaki, birbiri ile ilişkili olan verilerin düzenli ve sistematik bir şekilde kaydedilebilmesini sağlamaktadır.

Her türden bilgiyi çeşitli amaçlara hizmet edecek şekilde toplayan çok sayıda veri tabanı bulunmaktadır. Kurumların amaçlarına uygun olarak kullandıkları veri tabanları farklılık göstermektedir. Microsoft'un ardından dünyanın en büyük ikinci yazılım

şirketi olan Oracle Türkiye, bazı veri tabanları örneklerini şu şekilde tanımlamaktadır (Oracle, 2021);

- İlişkisel veri tabanları: Öğeler, sütunlar ve satırlardan oluşan bir tablo kümesi şeklinde organize edilen veri tabanlarını ifade eder. Yapılandırılmış bilgilere en verimli ve esnek şekilde erişim imkanı sağlar.
- Nesne odaklı veri tabanları: Bu veri tabanındaki bilgiler, nesneler biçiminde temsil edilir.
- Veri ambarları: Merkezi bir veri havuzudur. Özel olarak hızlı sorgulama ve analiz amaçlarıyla tasarlanmış bir veri tabanı türüdür.
- NoSQL veri tabanları: Bir NoSQL veya ilişkisel olmayan veri tabanı yapılandırılmamış ve yarı yapılandırılmış verilerin depolanmasına ve değiştirilmesine olanak tanımaktadır.
- Açık kaynak veri tabanları: Kaynak kodu açık kaynak olan bir sistemdir. SQL ve NoSQL veri tabanları olabilir.
- Bulut veri tabanları: Bir bulut veri tabanı özel, genel veya hibrit bulut bilgi işlem platformunda bulunan yapılandırılmış veya yapılandırılmamış bir veri koleksiyonudur.

Sağlık hizmetlerinde kullanılan elektronik veri tabanları, yukarıda belirtilen veri tabanlarından ilişkisel ve nesne odaklı veri tabanları türü içinde tanımlanabilir.

2.1.2.3.Veri işleme kavramı

Avrupa Veri Koruma Yönetmeliği (GDPR), "işleme" kavramını toplama, kaydetme, düzenleme, yapılandırma, depolama, uyarlama veya değiştirme, geri alma, kullanma, açıklama, yayma veya başka bir şekilde kullanıma sokma, sıralama veya birleştirme, kısıtlama, silme ve/veya imha etme gibi otomatik araçlarla olsun veya olmasın, kişisel veriler veya veri kümeleri üzerinde gerçekleştirilen herhangi bir işlem veya işlem dizisi biçiminde tanımlanmaktadır (GDPR, 2016). Bu kapsamlı tanımda belirtildiği üzere kişisel bilgiye her bir dokunuş, veri işleme olarak kabul edilmektedir.

"Veri işleme" kavramı ise Kişisel Verilerin Korunması Kanunu'nun (KVK Kanunu) 3. maddesinde tanımlanmaktadır (Kişisel Verileri Koruma Kanunu, 2016);

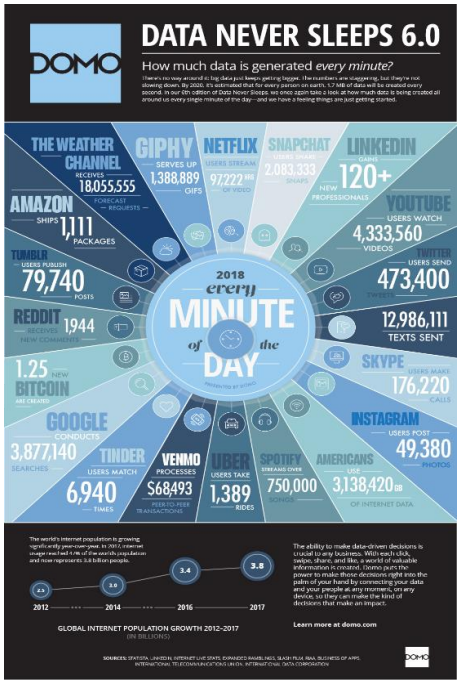
> “Kişisel verilerin tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla elde edilmesi, kaydedilmesi, depolanması, muhafaza edilmesi, değiştirilmesi, yeniden düzenlenmesi, açıklanması, aktarılması, devralınması, elde edilebilir hale getirilmesi, sınıflandırılması ya da kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlem”

İki tanımdan anlaşılacağı üzere, verilerin elde edilmesi, depolanması, kullanılması ve imha edilmesi başta olmak üzere kişisel bilgi üzerindeki her türlü eylem veya kişisel bilgiye dokunuş veri işleme olarak kabul görmektedir.

Veri işleyenin kim olduğuna açıklık getirmek konusunda GDPR, ayrıca “işleyen” kavramını tanımlamıştır. Buna göre işleyen kişi, yönetici adına kişisel verileri işleyen gerçek veya tüzel kişi, kamu otoritesi veya organı şeklinde tanımlanmaktadır. KVK Kanunu’na göre ise veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi ifade etmektedir.

2.1.3. Verinin nitelikli bilgiye dönüşümü

Günümüzde birçok uygulama aracılığı ile oldukça fazla veri işlenmektedir. Şirketlerin yalnızca 2018 yılında bir ayın her dakikasında üretilen veri miktarı Görsel 1’de gösterilmektedir.



Görsel 1. 2018 yılında bir ayın her dakikasında üretilen veri miktarı
(kaynak: https://www.domo.com/learn/infographic/data-never-sleeps-6)

Toplanan bu kadar fazla ham verinin teknoloji şirketleri tarafından kullanılabilmesi için enformasyona *(information)* dönüştürülmesi gerekmektedir. Bilgiye göre daha dar bir anlamı olan enformasyon kısaca, verinin belli bir formülle düzenlenmesini (sınıflandırma, gruplandırma vs.) ifade etmektedir. En küçük bilgi parçacığından yola çıkarak olay ve olguları tanıma, anlama ve özellikle açıklamaya yönelik, eğitim, gözlem, araştırma veya deneyim yoluyla elde edilen ve insanın zihinsel değerlendirmesi ile ortaya çıkan olgular veya fikirler bilgi *(knowledge)*'dir (AÖF, 2021). Diğer bir deyişle ham halde bulunan verinin anlamlı hale getirilmesi sürecinin sonunda bilgi ortaya çıkmaktadır. Enformasyona dönüşen verinin rasyonel bir biçimde akıl süzgecinden geçerek yorumlanması gerekir. Yorumlanarak kullanılması sonucu bilgi ortaya çıkar. Dr. John Snow'un kolera salgınına yaklaşımı burada da anımsatılabilir. Verinin bu dönüşüm süreci "veri hiyerarşisi" olarak adlandırılmaktadır (Uçar & İlkılıç, 2020).

İşlenen verilerin nitelikli bilgiye dönüşümü Büyük Veri analizi yöntemiyle oldukça kolaydır. Gün geçtikçe çoğalan ham verinin nitelikli bilgiye dönüştürülmesi sürecinde farklı Büyük Veri analiz yöntemleri kullanılmaktadır. Büyük Veri analizinin temelinde, tek değişkenli istatistik modellerin koşulları oluşturulmadığı durumlarda çok değişkenli istatistik yöntemlerin kullanılması anlayışı vardır (Ankaralı, 2020). Bu yöntemlerin en çok kullanılanı ve en önemlileri veri madenciliği, makine öğrenmesi ve metin madenciliği yöntemleridir. Veri istatistiği için özellikler arası ilişkilerin bilgisayarlara öğretilmesi makine öğrenmesi; metinlerin sınıflandırılması, gruplanması, metinlerden konu çıkarılması ve özetleme, duygusal analiz ve varlık ilişki modellemesi hedefleri metin madenciliğidir (Ankaralı, 2020). Piatetsky-Shapiro'ya göre, veriden anlamlı ilişkiler ve örüntüler çıkarma sürecine, "veri madenciliği", "bilgi çıkarımı", "bilgi keşfi" gibi isimler verilmektedir (aktaran Balkan, 2020). Buna göre nitelikli bilgiyi, veri madenciliği teknolojisi içeren uygulamalar sayesinde, veri içerisindeki gizli eğilim ve örüntülerin ortaya çıkarılması biçiminde tanımlamak mümkündür (Balkan, 2020).

2.2.Kişisel Verinin Tanımı

Kişisel veri kavramının tam olarak ne anlama geldiği konusunda uzlaşı sağlanmış bir tanım bulunmamakla birlikte, kişiyi belirlenebilir kılan her türlü bilgi kişisel veri

şeklinde kabul görmektedir. Dülger'e göre kişisel verinin tanımı kabaca ikiye ayrılmaktadır. Birinci grupta, "insanın varoluşundan kaynaklanan kişiliğine ilişkin bilgiler" bulunurken ikinci grupta, "insanın modern bilişim toplumunda yer alması nedeniyle kendisine verilen ya da çeşitli hizmetlere ulaşmasında kullanılan bilgiler" bulunmaktadır (Dülger, 2020). Türk Dil Kurumu'nun (TDK) kişisel veri tanımı incelendiğinde, "kişisel" kelimesi, "kişi ile ilgili, kişiye ilişkin, kişinin kendi malı olan, şahsi, zati" şeklinde tanımlanmaktadır (TDK, 2022a). Bu tanıma göre "kişisel" sözcüğü "veri" ile birlikte kullanıldığında "kişi ile ilgili, kişiye ilişkin olan bilgi veya veri" anlamına gelmektedir. Uluslararası belgelerde "personal data" biçiminde kullanılan kavramda geçen "data" sözcüğünün bazı Türkçe kaynaklarda "veri", bazılarında "bilgi" olarak kullanıldığı ifade edilmektedir (Boz, 2014).

KVK Kanunu'nda kişisel veri, "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" biçiminde tanımlanmaktadır (Kişisel Verileri Koruma Kanunu, 2016). Tanımın içerisinde yer alan "her türlü bilgi" ifadesine göre kişisel veriler şu şekilde sınıflandırılmaktadır (Kişisel Verileri Koruma Platformu, 2021);

- Kimlik bilgileri: ad soyad, anne-baba adı, anne kızlık soyadı, doğum tarihi, doğum yeri, medeni hali, T.C. kimlik numarası
- İletişim: adres, telefon numarası, e-posta adresi, iletişim adresi, kayıtlı elektronik posta adresi
- Lokasyon: kişinin bulunduğu yerin konum bilgisi
- Özlük bilgileri: bordro bilgileri, disiplin soruşturması, işe giriş çıkış belgesi kayıtları, mal bildirimi bilgileri, özgeçmiş bilgileri, performans değerlendirme raporları
- Hukuki işlem: adli makamlarla yazışmalardaki bilgiler, dava dosyasındaki bilgiler
- Müşteri işlem: çağrı merkezi kayıtları, fatura, senet, çek bilgieri, gişe dekontlarındaki bilgiler, sipariş bilgisi, talep bilgisi
- Fiziksel mekan güvenliği: çalışan ve ziyaretçilerin giriş çıkış kayıt bilgileri, kamera kayıtları
- İşlem güvenliği: IP adresi bilgileri, internet sitesi giriş çıkış bilgileri, şifre ve parola bilgileri
- Risk yönetimi: ticari, teknik ve idari risklerin yönetilmesi için işlenen bilgiler

- Finans: finansal performans bilgileri, bilanço bilgileri, kredi ve risk bilgileri, mal varlığı bilgileri
- Mesleki deneyim: diploma bilgileri, gidilen kurslar, meslek içi eğitimler, sertifikalar, transkript bilgileri
- Pazarlama: alışveriş geçmişi bilgileri, anket, çerez kayıtları, kampanya çalışmasıyla elde edilen bilgiler
- Görsel ve işitsel kayıtlar: gerçek kişiye ait fotoğraf, ses kayıtları, video

Bu verilerin doğrudan ya da dolaylı olarak gerçek bir kişiyle ilişkilendirilmesi yoluyla kişinin tanımlanabilmesi durumu, kişinin belirlenebilir kılınması anlamına gelir. Örneğin bir kişinin verilerinin sigorta numarası veya kimlik numarası ile ilişkilendirilmesi sonucunda kişi belirlenebilir hale gelmektedir.

Yargıtay 12. Ceza Dairesinin 23.03.2016 tarihli ve 2016/2472 esas, 2016/4849 sayılı kararda kişisel veri ayrıntılı bir şekilde tanımlanmaktadır;

> "(...) Belirli veya belirlenebilir bir kişiye ait her türlü bilginin, başkasına verilmesi, yayılması ya da ele geçirilmesi, TCK'nın 136/1. maddesinde 'Verileri hukuka aykırı olarak verme veya ele geçirme' başlığı altında suç olarak tanımlanmış olup, eylemin; kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak ya da belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle gerçekleşmesi hali, aynı Kanunun 137. maddesinde cezada artırım nedeni olarak öngörülmüştür. Verileri hukuka aykırı olarak verme veya ele geçirme suçunun maddi konusunu oluşturan 'kişisel veri' kavramından, kişinin, yetkisiz üçüncü kişilerin bilgisine sunmadığı, istediğinde başka kişilere açıklayarak ancak sınırlı bir çevre ile paylaştığı nüfus bilgileri (T.C. kimlik numarası, adı, soyadı, doğum yeri ve tarihi, anne ve baba adı gibi), adli sicil kaydı, yerleşim yeri, eğitim durumu, mesleği, banka hesap bilgileri, telefon numarası, elektronik posta adresi, kan grubu, medeni hali, parmak izi, DNA'sı, saç, tükürük, tırnak gibi biyolojik örnekleri, cinsel ve ahlaki eğilimi, sağlık bilgileri, etnik kökeni, siyasi, felsefi ve dini görüşü, sendikal bağlantıları gibi kişinin kimliğini belirleyen veya belirlenebilir kılan, kişiyi toplumda yer alan diğer bireylerden ayıran ve onun niteliklerini ortaya koymaya elverişli, gerçek kişiye ait her türlü bilginin anlaşılması gerekir (...)"

Tanımdan da anlaşılacağı üzere kişisel veri, kişinin adı soyadı, doğum tarihi, doğum yeri gibi kimlik bilgilerinin yanı sıra kişinin sağlık, genetik, psikolojik, etnik, dini, ailevi, siyasi, fiziksel, ekonomik, sosyal vs. özelliklerine ilişkin bilgilerin tamamı

kişisel veri kapsamındadır. Bu özelliklere sahip bir bilgi ile kişiyi herhangi bir şekilde belirlenebilir kılan bir bilginin bir araya getirilmesi ile oluşan bilgi, kişisel veridir.

2.2.1. Özel nitelikte (hassas) kişisel veri

Bazı verilerin daha fazla korunması gerekmektedir. Bu nedenle "özel nitelikli kişisel veri" kavramı tanımlamakdır. Özel nitelikli veriler, kişiyi mağdur etme ve kişi hakkında ayrımcılığa yol açabilme potansiyeline sahip bilgileri ifade ederler.

KVK Kanun'da özel nitelikli kişisel veri,"Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri" (Md. 6) biçiminde tanımlanmaktadır (Kişisel Verileri Koruma Kanunu, 2016). Tanımda belirtilen genetik veriler, bir kişinin fizyolojisi ve sağlığı hakkında benzersiz bilgiler veren, gerçek kişinin biyolojik örneğinin analizinden kaynaklanan, kalıtsal veya edinilmiş genetik özelliklerle ilgili kişisel verileri ifade etmektedir. Biyometrik veriler ise, yüz görüntüleri veya parmak izinden kimlik saptama işlemlerinin yapılması gibi gerçek kişinin benzersiz kimliğinin belirlenmesine izin veren kişisel verileri ifade etmektedir. Kanunun maddesinde ayrıca "Burada sayılan kişisel verilerin, başkaları tarafından öğrenildiği takdirde ilgili kişinin mağdur olabilmesine veya ayrımcılığa maruz kalabilmesine neden olabilecek nitelikte veriler özel nitelikte (hassas) veri olarak kabul edilmektedir" (Md. 6) şeklinde bir açıklama ifadesi de bulunmaktadır (Kişisel Verileri Koruma Kanunu, 2016).

Kişiye ait fiziksel veya ruhsal sağlığına ilişkin her türlü bilgi, kişisel sağlık verilerini oluşturmaktadır. Bu kapsamda kişisel sağlık verileri özel nitelikli veya hassas veri kategorisinde yer almaktadır. 108 sayılı Avrupa Konseyi Sözleşmesi, Birleşmiş Milletler Rehber İlkeleri, 95/46/EC sayılı Direktif ve GDPR gibi uluslararası düzenlemeler, özel nitelikli kişisel verileri kişisel veriden ayırarak ifade etmektedir (Dülger, 2020).

Tablo 2. Hassas verinin içerdiği anlama ilişkin düzenlemerin karşılaştırılması (Boz, 2014)

KVKKT 7. Md.	**TCK 135. Md.**	**AB 95/46/EC Direktifi 8. Md.**	**AK 108 sayılı Sözleşme 6. Md.**
Irk	Irki köken	Irki, etnik köken	Irki köken
Siyasi düşünce	Siyasi görüş	Siyasi görüş	Siyasi düşünce
Felsefi inanç	Felsefi görüş	Felsefi inanç	Diğer inançlar
Dernek, vakıf, sendika üyeliği	Sendikal bağlantı	Sendika üyeliği	
Sağlık	Sağlık durumu	Sağlık durumu	Sağlık durumu
Özel yaşam			
	Cinsel yaşam	Cinsel yaşam	Cinsel yaşam
	Ahlaki eğilim		
Her türlü mahkumiyet		Ceza mahkumiyeti	Ceza mahkumiyeti

Literatürde hassas verinin tanımına ilişkin çeşitli tartışmalar mevcuttur. Tablo 2'de kişisel verileri konu alan düzenlemelerde geçen hassas veri kavramının hangi anlamlarda kullanıldığı karşılaştırılmaktadır.

2.2.2. Mahremiyet kavramı

Mahremiyet kavramı, İngilizce *privacy* sözcüğünün Türkçe karşılığı olarak çevrilmekte ve bazı metinlerde "özel yaşamın gizliliği" biçiminde tanımlanmaktadır (Küzeci, 2010, s.13). Latince *privatus* sözcüğünden türeyen kavram aynı kökenden gelen *privatum* sözcüğü de ev gibi özel varlıkları içeren bir anlamda kullanılmaktadır (Dülger, 2020). Türkçe'deki sözlük anlamına bakıldığında TDK tarafından "gizlilik" biçiminde tanımlanmaktadır (TDK, 2022b). Bir başka mahremiyet tanımında, "kişinin herkesle paylaşmayacağı veya herhangi bir kimse ile paylaşmamak hakkının bulunduğu olay, inanç veya duygularının, isteği üzerine o kişiyle paylaşılması" durumunu ifade eden *intimacy* kavramının karşılığı olarak ifade edilmektedir (aktaran Küzeci, 2010, s.14).

Mahremiyet kavramının tanımı oldukça geniştir. Tarih boyunca dönemin anlayışına bağlı olarak değişkenlik göstermiş ve farklı anlamlara sahip olmuştur. Örneğin 1950'lerde mahrem alan, özel alan, sosyal alan veya kamusal alan gibi kullanımları olan "alan" kavramı ile ilişkilendirilmiştir (Dülger, 2020). Dijital dünyadaki mahremiyeti ayrıntılı bir şekilde inceleyen Lokke'a göre mahremiyet, "Kişinin, kişisel

bilgilerini denetleyebilmesi ve bu bilgilerin akıbetine mümkün olduğunca kendisinin karar vermesi, ayrıca başkalarının kendisi hakkında hangi bilgilere sahip olduğunu bilme hakkı" dır (Lokke, 1980, s.24). Çeşitli şekillerde ifade edilen mahremiyet, insanın kendi bedenine, zihnine ve gelişimine yani kendi varoluş koşullarına sahip olma ya da olmaya çalışma özgürlüğü ile ilişkilendirilmektedir (Şahin, 2020).

Mahremiyet, özellikle hasta-hekim ilişkisindeki güvene dayalı ilişkiyi koruyan tıp etiğinin en önemli kavramlarından biridir. Sağlıkla ilgili birçok belgede mahremiyetin önemi vurgulanmaktadır. Bu metinlerden en eskisi hasta-hekim ilişkisi kapsamında düzenlenen Hipokrat Yemini'dir. Güncellenen haliyle Hekimlik Andı şeklinde uyarlanan metinde, "Hastamın bana açtığı sırları, yaşamını yitirdikten sonra bile gizli tutacağıma" şeklinde hekimin sır saklama yükümlülüğü kapsamında değerlendirilmektedir (TTB, 2017). And'ın bu ifadesinde hekimin bilgileri gizli tutma ödevinde herhangi bir ayrıcalık tanınmamakta ve hatta hastanın ölümünden sonra dahi sırlarını saklamayı sürdürmesi gerektiği bildirilmektedir. "Sır" ise, hasta ve hekim arasındaki her türlü bilgi biçiminde ifade edilebilir. Hekimin sır saklama yükümlülüğünün başlangıcı, mahremiyet kavramı ile doğrudan ilişkilidir. Hekimin sır saklama yükümlülüğü ve buna bağlı olarak mahremiyet kavramı hasta-hekim ilişkisindeki güveni belirleyen en önemli iki kavramdır. Avrupa İnsan Hakları Mahkemesinin *data protection* ile ilgili rehberinde hastanın özel hayatına saygı gösterilmesi, yalnızca hastanın mahremiyet duygusuna saygı göstermek için değil, aynı zamanda tıp mesleğine ve genel olarak sağlık hizmetlerine olan güvenini korumak için de önemli olduğu belirtilmektedir (ECHR, 2021). Aksi durumda hasta, sağlık kurumuna gelmek istemeyebilir veya sağlık durumunu ilgilendiren bilgileri hekimden saklayabilir.

Mahremiyetin özellikle psikiyatride özel bir yeri olduğu sıkça vurgulanmaktadır. Çünkü bu uzmanlık dalının özelliği gereği hastanın hekim karşısında sadece bedeni ile değil ruhu ile de çıplak ve savunmasız kaldığı ifade edilmektedir (Arslan Hızal, 2018).

Mahremiyet ve gizlilik çoğunlukla birbirinin yerine kullanılabilmektedir. Örneğin TDK mahremiyeti, "gizlilik" olarak tanımlamaktadır (TDK, 2022b). Bu iki kavramın birbirinden farklı olduğunu belirtmek gerekir. Buna göre mahremiyet, sadece bilgi ile

sınırlı olmayan, bireylerin özel alanında tanımladığı ve başkasının görmesini istemediği her şeydir. Buna sadece kişinin kendisi karar verebilir. Bu bağlamda mahremiyet kişinin özerkliğini koruma yollarından biri olarak belirtilebilir. Edward Snowden mahremiyetin önemine şu cümleleri ile dikkat çekmektedir; "Çağdaş yaşamda devletin dışarıda bırakıldığı tüm bu negatif ya da olası alanı kapsayan tek bir kavramımız var: 'özel hayat'. Burası, devletin elinin uzanmadığı boş bir bölge, yasanın içinde dolaşmasının ancak izinle mümkün olduğu bir boşluk." (Snowden, 2020, s.239). Gizlilik ise kişi hakkında işlenen bilgilerin gizli tutulmasıdır. Buna göre gizlilik, bilgi ve belgelerin güvenli bir şekilde saklanması ve başkalarının yetkisiz erişiminden korunması eylemlerini ifade etmektedir.

2.3.Gözetim Toplumunda Büyük Veri

Fransızca kökenli olan gözetim sözcüğünün ilk kez 18. yüzyılın sonlarına doğru bir kişinin hareketlerinin yakından izlenmesi anlamına gelecek şekilde kullanılmaya başlandığı belirtilmektedir (Dülger, 2020). Yeni bir olgu olmayan gözetim, bir veya birden fazla kişinin özellikle elektronik cihazlar aracılığıyla bütün eylemlerinin sistematik bir şekilde izlenmesi demektir (Dülger, 2020).

Mahremiyete yönelik en önemli tehdit kaynaklarından biri gözetimdir. Mahremiyet hakkını ve sosyo-tarihsel gelişimini inceleyen Yüksel'in Breckendridge'den aktardığına göre "Hızlı bir şekilde mahremiyetin olmadığı bir çağa giriyoruz. Herkes, her zaman gözetime açıktır. Hükümetten saklanabilecek hiçbir sır kalmamıştır. Hükümet tarafından mahremiyete yönelik aşırı ihlaller, geometrik diziyle artmaktadır. Herhangi bir etkin yasal ve yargısal denetim olmaksızın, telefon dinleme ve gizli kayıt faaliyetleri önlenemez yaygın bir hal almaktadır. Hükümet birimlerindeki gizli gözetleme birimlerinden endüstri alanındaki kapalı devre televizyon devrelerine ve dinlenme odalarına kadar uzanan gizli gözetleme, ortak bir karakter taşımaktadır. Hükümetin selameti bakımından bürolar, konferans salonları, otel odaları ve hatta yatak odaları bile gizli olarak dinlenmektedir" (Yüksel, 2014).

Filozofların gözetim kavramına yaklaşımları incelendiğinde, Karl Marx üretim sürecinden hareket ederek gözetim olgusunu sınıf ilişkileri bağlamında analiz ederken, Max Weber, bir gözetim unsuru olarak bürokrasiyi incelemiştir (aktaran Arslantaş-

Toktaş ve ark., 2012). Gözetime ilişkin en çarpıcı vurguyu ise postmodern filozof Michel Foucault yapmıştır. Foucault, Jeremy Bentham'ın 18. yüzyılda hapishane modeli olarak tasarladığı "panoptikon" kavramını daha geniş biçimde ele alarak bütün toplumun gözetimi şeklinde incelemiş ve iktidarın her yerde oluşuna vurgu yaparak açıklamıştır (Arslantaş-Toktaş ve ark., 2012). Bentham'ın mimari bir yapı olarak tasarladığı panoptikon modeli, modern toplumlardaki gözetim olgusunu açıklamak için kullanılan bir metefor olarak bilinmektedir. Buna göre günümüzün panoptikon anlayışı, Foucault'un iktidar üzerinden tanımladığı şekilde devam ettiği belirtilebilir. Çeşitli iktidar örnekleri bu konuda anımsatılabilir. Örneğin 2001 yılı Amerika başkanı George W. Bush yönetiminde, yasadışı bir biçimde Ulusal Güvenlik Dairesi'ne (NSA) gizlice Amerikalıların elektronik iletişimlerini izleme emri verilmiştir (Greenwald, 2015). Devletlerin "güvenlik" kaygısı ile oluşabilecek zararları önlemek için gerektiğinde hukuku çiğnemek de dahil olmak üzere her şeyi yapma hakkını kendinde gören Amerika Birleşik Devletleri, gizlice toplumu gözetlemiş ve günlük hayatın içindeki en mahrem bilgileri kaydetmiştir. Özellikle 11 Eylül sonrasında toplumda oluşan güvenlik kaygısı, gözetimin oluşmasına zemin hazırlamıştır. Bu konuda terör siyasetinin terörün kendisinden daha güçlü bir hale geldiğini belirten CIA ve NSA teknoloji ajanı Edward Snowden, hükümetin ve istihbarat örgütlerinin tüm dünyayı gözetlediğini belgeleriyle ifşa etmiştir. Onun bu ifşası, George Orwell'ın 1984 distopyasındaki "Büyük birader seni izliyor" ifadesinin gerçeğe dönüştüğünü kanıtlar niteliktedir. Snowden ayrıca kitlesel gözetimin tehlikesini şu şekilde ifade etmektedir; "Sırf yaşayarak ya da yaşarken gözetlenmemize izin vererek ürettiğimiz veriyle özel şirketler zenginleşecek, özel yaşamımız da bununla orantılı olarak kaybolacaktır. Eğer devlet gözetimi, yurttaşı devlet gücünün affına tabi bir nesneye çeviriyorsa, şirket gözetimi de tüketiciyi şirketlerin başka şirketlere, veri simsarlarına ve reklamcılara sattığı bir ürüne çeviriyordu." (Snowden, 2020, s.222).

Dahası Bentham'ın hapishane modeli olarak tasarladığı panoptikon modeli dikkate alındığında, dünyanın tamamının bir panoptikon haline geldiği belirtilebilir. Panoptikonun insanlarda her an gözetleniyor olma hissi yaratması ve bu hissin kısa sürede doğallaşarak insanlarda boyun eğmeyi kolaylaştırmasını Foucault, "biyo-iktidar" olarak kavramsallaştırmıştır (Arslantaş-Toktaş ve ark., 2012). Sürekli

izlendiğinin farkında olan bir kişi, kısa sürede korkan ve itaat eden biri haline gelecektir (Greenwald, 2015).

Sistem Hatası isimli kitabında Snowden, dünyadaki gözetim tehdidi karşısında, dijital çağda mahremiyetin nasıl sağlanacağı sorusuna karşılık, her türlü gözetimle savaşmak için tek umudun "şifreleme"den geçtiğini bildirmektedir (Snowden, 2020, s.302). Lokke'a göre "şifreleme" veya "kriptolama", etimolojik olarak, gizli olan ya da saklanan şey anlamına gelmektedir. Bilgiyi koruyan bir araç olarak şifreleme, kişiler için paylaşılması istenmeyen bilgiyi anlaşılmaz hale getirmektedir (Lokke, 1980, s.34).

Buna karşın Jan van Dijk'in 21. yüzyılın sosyal gerçeği olarak ifade ettiği *network society (ağ toplumu)* kavramı, dijital teknoloji ile biraraya geldiğinde elektronik gözetim kaçınılmaz olmaktadır. Bireyin elektronik olarak gözetiminin yapıldığı en önemli panoptikonu ise Büyük Veri olarak ifade edilebilir. Bu anlamda Büyük Veri, ağ toplumunda bilgisayar teknolojisi ile gözetimin önündeki neredeyse bütün engellerin yıkıldığını gösteren bir ifadeye bürünmektedir. Bunun çarpıcı örneklerinden biri giriş bölümünde belirtildiği üzere çevrimiçi kitlesel gözetimdir. Bu gözetim modelinin bir örneği de Türkiye'de yaşanmıştır. Buna göre tüm kullanıcıların internet hareketlerinin yaklaşık bir buçuk yıldır, kimlik bilgileri ve kişisel verileriyle Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından kaydedildiği ortaya çıkmıştır (Eroğlu, 2022). İnternet servis sağlayıcıları, bilgisayar ya da mobil cihaz üzerinden internete bağlanan tüm kullanıcıların trafiğini her saat başı BTK'ya iletmektedir. E-posta ve whatsapp gibi uygulamalardan gönderilen mesaj içerikleri hakkında bilgi içermediği açıklanmaktadır. Ancak bilişim uzmanlarının görüşlerine göre, Türkiye'nin tamamından veri toplanması söz konusu olduğu için Büyük Veri analizi kullanılarak yazışmaların kimler arasında yapıldığına kadar anlaşılabileceği ifade edilmektedir (Eroğlu, 2022). Bütün bu örnekler göstermektedir ki; Büyük Veriye sahip olmak, gözetim yeteneğinin daha fazla gelişmesi potansiyelini taşımaktır.

2.4.Büyük Veri ve Kişisel Verilerin Korunması İlişkisi

Teknolojinin olanakları sayesinde verinin kaynakları genişlemiş ve çok karmaşık bir veri toplama ağı oluşmuştur. Amerikan Ulusal Güvenlik Kurumu tarafından kullanılan

ve bütün uydu, mikrodalga, hücresel ve fiberotik iletişim trafiğinin tutan ve analiz eden bir sistem olarak tanımlanan Eclehon ve devlet gibi güçlü örgütlerin elinde bulunan geniş çaplı veri toplama araçlarının yanı sıra kişisel verileri toplayan birçok araç mevcuttur (Küzeci, 2010, s.36). Akıllı telefonlar başta olmak üzere akıllı araba ve evler, kredi kartları, sosyal medya uygulamaları, güvenlik kameraları ve çeşitli hizmetleri almak için kullanılan elektronik veri tabanları aktif olarak bilgilerimizi toplamaktadır. Toplanan bu bilgilerden oluşan Büyük Veri, fotoğraflardan videolara, ses kayıtlarından yazılı metinlere kadar hemen her şeyi kapsamaktadır. Her yerden hızla akan ve sürekli artarak yığınlar oluşturan verinin dar bir alanda saklanabilme özelliği kazanması sonucunda Büyük Veri, özellikle şirketler için çok kıymetli hale gelmiştir. Başta Google, Facebook, Twitter ve Youtube şirketleri olmak üzere, kullanıcıya ücretsiz olarak sunulan sosyal medya uygulamaları aracılığıyla tüm kişisel bilgiler çok kolay bir şekilde toplanmakta ve bu uygulamalar aracılığı ile tüm davranışsal hareketlerimiz sürekli olarak izlenmektedir. Bu verilerden bireyin nasıl bir karaktere sahip olduğu, ne zaman nasıl bir tepki vereceği veya hareket edeceği bilgisi üzerine olasılık tahminleri yapılabilmektedir. Bu tahminlerden hareketle kullanıcı profilleri çıkarılmakta ve insanlar şirketlerin hedeflerine uygun bir şekilde sınıflandırılmaktadır. Böylece şirketler Büyük Veriden elde ettikleri müşteri profil analizleri sayesinde kendi satış stratejilerini belirlemekte ve bunu geliştirmektedirler. Dolayısıyla şirketler açısından insanların internette yaptığı her şey izlenmeli, takip edilmeli ve gelecek tahmin algoritmaları oluşturulmalıdır. Zuboff bu durumu "gözetim kapitalizmi" olarak ifade etmektedir (Zuboff, 2021). Ona göre şirketler, yüksek hacimdeki verinin işlenmesiyle çıkarımlarda bulunarak "hedefli reklam" yapmaya odaklanmış ve bundan çok büyük karlar elde etmeye başlamıştır. Bununla birlikte Zuboff, gözetimin reklamlarla başladığını, ancak bunun genele yayıldığını ileri sürmektedir. Bütün bu süreçte gözetim ile bireyin bütün hakikatlerinin ortaya çıkartıldığı ileri sürülebilir.

Çeşitli yöntemlerle toplanan Büyük Veri'nin etkin bir şekilde kullanılması sürecindeki olası riskler karşısında kişisel verinin hukuken korunması ihtiyacını doğurmaktadır. İzleme veya gözetleme, Büyük Veri teknolojisinin kaynakları çeşitlendikçe kolaylaşmaktadır. Bu da kişisel verilerin korunmasını güçleştirmekte veya kişisel verilerin korunmasını ihlal edebilecek eylemleri genişletmektedir. Hatta kişisel

verilerin korunmasını ihlal eden eylemlerin tanımlanması dahi zorlaşmaktadır (Küzeci, 2010). Günümüzde çok büyük sayıda verinin toplanabilir olması, kaydedilmesi ve dijital ortamda aktarılması oldukça kolay hale gelmiştir. Bu kolaylık, kişisel verilerin korunması yönündeki tehlikelerin önlenmesi ihtiyacını doğurmaktadır.

2.5.Uluslararası Düzenlemelerde Kişisel Verinin Korunması

Bilgi veya bilişim çağında her türden bilginin işlenebilir olması kişisel bilgilerin korunmasını zorunlu hale getirmiştir. Çünkü verinin kapladığı alan daralmış, çok kolay bir şekilde işlenen veri, dünyanın herhangi bir yerine aktarılabilir hale gelmiştir. Bu özellikler, verinin ülkelerin ekonomilerinde temel belirleyici rol üstlenmesini sağlamıştır. Bu durumda kişisel verinin ulusal ve uluslararası düzeyde korunması gerektiği anlayışı doğmuş, yaşanan kişilik hakkı ihlalleri karşısında verilerin korunmasına yönelik çeşitli yasal düzenlemeler oluşturulmaya başlanmış ve hukuken bir hak olarak tanımlanması ile yasalarla güvence altına alınmasının gerekli olduğu anlaşılmıştır. Bu bağlamda özel yaşamın gizliliği hakkı tanımlanmış ve birçok uluslararası düzenleme ile güvence altına alınmaya çalışılmıştır. Bu hakkın gelişimine kısaca değinilecek olursa, Brendeis ve arkadaşları, 1980 yılında ilk kez özel yaşama saygı çerçevesinde "mahremiyet hakkı" kavramını tanımlamışlardır (Geuss, 2007). Brandies'in mahremiyet tanımı "yalnız bırakılma hakkı; hakların en kapsamlısı ve özgür insanlar tarafından en çok değer verilen hak" olarak ifade edilmektedir (aktaran İzgi, 2014). Mahremiyet hakkının ihlali konusunda Amerika Birleşik Devletleri'nde ilk kesin davanın 1905 yılında karara bağlandığı belirtilmektedir (Öncü, 2009). Kişisel verinin korunmasına ilişkin tartışmalar Amerika'da çıkmış olsa da dünyanın ilk veri koruma kanunu, 1970 yılında Almanya'nın Hessen eyaletinde kabul edilmiştir (Kişisel Verileri Koruma Kurumu, 2018b).

Kişisel verinin uluslararası düzeyde Avrupa Konseyi, OECD, Birleşmiş Milletler ve Avrupa Birliği bünyesindeki düzenlemelerle özel olarak korunmaktadır.

2.5.1. Avrupa Konseyi düzenlemeleri

Kurucu ülkeleri arasında Türkiye'nin de bulunduğu Avrupa Konseyi tarafından hazırlanan ve 1953 yılında yürürlüğe giren İnsan Hakları ve Özgürlüklerinin Korunmasına İlişkin Avrupa Sözleşmesi (AİHS), kişisel verilerin işlenmesi hakkında doğrudan bir düzenleme maddesi içermemekle birlikte "özel ve aile hayatına saygı hakkı" kapsamında kişisel verileri koruma altına almaktadır.

Avrupa Konseyi'nin kişisel verinin korunması yönündeki çalışmaları sonucunda 28 Ocak 1981 tarihinde Strazburg'da imzaya açılan 108 sayılı "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi", 1 Ekim 1985 tarihinde yürürlüğe girmiştir. Sözleşme kişisel verilerin korunması konusunda hukuksal bağlayıcılığı olan geniş kapsamlı ilk uluslararası sözleşme olarak kabul edilmektedir (Kişisel Verileri Koruma Kurumu, 2018b). 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 almak biçimindedir (Boz, 2014). Bu sözleşmenin kişisel veri güvenliğinin artırılması ve gizliliğin sağlanması adına 181 sayılı "Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşmeye Ek Protokol", 8 Kasım 2001 tarihinde kabul edilmiştir. Protokolün 3. maddesinde, protokolün kabul edilebilmesi için ön koşul olarak 108 sayılı sözleşmenin imzalanmış ve yürürlüğe girmiş olması şartı bulunmaktadır. Bu nedenle Türkiye bu protokolü 8 Kasım 2001 tarihinde imzalamış olmasına rağmen onaylayamamış ve yürürlüğe koyamamıştır (Boz, 2014).

Avrupa Komisyonu bu sözleşmeleri güncellemek amacıyla birçok karar almıştır. Buna göre Avrupa Komisyonu Bakanlar Komitesi 108 sayılı Sözleşmenin uygulanmasına yönelik usul ve esasları belirleyen toplam 13 tavsiye kararı çıkarmıştır (Kişisel Verileri Koruma Kurumu, 2018b). Bunlar; 1997 yılı 5 sayılı tavsiye kararı "Tıbbi verilerin korunması", 1997 yılı 18 sayılı tavsiye kararı "İstatistik amaçlı toplanan ve işlenen kişisel verilerin korunması", 1999 yılı 5 sayılı tavsiye kararı "İstatistik amaçlı toplanan ve işlenen kişisel verilerin korunması", 1999 yılı 5 sayılı tavsiye kararı "İnternet üzerinde gizliliğin korunması", 2002 yılı 9 sayılı tavsiye kararı "Sigorta amaçlı

toplanan ve işlenen kişisel verilerin korunması", 2010 yılı 13 sayılı tavsiye kararı "Profil bilgisi içindeki kişisel verilerin otomatik işleme karşısında korunması", 2012 yılı 3 sayılı tavsiye kararı "Arama motorları ile ilgili insan haklarının korunması" ve 2012 yılı 4 sayılı tavsiye kararı "Sosyal ağ hizmetleri ile ilgili insan haklarının korunması" kararlarıdır (Council of Europe, 2020).

2.5.2. Ekonomik İşbirliği ve Kalkınma Teşkilatı (OECD) düzenlemeleri

Aralık 1960 yılında imzalanan Paris Sözleşmesi'ne dayanılarak kurulan ve 30 Eylül 1961'de işlerlik kazanan OECD, II. Dünya Savaşı'nın etkisinde ciddi zarar gören Avrupa'nın Marshall Planı çerçevesinde yeniden toparlanması amacıyla 1948 yılında kurulan Avrupa Ekonomik İşbirliği Örgütüne dayanmaktadır (Boz, 2014).

OECD bünyesinde kişisel verilerin ülkeler arasında transferinin sağlanması için izlenmesi gereken prosedürler belirlenmiştir. Uluslararası bir temel teşkil edecek şekilde 23 Eylül 1980 tarihinde OECD tarafından "Özel Yaşamın Korunması ve Kişisel Verilerin Sınırötesi Akışına İlişkin Rehber İlkeleri" kabul edilmiştir. Tavsiye niteliğinde kararlardan oluşan bu ilkeler, üye ülkelerin yasal düzenlemelerinde toplanan verinin sınırlı olması, verilerin belirli bir niteliği karşılaması ilkesi, veri toplama amacının belirli ve sınırlı olması, veri güvenliği ilkesi, açıklık ilkesi, bireyin katkılımı ve hesap verebilirlik ilkeleri üzerinde durmuştur.

2.5.3. Birleşmiş Milletler

Uluslararası düzeyde söz konusu bireylerin korunması için bir başlangıç olarak kabul edilebilecek düzenleme 1948 yılında kabul edilen Birleşmiş Milletler İnsan Hakları Evrensel Beyannamesi'dir. Bu bildirge özel hayat ve aile yaşamına, düşünce özgürlüğüne önem vermesi ve daha sonra ortaya çıkacak olan kişisel verinin güvenliği açısından yol gösterici bir rehber olarak nitelendirilmektedir (Öncü, 2009).

II. Dünya Savaşı'ndan sonrasında kurulan Birleşmiş Milletler, sağlık, eğitim, temel hak ve özgürlükler, çevre sorunları, kadın ve çocuk hakları, ticaret ve kalkınma gibi birçok konuda önemli çalışmalarda bulunmuştur (Birdişli, 2010). BM'nin kişisel verileri korunması konusundaki ilk adımı 14 Aralık 1990 tarihinde; 45/95 sayılı "Bilgisayarla İşlenen Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri" kılavuz belgesi

ile atılmıştır (Bakırel, 2020). On maddeden oluşan ve üye devletlerin veri korunması alanında asgari bir standarda kavuşmasını amaçlayan bu ilkelerin uygulanması üye ülkelerin inisiyatifine bırakılmıştır (Dinç, 2006).

2.5.4. Avrupa Birliği düzenlemeleri

Son olarak II. Dünya Savaşı sonrasında ortaya çıkan çıkar çatışmalarının olası zararlarını engellemek amacıyla gelişen Avrupa Birliği'nin de kişisel verinin korunmasına ilişkin başlıca iki önemli düzenlemesi bulunmaktadır. Bunlardan ilki 1995 yılında kabul edilen 95/46 /EC sayılı "Avrupa Parlamentosu ve Avrupa Konseyi Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Direktif"tir. Direktifin temel amacı, Avrupa Birliği üye ülkelerindeki kişisel verilerin korunmasına ilişkin düzenlemelerin uyumlaştırılması biçiminde belirtilmektedir (Kişisel Verileri Koruma Kurumu, 2018b).

Avrupa Birliği'ne üye ülkeler, kişisel verilerin korunmasına ilişkin kendi yasal düzenlemelerini bu direktifi esas alarak gerçekleştirmişlerdir. 6698 sayılı Kişisel Verileri Koruma Kanunu'nun hazırlanmasında da bu direktifin esas alındığı bildirilmektedir (Boz, 2014). Avrupa Birliği'nde kişisel verilerin korunmasına yönelik 95/46/EC sayılı Direktif ile başlayan süreç, 2002/58/EC sayılı Direktif ile devam etmiş ve sonunda 2016 yılında, 25 Mayıs 2018'de yürürlüğe girmek üzere Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR) çıkarılmıştır (Kart, 2019).

2.6.Ulusal Düzenlemelerde Kişisel Veri

Türkiye'de kişisel verinin korunması yönündeki yasal zemin, 2010 yılında Anayasa değişikliğine gidilerek oluşmaya başlamıştır. Kişisel verilerin korunması ilk kez 2004 yılında yürürlüğe giren "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğin Korunması Hakkında Yönetmelik" ile gündeme geldiği bildirilmektedir (Bakırel, 2020). Daha sonra 2005 yılında yürürlüğe giren 5237 sayılı Türk Ceza Kanunu ile de ilk defa kanuni düzeyde kişisel verilerin hukuka aykırı biçimde elde edilmesi, kaydedilmesi ve belirlenen süreçler içerisinde yok edilmemesi suç sayılmıştır (Bakırel, 2020). Ancak bu kanunda suç tanımlarında teknik kavramlara yer verilmesi ve tanımlar içeren temel bir kanun olmaması nedeniyle uygulamada sıkıntılar yaşandığı vurgulanmaktadır (Bakırel, 2020).

Kişisel verilerin korunmasına yönelik yasal düzenlemelerin oluşturulması Avrupa'da 1970'li yıllarda yapılmaya başlanırken Türkiye'de doğrudan bir düzenleme oluşturulması süreci, 2014 tarihinde "Kişisel Verilerin Korunması Kanunu Tasarısı" TBMM Başkanlığına sunulmasıyla başlamıştır. Bu tasarı 24 Mart 2016 tarihinde kanunlaşmış ve 6698 sayılı Kişisel Verilerin Korunması Kanunu 7 Nisan 2016 tarihinde resmi gazetede yayımlanarak yürürlüğe girmiştir. Bu kanunun yürürlüğe girmesinden sonra kişisel verinin korunmasıyla ilgili yönetmelik, tebliğ ve Kişisel Verileri Koruma Kurumu'nun çıkardığı veri koruma ile ilgili rehberleri yayınlanmıştır. Ayrıca Türkiye, 1997 tarihinde imzalanan Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Hakları ve İnsan Haysiyetinin Korunması Sözleşmesi: İnsan Hakları ve Biyotıp Sözleşmesi'ni de 2003 yılında kabul etmiştir.

Kişisel Verilerin Korunması Kanunu'ndan (KVK Kanunu) önce kişisel veriler Anayasal korunma ile güvence altındadır. Anayasanın ikinci bölümünde temel hak ve özgürlükler düzenlenmiş ve bu bağlamda, özel hayatın gizliliği kişinin temel haklarından biri olarak kabul edilmektedir. Diğer yandan teknolojide yaşanan hızlı gelişmeler, kişisel verileri hemen her kuruluşun toplamaya başlaması sonucu temel hak ve özgürlüklere müdahale kolaylaşmaya başlamıştır. Bu nedenle kişisel verinin güvenliğiyle ilgili yasal düzenlemeler yapılması ihtiyacı ortaya çıkmıştır (Kişisel Verileri Koruma Kurumu, 2018b). Bu ihtiyaç ilk önce 2010 yılında 5982 sayılı kanunla yapılan Anayasa değişikliği ile giderilmeye çalışılmıştır. Anasayanın 20. maddesine eklenen "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir." fıkrası ile kişisel verinin güvenliği konusuna yer verilmiş ve kişisel verinin korunmasıyla ilgili detaylı düzenlemelerin kanunla yapılacağı belirtilmiştir (T.C. Anayasası, 1982).

KVK Kanunu'nun 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 belirlemek

şeklinde açıklanmıştır (Md.1). Kanun kişisel veriyi, kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi biçiminde oldukça kapsamlı bir biçimde tanımlamaktadır (Md.3). Kanun ayrıca kişisel verinin işlenmesi, anonim hale getirilmesi, veri kayıt sistemi, veri işleyen ve veri sorumlulusunun kim olduğu kavramlarını da açıklamaktadır.

Kanunla korunması amaçlanan kişisel veriler için ayrıca Sağlık Bakanlığı tarafından Kişisel Sağlık Verileri Hakkında Yönetmelik (KSV Yönetmeliği), 2019 yılında yürürlüğe girmiştir. Birçok tartışmayı beraberinde getiren bu yönetmelikte, açık veri, açık sağlık verisi, kişisel verinin işlenmesi, merkezi sağlık veri sistemi gibi kavramlar tanımlanmış, kişisel sağlık verilerinin açıklanması ve aktarılması hususları yer almıştır. Bu durum söz konusu kişilik hakları ve mahremiyete ilişkin tartışmaları beraberinde getirmiştir. Yönetmelikte ayrıca (Md.21/3) "Merkezi sağlık veri sistemine Bakanlıkça belirlenen usul ve esaslara uygun bir şekilde veri gönderimi yapmayan sağlık hizmeti sunucularına, 3359 sayılı Sağık Hizmetleri Temel Kanunu'nun Ek 11 inci maddesinin üçüncü fıkrasına göre işlem tesis edilir." ibaresi ile sağlık kuruluşlarına veri gönderim zorunluluğu getirilmiştir. Bahsi geçen 3359 sayılı Kanunun Ek 11. maddesi ise "Bakanlıkça belirlenen kayıtları uygun şekilde tutmayan veya bildirim zorunluluğunu yerine getirmeyen sağlık kurum ve kuruluşları iki defa uyarılır." biçimindedir. Veri gönderim zorunluluğu ayrıca Özel Hastaneler Yönetmeliği'nde (Md.49/4) "Özel hastaneler tarafından kayıt altına alınan kişisel sağlık verileri, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ikincil düzenlemelere uygun bir şekilde Bakanlıkça belirlenen usul ve esaslar çerçevesinde merkezi sağlık veri sistemine aktarılır ve işlenir. Bakanlık tarafından kurulan kayıt ve bildirim sistemine ve Bakanlıkça yapılacak diğer iş ve işlemlere esas olmak üzere, istenilen bilgi ve belgelerin Bakanlığa gönderilmesi zorunludur." şeklinde belirtilmiştir (Özel Hastaneler Yönetmeliği, 2022).

Türkiye'de KVK Kanunu ile korunan kişisel veriler için ayrıca Kişisel Verileri Koruma Kurulu oluşturulmuştur. Bu kurul, kişisel verilere ilişkin ayrıntılı açıklamalar yapmakta ve kişisel verilerin korunması ile ilgili somut olayları değerlendirerek kanaat ve yaptırımlarını resmi internet sitesinde yayınlamaktadır. Ayrıca Kurulun aldığı karar ve yaptırımlar Resmi Gazetede de yayınlanmaktadır. Kurul, kişisel verileri işleyen

gerçek ve tüzel kişilere yönelik getirdiği yükümlülüklerin en önemlilerinden biri olan Veri Sorumluları Sicil Bilgi Sistemi'ni (VERBİS) hayata geçirmiştir. Kişisel veri sorumluları kişisel veri işlemeye başlamadan önce Başkanlık tarafından oluşturulan ve kamuya açık olan VERBİS'e kaydolmak zorundadırlar.

2.7.Sağlıkta Büyük Veri'nin Yönetimi

Büyük sağlık verileri, gözlemlenebilir bir fenomen hakkında eyleme dönüştürülebilir bilginin çıkarılması sürecini hem kolaylaştıran hem de karmaşıklaştıran, büyük boyutlarının ötesinde bazı benzersiz özelliklere sahip karmaşık veri kümelerini ifade etmektedir (Dinov, 2016). Hastaların demografik özellikleri başta olmak üzere sağlık hizmetindeki tanı ve tedavileri hakkındaki bilgileri, hastalıklar ve hastalıkların önlenmesi ile ilgili bilgileri, fiziksel ve zihinsel bozukluklara dayalı bilgileri, çok hassas nitelikteki bilgiler, Büyük Sağlık verisinin en önemli kaynakları olarak ifade edilmektedir (Dinov, 2016).

Sağlık hizmeti sırasında toplanan hassas bilgilerin yanı sıra fitness izleme cihazları, kan basıncı monitörleri ve kilo tartım terazileri gibi IoT (Nesnelerin İnterneti) cihazları ile hasta tarafından oluşturulan verilerle de bir bireyin günlük yaşam tarzı ve özellikleri hakkında çok kritik bilgiler toplanmaktadır (Altındiş & Kıran Morkoç, 2018).

Çok sayıda hassas bilginin toplanması, Büyük Veri'nin sağlık alanındaki yönetimini önemli hale getirmektedir. Buna göre sağlık alanında toplanan veri türleri üç başlıkta sınıflandırılabilir.

2.7.1. Tıp alanında Büyük Veri

Klinikte toplanan sağlık verileri, en hassas veri türü olarak belirtilebilir. Hastane bilgi kaynakları, cerrahların çalışmaları, anestezi faaliyetleri, fizik muayene, radyografi, manyetik rezonans görüntüleme, bilgisayarlı tomografi, hasta kimlik bilgileri, tanı, tedavi, hekim notları, hemşire bakım planı, sosyal hizmet değerlendirmeleri, taburculuk özeti (epikriz), konsültasyon, ilaç şeması ve değerlendirme raporları ile ilgili tüm bilgiler bu başlık altında toplanmaktadır (Hong ve ark., 2018; Tekin & Köksal, 2018).

Sağlıkta Büyük Veri açısından toplanan bu bilgiler “elektronik sağlık kayıtları”, “tıbbi sağlık kayıtları” ve “kişisel sağlık verileri”; görüntüleme ile ilgili kayıtlar “tıbbi görüntüler ve elektrokardiyogram” biçimlerinde isimlendirilmektedir (Hong ve ark., 2018).

Büyük Veri’nin tıp açısından en önemli yararı, çok sayıda tıbbi kayıt ve görüntülemenin analiz edilmesi yoluyla elde edilen çıktılardır. Bu çıktılarla hastalıkların erken teşhisi yapılabilir ve yeni ilaçlar geliştirilebilir. Günümüz modern tıbbı çoğunlukla veri odaklı olduğu için Büyük sağlık verisi, çok değerlidir.

Diğer yandan Büyük Veri açısından veri odaklı tıbbın önemi, tıp literatürünün yapılandırılmış veri üretiminde öne çıkmaktadır. Modern tıpta sürekli olarak yaşanan gelişmeler, yapılandırılmış bilgilerin yüksek hızda üretilmesini sağlamaktadır (Hong ve ark., 2018). Sağlık alanında yapılan birçok araştırma, bilgiyi yapılandırılmış biçimde sunmaktadır. Bu da Büyük Veri analizi açısından verinin yapılandırılmış bir şekilde Büyük Veriye kaynaklık edeceğini ve çok daha ileri düzey bilgiler üretilebileceği anlamına gelmektedir.

Büyük Veri’nin sağlık alanındaki bir diğer kaynağı, tıbbi literatürün kolaylıkla incelenebildiği biyomedikal veri tabanlarıdır. Bu konuda örneğin sağlık bilimleri konusundan yapılan uluslararası çalışmaların yayımlandığı, yapılan çalışmaların takip edilebildiği biyomedikal veri tabanı PubMed’dir. Bu veritabanı Büyük Veri için çok önemli bir yapılandırılmış veri üretim kaynağı olarak ifade edilebilir.

2.7.2. Halk sağlığı açısından Büyük Veri

Küresel ve ulusal ölçekte mevcut ve gelecekte ortaya çıkabilecek sağlık sorunlarına ilişkin etkili planlama ve uygulama yapabilmek için Halk Sağlığı disiplininden yararlanılır. Halk sağlığı, Sağlıkta Büyük Veri için önemli bir veri alanını temsil etmektedir. Sağlığın geliştirilmesi açısından Büyük Veri, halk sağlığını korumak ve toplum sağlığını geliştirmek gibi bir görev üstlenmesi bakımından oldukça önemli görünmektedir. Günümüzde halk sağlığının korunup geliştirilmesi için daha çok kişilerin fizyolojik özelliklerine odaklanılmaktadır. Özellikle giyilebilir cihazlar, spor ve diyet gibi özellikle mobil cihazlar aracılığıyla tutulan günlük sağlık

kayıtları da Büyük sağlık verisine kaynaklık etmektedir (Hong ve ark., 2018). Yanı sıra Android saatler, Google gözlükler ve diğer mobil sağlık uygulamalarından elde edilen bilgiler bu kapsamda değerlendirilmektedir (Hong ve ark., 2018).

Büyük sağlık verisi, insanların günlük yaşam tarzı ve yaşamları ile ilgili bilgileri ayrıntılı kaydeden cihazları kaynak olarak kullanır. Bu bilgiler hasta-hekim ilişkisi açısından hastalıkların teşhis ve tedavisinde yardımcı olabilmektedir. Bu anlamda halk sağlığı açısından Büyük Sağlık verisi, "birbirini tamamlayan bilgiler" olarak tanımlanmaktadır (Hong ve ark., 2018).

2.7.3. Tıbbi deneylerde Büyük Veri

Sağlık alanındaki Büyük Veri'nin bu türünün daha çok moleküler biyolojiye odaklandığı belirtilmektedir (Hong ve ark., 2018). İnsan vücudu için biyolojik laboratuvar numuneleri de diğer veri türlerine benzer şekilde Büyük Veri'nin kaynağını oluşturmaktadır. Klinik çalışmalar, biyoloji örnekleri, gen dizileri, klinik ve araştırma laboratuvarı testleri ve omics verilerden elde edilen bilgiler bu kapsamda değerlendirlmektedir (Hong ve ark., 2018).

2.8. Türkiye'de Kullanılan Elektronik Sağlık Kayıt Sistemleriyle İlgili Genel Bilgiler

Elektronik sağlık kayıtları, "kişilerin geçmişteki, şimdiki ve gelecekteki fiziksel ve ruhsal sağlığı veya hastalıkları ile ilgili elektronik sistemler kullanılarak kayıt altına alınan, saklanan, iletilen, erişilen, ilişkilendirilen ve işlenen her türlü bilgi" biçiminde tanımlanmaktadır (Sağlık Bakanlığı, 2014a). Bu bilgiler elektronik veri tabanları aracılığıyla kayıt altına alınmaktadır. Hastalara ait demografik bilgiler, hastalık ve tedavi bilgileri, yapılan her türlü tetkik bilgilerinin yanı sıra günümüzde faturalama ve idari işlere ait bilgiler de veri tabanlarına kaydedilmektedir.

Türkiye'de çeşitli düzlemlerde sağlık kayıt sistemleri kullanılmaktadır. Sağlık.NET, Merkezi Hastane Randevu Sistemi (MHRS), Tele-Tıp, Ulusal Sağlık Veri Standartları (USVS), Sağlık Kodlama Referans Sözlüğü (SKRS), Genel Sağlık Sigortası (MEDULA), e-Nabız, e-Reçete uygulamaları ve internet üzerinden sunulan birçok uygulama mevcuttur (Gedik & Yalçınkaya, 2019). SGK'nın kuruluşuyla birlikte

oluşturulan MEDULA adlı elektronik kayıt sistemiyle kişisel sağlık verileri artık daha kapsamlı bir biçimde toplanmaktadır. Ulusal düzeyde e-Nabız, kişisel sağlık veri kayıt sistemi olarak kullanılmaktadır. Sağlık hizmetlerinde sağlık çalışanların kullandığı veri tabanlarına kaydedilen her bilgi, e-Nabız kişisel sağlık kayıt sistemine aktarılmaktadır.

Birinci basamak sağlık hizmetlerinde kullanılan Aile Hekimliği Bilgi Sistemi ve kurumsal düzeyde özel hastane veya üniversite hastanelerinin kendi bünyelerinde kullandığı veri tabanları bulunmaktadır.

Dünya Sağlık Örgütü'nün bildirdiği üzere, Elektronik Sağlık Kaydı bireye ait tüm kişisel sağlık bilgilerini içeren sistemlerden oluşmaktadır. Sağlık hizmeti sağlayıcıları ve bireyin kendisi tarafından yaşam boyunca elektronik olarak kişisel bilgiler girilmekte ve bu bilgilere erişim sağlanmaktadır. Günümüzde elektronik sağlık kayıt sistemlerinin, hastanın bakım aldığı tüm ayakta tedavi ve yatarak tedavi durumlarının ötesine geçtiği belirtilmektedir (WHO, 2019). Bugün sağlık veri tabanları bireyin, hekim tarafından oluşturulan tıbbi kayıtları ile hasta tarafından oluşturulan kişisel sağlık kaydını entegre edecek şekilde tasarlanmaktadır (Garret & Seidman, 2011). Böylece hastanın toplam sağlığına odaklanılacak, standart klinik verilerin ötesine geçilecek ve hastanın bakımı konusunda daha geniş bir bakış açısı sağlanabilecektir (Garret & Seidman, 2011).

Sağlık Bakanlığı, bir elektronik veri kayıt sisteminin taşıması gereken özellikleri aşağıdaki şekilde ifade etmektedir (Sağlık Bakanlığı, 2014a):

- Hasta ile ilgili tüm bilgiler tek bir kayıt numarası ile ilişkilendirilmelidir,
- Sisteme girilen tüm hasta bilgilerine kurumun her yerinden ulaşılabilmelidir,
- Hastaların yakınmaları ve tüm sağlık bakım süreci kaydedilmelidir,
- Tanısal süreçlerde bilgisayar yardımı sağlanabilmelidir,
- Bir bakım planı geliştirilip izlenebilmelidir,
- Sistem kullanılarak isteklerde bulunulabilmeli ve istek sonuçları otomatik olarak alınabilmelidir,
- Verilere kolayca erişim ve kullanma olanağı vermelidir.
- Bir elektronik hasta kayıt sistemi aşağıdaki fonksiyonları da desteklemelidir:

- Hasta randevuları (muayene, yatış, tetkik vb.),
- Yönetim fonksiyonları (finansal yönetim, malzeme yönetimi, insan kaynakları yönetimi),
- Otomatik hastalık ve tıbbi girişim kodlamaları,
- Tanısal tetkik isteklerin üretilmesi ve iletilmesi.

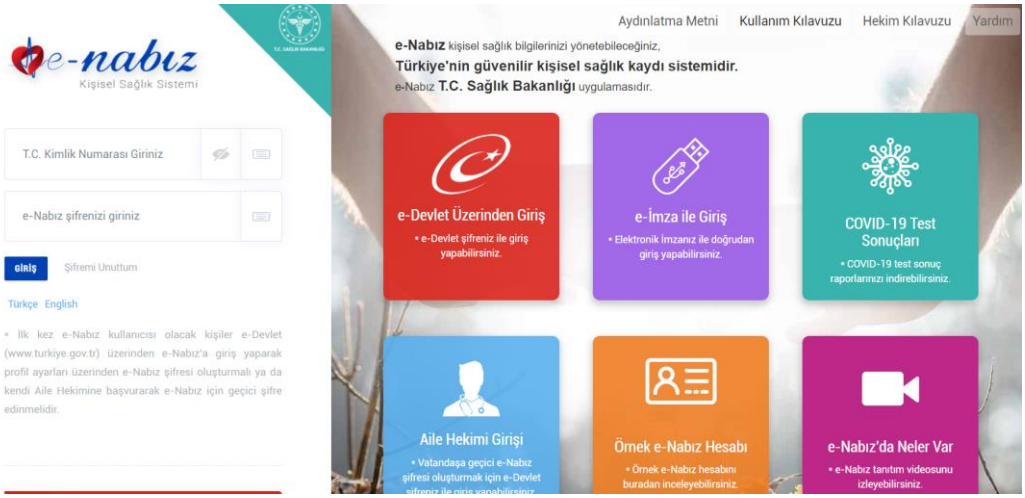
Elektronik sağlık kayıt sistemleri başlangıçta hastalar için sağlık hizmeti sunumunda klinik karar vermeyi kolaylaştırmak ve bakım kalitesini artırmak için tasarlanmıştır (Lee ve ark., 2020). Bu amaçla toplanan bilgilerin, yetkili kullanıcılara gerçek zamanlı ve güvenli bir şekilde hasta merkezli olarak sunulması beklenmektedir (HealthIT, 2020). Dünya Sağlık Örgütü'nün önerdiği sağlık kayıt sistemleri, üç bileşene sahiptir: (1) Hastanın hastaneye ilk gelişinden veya hastaneye gelmesinden itibaren hastanın tüm sağlık bilgilerini içermelidir, (2) Hastanın yaşamı boyunca sağlık bilgileri, sağlık hizmeti sunucuları tarafından girilmelidir ve (3) Hastayla ilgilenen tüm sağlık hizmeti sunucularının bilgilere kolayca ulaşabilmesi sağlanmalıdır (WHO, 2019).

Doğru ve etkili kullanım sağlandığında bu sistemlerin oldukça önemli yararları dile getirilmektedir. Örneğin birinci basamak sağlık hizmetlerinde toplanan bilgiler, acil servis hekimine hastanın yaşamı tehdit eden alerjisi hakkında bilgi verebilir ve böylece hasta bilinçsiz olsa bile bakımı uygun bir şekilde planlanabilir (Garret & Seidman, 2011). Hasta sağlık kurumunu değiştirdiğinde, tedavi süreci daha etkin ve doğru bir biçimde yürütülmesini sağlayabilir. Bunun için hastanın kişisel bilgileri başta olmak üzere tıbbi geçmişi, teşhis ve tedavi planları, aşı tarihleri, radyoloji görüntüleri, laboratuvar test sonuçları gibi birçok bilginin kayıt sistemlerinde bulunması gerekmektedir. Veri tabanlarının daha etkili kullanılabilmesi için birçok farklı sağlık kaydı uygulaması ile entegre bir şekilde çalışması gerekmektedir. Çünkü kurumların kullandığı veri tabanları birbirinden farklı olabilmektedir. Bu durum Türkiye'de e-Nabız ile aşılmaya çalışılmaktadır. Buna göre e-Nabız, sağlık bilgilerinin tek bir merkezde toplanmasını sağlayan kişisel veri kayıt sistemidir.

2.8.1. Kişisel sağlık kayıt sistemi: e-Nabız

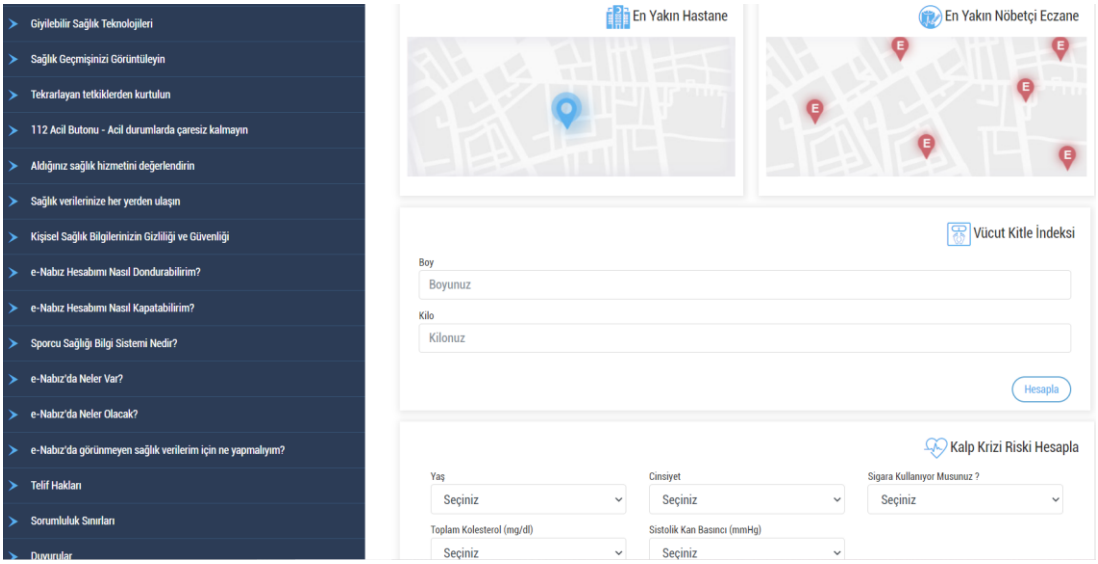
Türkiye'nin kullanmakta olduğu kişisel kayıt sistemi e-Nabız'dır. Sağlık Bakanlığı'nın 2013-2017 Stratejik Eylem Planı'nda "Bireyin kendi sağlığı ile ilgili

kararlara aktif katılımını sağlamak için rolünü güçlendirmek" biçiminde belirtilen hedef ile e-Nabız işaret edilmektedir (Sağlık Bakanlığı, 2012). E-Nabız, "sağlık kuruluşlarından toplanan sağlık verilerine vatandaşların ve sağlık profesyonellerinin internet ve mobil cihazlar üzerinden erişebilecekleri bir uygulama" biçiminde tanımlanmakta, "muayene, tetkik ve tedavilerinizin nerede yapıldığına bakılmaksızın, tüm sağlık bilgilerinizi yönetebildiğiniz, tıbbi özgeçmişinize tek bir yerden ulaşabildiğiniz bir kişisel sağlık kaydı sistemi" şeklinde açıklanmaktadır (Sağlık Bakanlığı, 2020).



Görsel 2. E-Nabız giriş ekranı

E-Nabız kişisel sağlık kayıt sistemi, Birleşmiş Milletler Dünya Bilgi Toplumu İnisiyatifi kapsamında verilen Dünya Zirve Ödülleri'nde "En İyi Sağlık Uygulaması" seçilmiştir. Böylece Sağlık Bakanlığı'nın dünya çapında bir başarı elde ettiği Bakanlık tarafından bildirilmektedir (Sağlık Bakanlığı, 2018).



Görsel 3. E-Nabız örnek kullanıcı ekranı

Sağlık Bakanlığı'nın 2019 verilerine göre 10 milyon kişi e-Nabız kullanmaktadır (Sağlık Bakanlığı, 2019). E-Nabız kullanıcısı, sağlık geçmişi, sağlık profili, profil bilgileri, sağlık tesisi ziyaretleri, reçeteleri, raporları, hastalıkları, tahlilleri, görüntüleri, kemik iliği ve kan bağışı, alerjileri, acil durum notları, dokümanları ve erişim bilgileri konularında kişiselleştirilmiş bir dijital alana sahip olmaktadır. Bu kişisel sayfada kullanıcı, veri ekleme (tansiyon, şeker, nabız, ağırlık), organ bağışı, randevu ve paylaşım yapabilmektedir.

2.8.2. Birinci basamakta kullanılan Aile Hekimliği Bilgi Sistemi (AHBS)

Aile Hekimliği Bilgi Sistemi, 2005 yılında Sağlıkta Dönüşüm Programı ile Sağlık Ocakları Aile Sağlığı Merkezlerine dönüştürülmeye başlanmış ve ilk kez Düzce'de pilot uygulama ile kullanılmaya başlanmıştır.

AHBS, aile hekimlerinin görev ve sorumluluklarını yerine getirmesi için tasarlanan bir veri tabanıdır. Hastaların erişim sağlayamadığı AHBS, aile hekimleri, tıbbı sekreter ve hemşirelerin kullanımına yöneliktir.

2.8.3. Hastane Bilgi Yönetim Sistemi (HBYS)

Hastane Bilgi Yönetim Sistemi, ikinci ve üçüncü basamak veya yataklı tedavi kurumlarında verilen sağlık hizmetleri için kullanılan elektronik sistemlerin bütününü ifade etmektedir.

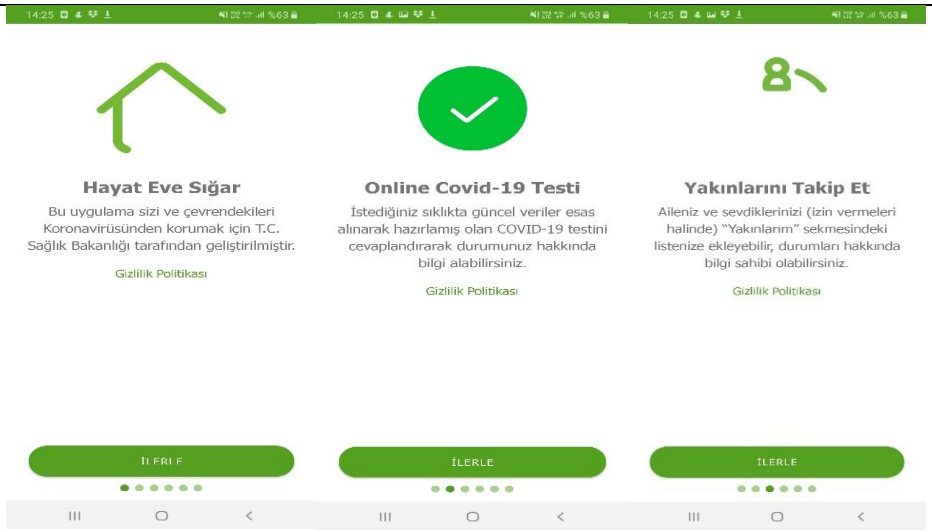
Sağlık Bakanlığı HBYS'yi "bilgisayar programları ve etkileşim içinde olduğu hastanelerin yapmış olduğu işlemleri bilgisayar üzerinde gerçekleştiren yazılımlar grubuna verilen genel ad" biçiminde tanımlamaktadır. Yanı sıra HBYS'nin "laboratuvar, radyoloji gibi tetkik birimlerinde gerçekleştirilen tüm operasyonlardan, ameliyathane, hastane eczanesi, sicil veya insan kaynakları birimlerine varıncaya kadar farklı uzmanlıklar üzerine çalışan birçok yazılımın bir araya gelerek oluşturduğu yazılım grubu" olduğu belirtilmektedir (Sağlık Bakanlığı, 2015).

2.8.4. Covid-19 pandemisi ile uygulamaya koyulan mobil sağlık uygulamaları

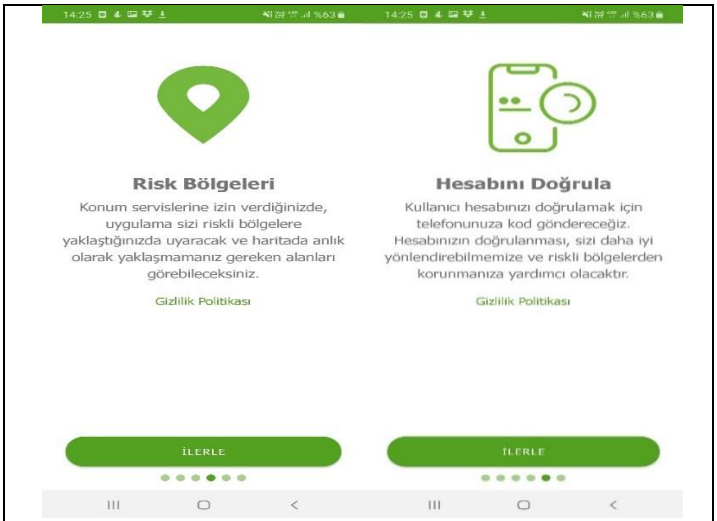
Pandeminin ilan edilmesi ile birlikte ülkede artan korku ve kaygının azaltılabilmesi ve pandeminin önlenebilmesi için teknolojinin olanaklarından da yararlanılmak istenmiştir. Bu amaçla Sağlık Bakanlığı farklı mobil uygulamaları yaşama geçirmiştir. Buna göre Korona Virüs Kontrolü Uygulaması (19 Mart 2020) ve Pandemi İzolasyon Takip Projesi (9 Nisan 2020) uygulamalarını; Hayat Eve Sığar (HES) (18 Nisan 2020) uygulaması adı altında birleştirilmiştir. Daha sonra Bakanlık korona olma ihtimalini değerlendirmeye yönelik bir semptom tanımlama uygulaması olarak, Korona Önlem mobil uygulamayı geliştirmiştir.

Pandemi döneminde temas takip uygulaması olarak planlanan HES mobil uygulaması, T.C. Sağlık Bakanlığı tarafından 18 Nisan 2020 tarihinde "Yeni tip koronavirüs hakkında bilgilendirmek, yönlendirmek, salgın hastalık ile ilgili yaşanabilecek riskleri en az seviyeye indirmek ve yayılmasını önlemek amacıyla geliştirilen mobil uygulama" biçiminde tanımlanmaktadır. Bu uygulamanın içine ayrıca kontrollü bir sosyal hayat yapılmasını amaçlayan HES kodu tanımlanmıştır.

HES uygulaması Sağlık Bakanlığı'nın, Bilgi Teknolojileri ve İletişim Kurumu (BTK) ve GSM operatörleri (Türkcell, Türk Telekom, Vodafone) iş birliğiyle yaşama geçirdiği bir uygulamadır (Çayır, 2020d). Mobil telefonlara indirilen uygulama, telefon numarası ile doğrulama yapıldıktan sonra kullanıma açılmaktadır.



Görsel 4. Hayat Eve Sığar mobil uygulaması ana ekranları



Görsel 5. Hayat Eve Sığar mobil uygulaması ana ekranları

Google Play'de uygulama, "harita üzerinden hastane, eczane, market zincirleri, metro ve duraklar gibi temel ihtiyaç noktalarına kolayca ulaşabilir, evde izolasyon, enfekte kişiler ve riskli bölgelerin yoğunluğunu görebilirsiniz" biçiminde tanıtılmaktadır. Ayrıca bu uygulama ile "Kontrollü Sosyal Hayat" geçişi sağlanabileceği belirtilmektedir.

Covid-19 hastalığı konusunda bilgilendirme ve yönlendirme yapma amacıyla T.C. Sağlık Bakanlığı tarafından kullanıma sunulmuş bir diğer mobil uygulama Korona Önlem uygulamasıdır. Google Play uygulamayı, "T.C. kimlik bilgilerinizi doğrulayarak adım adım size sorulan soruları cevaplayıp korona virüs hastalığına

yakalanmış olma ihtimalinizi öğrenip buna göre yönlendirme alabilirsiniz" biçiminde tanıtmaktadır.

2.9.Uygulamaların Birbirleriyle Entegrasyonu

Türkiye'nin sağlık alanında kullanılan bütün veri kayıt sistemleri birbirleri ile entegredir. Özel veya devlet kurumlarında kullanılan veri tabanları aracılığıyla toplanan kişisel sağlık verileri, Merkezi Sağlık Veri Sistemi veya Ulusal Sağlık Sistemi'nde toplanmaktadır.

Örneğin, laboratuvar programında Covid-19 test sonucu onaylanan kişinin sonuçları anında e-Nabız'a ve Halk Sağlığı Yönetim Sistemine (HSYS) aktarılmaktadır. Halk Sağlığı Yönetim Sistemi'ne aktarılan test sonucu pozitif hastalarını İlçe Sağlık Müdürleri görebilmektedir.

Uygulamalar aynı zamanda İçişleri Bakanlığı'nın kimlik paylaşım sistemi olan Mernis ile entegredir. Hastaların sistemde kayıtlı olmayan bazı kimlik bilgileri Mernis sisteminden çekilebilmektedir.

AHBS ile HSYS sistemi entegrasyonu ile Aile hekimleri evde izolasyondaki hastaların günlük izlemlerini yapabilmektedir.

Son olarak Sağlık Bakanlığı 2021 yılının başında, bütün sağlık hizmetlerini kapsayıcı bir uygulama olan Hastalık Yönetimi Platformu (HYP) uygulamasını hayata geçirmiştir. Diğer uygulamalar da olduğu gibi HYP de e-Nabız ile entegre bir şekilde çalışmaktadır. E-Nabız kişisel sağlık kaydına aktarılan bilgilerin neredeyse tamamı HYP kullanıcısının erişimine açılmaktadır. HYP'nin tanımladığı kullanım yetkisi ile Aile hekimleri, kendisine kayıtlı bireylerin kronik hastalıklara yönelik tarama süreçlerini başlatması, durdurulmuş bir süreci devam ettirebilmesi, iptal etmesi ve sonlandırabilme gibi işlemleri bu sistem üzerinden gerçekleştirebilmektedir. Sağlık profesyonellerine tanınan bu yetki ile birey ve hastalık düzeyinde tarama, izlem sonuçları ve tedavi planına erişim sağlanabileceği ve böylece kronik hastaların erken teşhisi ve kanıta dayalı tıp kılavuzu önerileri doğrultusunda uygun tedavinin gerçekleşebileceği düşünülmektedir (HYP, 2021).

E-Nabız kişisel sağlık kayıt sistemi genel olarak hastaların profil oluşturduğu bir kayıt sistemi iken, HYP sağlık çalışanlarının kullandığı bir sistemdir. Bu uygulama oldukça yeni bir veri tabanı olduğu için, bu çalışmanın kapsamı dışında tutulmuştur.

3. GEREÇ VE YÖNTEM

3.1.Çalışmanın Tasarımı

3.1.1. Uluslararası etik kılavuzların belirlenmesi:

Girişte belirtilen amaca yönelik olarak haklar ve etik değerler açısından soyut bir analiz yapabilmek için, uluslararası rehber/kılavuz olarak tanımlanan veri korumaya yönelik uzlaşı sağlanmış ortak ilkeleri temel almak geçerli bir dayanak noktası olarak kabul edilmiştir. Bu bağlamda uluslararası etik kılavuzlar şu şekilde belirlenmiştir:

- Avrupa Birliği - General Data Protection Regulation (GDPR) (Genel Veri Koruma Düzenlemesi)
    - GDPR'a CPME'in tavsiye metinleri: "Statement on the Proposal for a Regulation on the General Data Protection Regulation" ve "Consent in the field of research General Data Protection Regulation" (2012)
- OECD - Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (2013)
- International Working Group on Data Protection in Telecommunications - Working Paper on Big Data and Privacy Privacy principles under pressure in the age of Big Data analytics (2014),
- NUFFIELD - The collection, linking and research and health care: use of data in biomedical ethical issues (2015),
- Dünya Tabipler Birliği - WMA Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks (2016),
- Avrupa Konseyi - Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data (2017),
- Mobil sağlık uygulamalarının analizi için Avrupa Komisyonu - Guidance on Apps supporting the fight against COVID-19 pandemic in relation to data protection (2020)

İlkelerin oluşturulması: Genel olarak kişisel verinin korunmasına yönelik uluslararası kılavuzlarda belirtilen ilkeler, altı başlık altında gruplandırılmıştır. İlgili metinlerde belirtilen hiçbir ilke dışarıda kalmayacak şekilde dikkate alınmıştır. Kılavuzlarda ileri sürülen öneriler ışığında bu ilkelerin ortak bir tanımı yapılmıştır.

I. Uluslararası Kılavuzlarda Toplum Yararı İlkesinin Yeri:

WMA - Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks: "Araştırma ve diğer sağlık veri tabanları ve biyo-bankalarla ilgili faaliyetler, özellikle halk sağlığı hedefleri olmak üzere toplum yararına katkıda bulunmalıdır. (Md.8)

Bireylerin korunması: Yönetişim, bireylerin haklarının diğer paydaşların ve bilimin çıkarlarından üstün olacağı şekilde tasarlanmalıdır. Şeffaflık: Şeffaflık: Sağlık veritabanları ve biyobankalar ile ilgili her türlü bilgi halka açık olmalıdır. Katılım ve içerme: Sağlık Veritabanlarının ve biyobankaların Sorumluları, bireylere ve topluluklarına danışmalı ve onlarla ilişki kurmalıdır. Hesap verebilirlik: Sağlık veri tabanlarının ve biyo-bankaların sorumluları, tüm paydaşlar için erişilebilir ve duyarlı olmalıdır." (Md.20) (WMA, 2016).

OECD - Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: "Güvenlik önlemleri ilkesi: Kişisel veriler, verilerin kaybolması veya yetkisiz erişim, yok edilmesi, kullanılması, değiştirilmesi veya açıklanması gibi risklere karşı makul güvenlik önlemleri ile korunmalıdır. (Md.11)

Açıklık ilkesi: Kişisel verilere ilişkin gelişmeler, uygulamalar ve politikalar hakkında genel bir açıklık politikası olmalıdır. Kişisel verilerin mevcudiyetini, niteliğini, kullanımlarının temel amaçlarını ve veri sorumlusunun kimliğini ile adresini belirlemeye yönelik araçlar hazır olmalıdır. (Md.12)

Bireysel katılım ilkesi: (a) bir veri sorumlusundan veya başka bir şekilde, veri sorumlusunun kendisiyle ilgili verilere sahip olup olmadığının teyidini almak. b) kendisiyle ilgili verileri makul bir süre içinde kendisine iletmiş olması, varsa, aşırı olmayan bir ücret karşılığında, makul bir şekilde ve onun kolayca anlayabileceği bir biçimde. c) (a) ve (b) bentleri uyarınca yapılan bir talebin reddedilmesi durumunda gerekçe gösterilmesi ve bu reddin reddine itiraz edilebilmesi. d) kendisiyle ilgili verilere itiraz etme ve itiraz başarılı olursa verilerin silinmesini, düzeltilmesini, tamamlanmasını veya değiştirilmesini sağlamak. (Md.13).

Hesap verebilirlik ilkesi: Veri sorumlusu, belirtilen ilkeleri yürürlüğe koyan tedbirlere uymaktan sorumlu olmalıdır. (Md.14) (OECD, 2013).

Avrupa Komisyonu - Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data: "Veri işlemenin şeffaflığı ilkesine göre, Bölüm IV.2'de açıklanan değerlendirme sürecinin sonuçları, kanunla korunan gizliliğe ihlal gelmeksizin kamuya açık hale getirilmelidir. Bu tür bir gizliliğin varlığında, veri sorumlusu her türlü gizli bilgiyi değerlendirme raporunun ayrı bir ekinde sağlar. Bu ek kamuya açık olmayacak, ancak denetim makamları tarafından erişilebilir. (Md.3.3).

Veri sorumluları, kişisel verilerin işlenmesiyle ilgili olarak kişilerin korunmasını sağlamak için Büyük Veri kullanımının risklerine ve bunun bireyler ve toplum üzerindeki etkilerine ilişkin önleyici politikalar benimsemelidir. (Md.2.2)" (Conseil of Europe, 2017).

International Working Group on Data Protection in Telecommunication - Working Paper on Big Data and Privacy: "Gizlilikle ilgili zorluklar; Şeffaflık eksikliği: Kişisel verilerin işlenmesine ilişkin erişim ve bilgi edinme hakkı önemli gizlilik ilkelerini oluşturmaktadır. Verilerin nasıl derlendiğine ve kullanıldığına ilişkin açıklık ve bilgi eksikliği, anlamadığımız ve üzerinde hiçbir kontrolümüz olmayan kararların tuzağına düşmemize neden olabilir. Örneğin, ortalama bir İnternet kullanıcısı, çevrimiçi reklam pazarının nasıl işlediğine ve kişisel verilerinin çok çeşitli ticari taraflarca nasıl toplanıp kullanılabileceğine dair çok az bilgiye sahiptir. Çoğu insan, özellikle veri simsarları ve analiz şirketleri olmak üzere, bu pazarda faaliyet gösteren oyuncuların çoğuna aşina değildir. Bu nedenle, bireyin bilgiye erişim talep etme hakkının kullanılması zorlaşmaktadır. (Md.22).

Her birey hangi verilerin toplandığı, verilerin nasıl işlendiği, hangi amaçlarla kullanılacağı ve verilerin üçüncü kişilere dağıtılıp dağıtılmayacağı konusunda bilgilendirilmelidir." (Md.20) (International Working Group on Data Protection in Telecommunications, 2014b).

Nuffield Council on Bioethics - The collection, linking and use of data in biomedical researc and health care: ethical issues: "Kişilere saygı: Herhangi bir veri girişiminin koşulları hem özel hem de kamu çıkarlarını dikkate almalıdır. İlgili çıkarları olanların verilerinin nasıl kullanıldığı konusunda bireylerin söz sahibi olmalarını sağlamak ve onlara aslında nasıl kullanıldığını söylemek, veri girişimlerinin kişilere saygı gösterebileceği bir yoldur. (9. sayfa, 1. paragraf)

İnsan haklarına saygı: Herhangi bir veri girişiminin koşulları, insanların özel veya aile hayatının korunması hakkı gibi temel haklarına saygı göstermelidir. Bu, devletlerin ve diğerlerinin, kamu yararına bireysel vatandaşların mahremiyetine müdahale etme yetkisi üzerindeki sınırlamaları içerir. (9. sayfa, 1. paragraf)

Katılım: Karar vericiler, sadece insanların verilerinin nasıl kullanılmasını beklemeleri gerektiğini hayal etmemeli, aynı zamanda insanların aslında nasıl kullanıldığını keşfetmek için adımlar atmalı, aslında verilerinin kullanılmasını beklemeli ve bu beklentilerle meşgul olmalıdır. (9. sayfa, 1. paragraf)

Kararların şeffaflığı ilkesi: Veri girişimleri, beklentileri yeniden ayarlamanın bir yolu olarak, düzenleyici, adli ve siyasi prosedürler yoluyla resmi hesap verebilirliğin yanı sıra daha geniş bir halkla periyodik katılım yoluyla sosyal hesap verebilirliği içermelidir. Veri sorumluları, etkilenen kişilere verileriyle ilgili ne yapılacağını, herhangi bir güvenlik ihlali veya ilk politikadan ayrılma/sapma gibi konular dahil olmak üzere verilerle gerçekte ne yapıldığını bildirmelidir." (9. sayfa, 1. paragraf) (Nuffield Council on Bioethics, 2015).

GDPR'ın toplum yararı ilkesi ile ilgili 5, 6 ve 12. maddeleri ekte verilmiştir (EK-1).

Tez kapsamında tanımlanan toplum yararı ilkesi: Toplanan veriler halk sağlığı hedeflerine katkıda bulunmalı ve ortak yol gösterici etik değerler korunmalıdır. Toplum yararı amacıyla veri toplanırken ayrıca insan haklarına saygılı olunmalı, verilerin nasıl kullanıldığı konusunda bireylerin söz sahibi olmaları sağlanmalıdır.

II. Uluslararası Kılavuzlarda Minimum Veri İlkesinin Yeri:

CPME - Statement on the Proposal for a Regulation on the General Data Protection Regulation: "CPME, sağlık verilerinin tıbbi amaçlar dışındaki ikincil kullanımının mutlaka gerekli durumlarda minimum ölçüde ve tam olarak neden kullanılacağı tanımlanarak gerçekleştirilmesinden yanadır; sadece hastanın kişisel bilgileriyle bağlantı kurulmasını önlemeye yönelik anonimleştirme yapılabildiği koşullarda" (2. sayfa 4. paragraf) (CPME, 2012).

OECD - Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: "Veri toplamanın sınırlı tutulması ilkesi: Kişisel verilerin toplanmasına ilişkin sınırlamalar olmalı ve bu tür veriler, yasal ve adil yollarla ve uygun olduğunda, veri sahibinin bilgisi veya rızasıyla elde edilmelidir. (Md.10)

Veri Kalitesi İlkesi: Kişisel veriler, kullanım amaçlarıyla ilgili olmalı ve bu amaçlar için gerekli olduğu ölçüde doğru, eksiksiz ve güncel tutulmalıdır. (Md.8)

Amacın belirlenmesi ilkesi: Kişisel verilerin toplanma amaçları, veri toplamadan önce belirlenmeli ve sonraki kullanım, bu amaçların yerine getirilmesiyle veya bu amaçlarla bağdaşmayan ve her durumda belirtilen diğer amaçlarla sınırlı olmalıdır. (Md.9)

Toplanacak verilerin sınırlı tutulması ilkesinin uygulanması: Kişisel veriler, aşağıdakiler dışında, Madde 9'da belirtilen amaçlar dışında açıklanmamalı, erişilebilir kılınmamalı veya başka bir şekilde kullanılmamalıdır: a) ilgili kişinin rızası ile; veya b) kanunun yetkisiyle." (Md.10) (OECD, 2013).

Avrupa Komisyonu - Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data: "Kişisel veriler, belirli ve meşru amaçlarla işlenecek ve bu amaçlara aykırı şekilde kullanılmayacaktır. Kişisel veriler, veri sahibinin beklenmedik, uygunsuz veya başka bir şekilde sakıncalı olarak değerlendirebileceği şekilde daha fazla işlenmemelidir. Veri öznelerinin, başlangıçtaki amaçlarla öngörülenlerden farklı veya daha büyük risklere maruz bırakılması, verilerin beklenmedik bir şekilde daha fazla işlenmesi durumu olarak değerlendirilebilir." (Md.3.1) (Conseil of Europe, 2017).

International Working Group on Data Protection in Telecommunication - Working Paper on Big Data and Privacy: "Veri maksimizasyonu: Büyük Veri, veri maksimizasyonu ile ilgilidir. Özünde, Büyük Veri, veri minimizasyonu ve alaka düzeyine ilişkin gizlilik ilkeleri ilkelerinin tam karşıtıdır. Bu ilkeler, açıkça tanımlanmış amaçları yerine getirmek için gerekenden daha fazla kişisel bilginin toplanmamasını ve saklanmamasını sağlamayı amaçlamaktadır. İlk amaç için artık gerekli olmayan veriler silinmelidir. … Verilerin değeri, gelecekteki potansiyel kullanımlarıyla bağlantılıdır. Bu tür bir veri görünümü, verilerin işlenmesinin toplama sırasında tanımlanan ve belirtilen amaçlar için yeterli, ilgili ve aşırı olmamasını şart koşan gizlilik ilkesini ihlal edebilir. Ayrıca, bir veri denetleyicisinin verileri silme arzusunu ve motivasyonunu da etkileyebilir. Özel şirketler ve kamu kurumları, gelecekte bir noktada yeni anlayış ve gelir kaynağı olabilecek verileri silmek istemeyebilir. Büyük Veri'nin daha yaygın kullanımı, veri koruma yetkililerinin verileri silme yükümlülüğünü yerine getirmesini daha da zorlaştıracaktır." (Md.21) (International Working Group on Data Protection in Telecommunications, 2014b).

GDPR'ın minimum veri ilkesi ile ilgili 5. maddenin (c) fıkrası ekte verilmiştir (EK-1).

Tez kapsamında tanımlanan minimum veri ilkesi: Toplanacak kişisel veri işlendiği amaçla bağlantılı, sınırlı ve ölçülü olmalıdır. Kişisel verilerin işlenmesi gerekliliğinin ve bu kişisel verilerin uygunluğunun değerlendirilmesi, belirlenen amaç(lar) ışığında yapılmalıdır.

III. Uluslararası Kılavuzlarda Hassas Veri İlkesinin Yeri:

CPME - Statement on the Proposal for a Regulation on the General Data Protection Regulation: "Tıbbi kayıtlarda (kağıt versiyonu ve/veya e-kayıtlar) yer alan tüm veriler özellikle hassas veriler olarak kabul edilmeli ve bu temel ilkelerin korunmasını sağlamak için mümkün olan en yüksek düzeyde koruma sağlanmalıdır. …genetik veriler dahildir" (1. sayfa, 3. paragraf) (CPME, 2012).

International Working Group on Data Protection in Telecommunication - Working Paper on Big Data and Privacy: "Verilerin derlenmesi hassas bilgileri açığa çıkarabilir: Büyük Veri'nin analizi ile ilgili zorlu bir husus, kendi içinde hassas

olmayabilecek toplanan bilgi parçalarının derlenmesinin hassas bir sonuç üretebileceği gerçeğidir. Büyük Veri araçlarının kullanımıyla, örneğin sağlık, siyasi bakış açısı veya cinsel yönelim ile ilgili insanların eğilimleri tahmin edilebilir. Bu nedenle özel korumaya tabi bilgilerdir. Veri sorumluları, verileri derlerken ve analiz ederken bu riskin farkında olmalıdır." (Md.23) (International Working Group on Data Protection in Telecommunications, 2014b).

Nuffield Council on Bioethics - The collection, linking and use of data in biomedical researc and health care: ethical issues: "Tıbbi kayıtlar açıkça kişiseldir, ancak bir hastanın pratisyen hekimine gidip gitmediği gibi bireysel veriler, doğası gereği, insanlarla ilgili diğer kişisel bilgilerden daha az hassas değildir. Önemli olan bağlamdır – örneğin, doğurganlık tedavisi kayıtları bazı bağlamlarda bazı insanlar için oldukça hassas olabilir… Verilerin hassasiyeti, verilerin nasıl kategorize edildiğinden çok, kullanıldıkları bağlama ve diğer bilgilerle, kişilerle, kararlarla ve eylemlerle olan ilişkiye bağlıdır." (4. sayfa 2. ve 3. paragraf) (Nuffield Council on Bioethics, 2015).

GDPR'ın hassas veri ilkesi ile ilgili 9. maddesi ekte verilmiştir (EK-1).

Tez kapsamında tanımlanan hassas veri ilkesi: Sağlıkla ilgili toplanan tüm bilgiler hassas veri kabul edilmelidir. Ayrıca verilerin hassasiyet düzeyi, doğrudan nasıl kategorize edildiklerinden çok, bağlamı ile diğer veriler, kişiler, kararlar ve eylemlerle ilişkisine göre değerlendirilmelidir.

IV. Uluslararası Kılavuzlarda Eşitlik ve Adalet İlkesinin Yeri:

Avrupa Komisyonu - Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data: "Veri sorumluları gereksiz veya marjinal verilerin varlığını en aza indirmek, potansiyel gizli veri önyargılarından, ayrımcılık veya verilerin haklar ve temel özgürlükler üzerinde olumsuz etki riskinden kaçınmak için, veri işleme tasarımını dikkatli bir şekilde değerlendirmelidir (hem toplama hem de analiz aşamalarında)" (Md.4.2) (Conseil of Europe, 2017).

WMA - Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks: "İlgili toplulukların çıkarları ve hakları, özellikle de

savunmasız olduklarında, özellikle fayda paylaşımı açısından korunmalıdır.” (Md.17) (WMA, 2016).

Tez kapsamında tanımlanan eşitlik ve adalet ilkesi: Sağlık hakkı kapsamında sağlık veri tabanlarına herkes erişebilir olmalıdır. Kullanılmakta olan veri kayıt sistemleriyle ilgili sosyoekonomik, coğrafi ve etnik ayrımcılık yapılmamalıdır. Veri kayıt sistemleri damgalanmaya yol açmamalıdır. Bilgi ve iletişim teknolojilerine erişim, kültür, dil, gelir düzeyi ve yaş gibi değişkenler açısından sağlanmalıdır. Dezavantajlı grupların menfaatleri ve hakları korunmalıdır.

V. Uluslararası Kılavuzlarda Özerklik İlkesinin Yeri:

WMA - Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks: “Bireylerin haysiyetine, özerkliğine, mahremiyetine ve gizliliğine saygı duyan hekimlerin, hastaları tarafından sağlanan bilgileri koruyan görevliler olarak hem etik hem de yasal özel yükümlülükleri vardır. Özerklik, mahremiyet ve gizlilik hakları ayrıca bireylere kişisel verilerinin ve biyolojik materyallerinin kullanımı üzerinde kontrol etme hakkı verir. (Md.9)

Bireyler, verileri hakkında bilgi talep etme ve bu bilgilerin kendilerine verilmesi hakkına sahip olmasının yanı sıra hata veya eksikliklerin düzeltilmesini isteme hakkına sahiptir. Sağlık Veri Tabanları ve Biyo-bankalar, ilgili kişileri faaliyetleri hakkında bilgilendirmek için yeterli önlemleri almalıdır. (Md.14)

Açıkça tanımlanmış, ciddi ve acil bir tehdit olması durumunda, anonim verilerin yeterli olmayacağı durumlarda, nüfusun sağlığını korumak için onam gerekliliklerinden feragat edilebilir. Bağımsız bir etik kurul, her istisnai durumun haklı olduğunu doğrulamalıdır. (Md.16)

Onam verebilen bireylerden veri ve biyolojik materyalin toplanması, saklanması ve kullanılması gönüllülük esasına dayalı olmalıdır. Belirli bir araştırma projesi için veriler ve biyolojik materyaller toplanırsa, Helsinki Bildirgesi uyarınca katılımcıların özel, özgür ve bilgilendirilmiş oluru alınmalıdır. ... Onam ancak ilgili kişilerin aşağıdakiler hakkında yeterince bilgilendirilmesi durumunda geçerlidir: Sağlık Veri tabanının veya Biyo-bankanın amacı, Veri ve materyalin toplanması, saklanması ve

kullanılmasıyla ilgili riskler ve yükler, Toplanacak veri veya materyalin niteliği, Tesadüfi bulgular da dahil olmak üzere sonuçların iadesi için prosedürler, Sağlık veri tabanına veya Biyo-bankaya erişim kuralları, Mahremiyet/gizlilik'in nasıl korunacağı, Veri ve materyalin tanımlanamaz hale getirilmesi durumunda, kişinin veri/materyal ile ne yapıldığını bilemeyebileceğini ve onamı geri çekme seçeneğinin olmayacağını, Uygulanabilir olduğunda, ticari kullanım ve fayda paylaşımı, fikri mülkiyet konuları ve veri veya materyalin diğer kurumlara veya üçüncü ülkelere aktarılması. … Onam alınamayan, verileri ve biyolojik materyalleri gelecekteki araştırmalar için saklanan kişilerin, onam verme kapasitesine ulaştıklarında, onam alınması için makul çabalar gösterilmelidir." (Md.11 ve Md.12) (WMA, 2016).

International Working Group on Data Protection in Telecommunication - Working Paper on Big Data and Privacy: "Her birey kendi profiline ve veri denetleyicisinin kendisi hakkında sahip olduğu tüm bilgilere erişebilmelidir. Her birey, çeşitli kişisel verilerin kaynakları hakkında da bilgilendirilmelidir. Ayrıca, yürürlükteki yasalara tabi olarak, bilgilerini düzeltebilmeli ve profil oluşturma amacıyla kullanılan toplama tasarılarından vazgeçebilmeli veya kabul edebilmelidirler. (Md.47)

Sınıflandırma sistemlerinin birey için olumsuz sonuçları olabilir. Bu nedenle her birey, profil oluşturma veya karar verme için temel olarak hangi algoritmaların kullanıldığına ilişkin bilgilere erişebilmelidir. Bilgiler açık ve anlaşılır bir biçimde sunulmalıdır. Bu, haksız ayrımcılığı önlemek ve bireyler için önemli kararların yanlış gerçeklere dayalı olarak verilmesini önlemek için önemlidir. (Md.48)

Kişisel verilerin analiz ve profil oluşturma amaçlarıyla kullanılmasıyla bağlantılı olarak veri sahiplerinden geçerli onam alınmalıdır. (Md.36)

Onam almanın mümkün olmadığı durumlarda, verilerin dikkatle dengelenmiş sınırlar içinde işlenmesi mümkün olabilir. Örneğin, veri sorumlusunun meşru çıkarları için işlemenin gerekli olması halinde, bu menfaatlerin bireyin menfaatleri tarafından geçersiz kılınmadığı sürece, veri sorumlusu verileri işleyebilir. Veri sorumlusu, iki karşıt menfaati - meşru menfaatler ve bireyin menfaatleri - birbiriyle dengelemelidir. Menfaatlerin dengelenmesinin sonucu, bireyin mahremiyetle ilgili hangi

menfaatlerinin tehlikede olduğuna ve veri sorumlusunun meşru menfaatlerine bağlı olarak vakadan vakaya farklılık gösterecektir. Veri sahipleri üzerindeki etki ne kadar önemliyse, ilgili güvencelere o kadar fazla dikkat gösterilmelidir." (Md.37) (International Working Group on Data Protection in Telecommunications, 2014b).

CPME - Statement on the Proposal for a Regulation on the General Data Protection Regulation: "… Sınır ötesi bilgi aktarımı durumlarında, hastaların haklarına ilişkin tam bilgiye ve yasal kesinliğe sahip olmalarının ve verilerinin aktarımı ve işlenmesine ilişkin açık rıza göstermelerinin sağlanması son derece önemlidir. (2. sayfa, 2. paragraf)

… Hastanın kendi sağlık verileriyle ilgili rızasını vermekten 'vazgeçme' hakkı olmalıdır." (2. sayfa, 4. paragraf) (CPME, 2012).

CPME - Consent in the field of research General Data Protection Regulation - 2012/0011(COD) Compromise amendments on Articles 81 and 83: "Uygulamada, "Tek seferlik onam", bir hastadan gelecekteki olası herhangi bir araştırma çalışması için kişisel verilerinin kullanımına körü körüne onay vermesinin istenebileceği anlamına gelir. Bu istenmeyen sonuçlara yol açabilir." (1. sayfa, 3. paragraf) (CPME, 2013).

Avrupa Komisyonu - Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data: "Serbest, özel, bilgilendirilmiş ve açık rıza, veri işlemenin şeffaflığı ilkesine göre ilgili kişiye sağlanan bilgilere dayanacaktır. Büyük Veri kullanımının karmaşıklığı göz önüne alındığında, bu bilgiler, Bölüm 4.2'de açıklanan (potansiyel veri ön yargıları, ayrımcılık, haklar veya temel özgürlükler üzerinde olumsuz etki risklerinden kaçınmak) değerlendirme sürecinin sonucunu kapsamlı olarak içermelidir. Ayrıca, deneyimden öğren yaklaşımıyla veri kullanımının etkilerini ve veri öznesi üzerindeki potansiyel etkisini simüle eden bir ara-yüz aracılığıyla da sağlanabilir. (Md.5.1).

Veri öznesinin rızasına dayalı olarak veri toplandığında, veri öznelerinin ilk amaçlarla uyumlu olmayan verileri için veri işlemeye tepki göstermeleri ve onamlarını geri çekebilmeleri için kolay ve kullanıcı dostu teknik yollar sağlanmalıdır. (Md.5.2).

Veri sahibi ile veri sorumlusu arasında, veri sahibinin işlemeye ilişkin kararlarını etkileyen açık bir güç dengesizliği varsa, onam serbestçe verilmez. Veri sorumlusu, bu dengesizliğin mevcut olmadığını veya veri sahibi tarafından verilen onamı etkilemediğini göstermelidir." (Md.5.3) (Conseil of Europe, 2017).

Nuffield Council on Bioethics - The collection, linking and use of data in biomedical researc and health care: ethical issues: "Onamın geçerli olabilmesi için özgürce verilmiş olması ve zorlama veya aldatma yoluyla elde edilmemesi gerekir. Onam veren kişi, bunu yapmanın sonuçlarının farkında olmalıdır. Bu, bilgilerin nasıl kullanılacağına dair her ayrıntının farkında olmaları gerektiği anlamına gelmez, ancak kendileriyle ilgili olduğunu düşündükleri ayrıntıların farkında olmaları gerekir." (4. ve 5. sayfa "Confidentiality and consent" başlığı) (Nuffield Council on Bioethics, 2015).

GDPR'ın özerklikle ilgili 7, 8, 13, 14, 15, 16, 17, 18, 19, 20, 21 ve 22. maddeleri ekte verilmiştir (EK-1).

Tez kapsamında tanımlanan özerklik ilkesi: Her bireyin profiline ve veri denetleyicisinin kendileri hakkında sahip olduğu tüm bilgilere erişimi olmalı; profil oluşturma veya karar verme için temel olarak hangi algoritmaların kullanıldığı bilgisine erişimi olmalı; bireyler, verilerin kullanımı hakkında bilgi talep edebilmeli, bunlarla ilgili hata veya eksikliklerin düzeltilmesini isteyebilmeli, uygulamayı devre dışı bırakabilmeli ve tanımlanabilir verileri silebilmelidir.

Özerklik ilkesinin korunabilmesi için aydınlatılmış onam alınmalıdır (geçerli bir onam için belirtilen koşullar sağlanmalı). Bu onam, kişinin aşağıdaki noktalarda aydınlatılmasına dayanmalıdır:

- Bilgilendirme belirli bir konuya ilişkin, açık ve anlaşılır olmalı.
- Bilgilendirme kapsamında; veri tabanının amacı, verinin toplanması, depolanması ve kullanımındaki riskler ve yükler, toplanacak verinin niteliği, sağlık veri tabanına erişim kuralları, gizliliğin nasıl sağlandığı/korunduğu, bilgilere kimlerin erişim sağlayabileceği, ticari kullanımı ve üçüncü taraflara paylaşım bilgilerine yer verilmeli.
- Onam özgür iradeyle verilmeli.

- Verilen onamı geri çekilebilmek için kolay ve kullanıcı dostu teknik yollar sağlanmalı.
- Veriler, birden fazla ve belirsiz kullanım için bir sağlık veri tabanında toplanır ve saklanacaksa, onam yalnızca ilgili bireyler yeterince bilgilendirilmişse geçerli olmalı.
- Bireyler istedikleri zaman onamlarını değiştirebilmeli, tanımlanabilir verinin sağlık veri tabanından silinmesini isteyebilmeli.
- Veri ilgilisi ve veri sorumlusu arasında güç dengesizliği varsa, veri ilgilisinin kişinin onamını etkilemediği gösterilmeli.

VI. Uluslararası Kılavuzlarda Mahremiyet ve Gizlilik İlkesinin Yeri:

Avrupa Komisyonu - Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data: "Hassas verilerin kullanımıyla ilgili olarak, hassas bilgilerin çıkarılması için hassas olmayan verilerin kullanılmasından mümkün olduğunca kaçınmak ve kullanılıyorsa, hassas veriler için benimsenen aynı koruma önlemlerini bu verilere genişletmek için tasarım kaynaklı çözümler benimsenecektir. (Md.4.4).

İlgili veri koruma ilkelerinin uygulanmasından muaf olmayan kimliksizleştirme önlemleri, veri sahiplerine yönelik riskleri azaltabilir. (Md.4.5).

Veri sorumlusu, verilerin doğası, kullanım bağlamı, mevcut yeniden tanımlama teknolojileri ve ilgili maliyetler ışığında ihtiyaç duyulan zaman, çaba veya kaynakları dikkate alarak yeniden tanımlama riskini değerlendirmelidir. Veri sorumlusu verileri anonimleştirmek ve kimlik gizlemenin etkinliğini sağlamak için alınan önlemlerin yeterliliğini göstermelidir. (Md.6.2)

Teknik önlemler, ilgili kişilerin olası yeniden tanımlanmasını önlemek için yasal veya sözleşmeden doğan yükümlülüklerle birleştirilebilir. Veri sorumlusu, anonimleştirme tekniklerine ilişkin teknolojik gelişme ışığında, yeniden tanımlama riskinin değerlendirmesini düzenli olarak gözden geçirecektir." (Md.6.3) (Conseil of Europe, 2017).

International Working Group on Data Protection in Telecommunication - Working Paper on Big Data and Privacy: Güvenlik etkileri. Büyük Veri aynı zamanda gizliliğin korunması açısından da sonuç doğurabilecek bilgi güvenliği açısından zorluklar içerir. Bu tür güvenlik sorunlarına örnek olarak şunlar verilebilir: Büyük Veriyi işlemek için çeşitli altyapı katmanları, muazzam veri akışını işlemek için yeni altyapı türleri ve Büyük Veri kümelerinin ölçeklenemeyen şifrelemesi. Ayrıca, çok Büyük Veri kümeleri depolandığında bir veri ihlali daha ciddi sonuçlar doğurabilir. Büyük kişisel veri setleri edinen ve muhafaza eden şirketler, bu bilgilerin sorumluları olmalıdır. (Md.25).

…Anonimleştirilmiş verilerin kabul edilebilir risk düzeyi açısından test edilmesi önemlidir. Bu, örneğin Gizlilik Etki Değerlendirmesinin bir parçası olarak belgelenmelidir. (Md.40).

Şeffaflık önemli bir gizlilik ilkesidir. Şeffaflık, veri sahipleri ve veri denetleyicileri arasında güven oluşturur. Veri denetleyicilerinin hesap verebilir olduklarını ve Büyük Veri kullanımları konusunda sorumlu ve etik kararlar alabileceklerini göstermeleri gerekir. Örneğin, veri denetleyicileri, anonimleştirilmiş bir veri kümesinin bireyler üzerinde hala bir etkisi olabileceğinin farkında olmalıdır. Anonimleştirilmiş veri kümeleri, bireylerin mevcut profillerini zenginleştirmek için kullanılabilir, böylece yeni veri koruma sorunları ortaya çıkar. Hem profiller hem de altta yatan algoritmalar sürekli değerlendirme gerektirir. Bu, profil oluşturmadan kaynaklanan kararların sorumlu, adil, etik ve profillerin kullanım amacı ile uyumlu olmasını sağlamak için düzenli kontrolleri gerektirir. Tam otomatik yanlış pozitif veya yanlış negatif sonuçlar nedeniyle bireylere yönelik adaletsizlikten kaçınılmalıdır.” (Md.53) (International Working Group on Data Protection in Telecommunications, 2014b).

WMA - Declaration of Taipei on Ethical Considerations Regarding Health Databases and Biobanks: “Sağlık Veri tabanlarında ve Biyo-bankalarda güveni ve bütünlüğü korumak için gizlilik esastır. Mahremiyetlerine saygı duyulacağını bilmek, hastalara ve bağışçılara hassas kişisel verileri paylaşma güveni verir. Onların mahremiyeti, veri ve biyolojik materyalin işlenmesine dahil olan herkesin gizliliğini korumak yükümlülüğü vardır.” (Md.10) (WMA, 2016).

Nuffield Council on Bioethics - The collection, linking and use of data in biomedical researc and health care: ethical issues: "Gizlilik, bireyler ve gruplar için kimliklerini ve başkalarıyla ilişkilerini kurarken ve sürdürürken temel olarak önemlidir. Aile, grup, topluluk ve hatta ulusal kimlikler, bilgilerin paylaşılma şekliyle oluşturulabilir ve doğrulanabilir. Bireyler genellikle kişisel bilgilere erişimi kontrol etmeyi, mahremiyetlerini korumanın önemli bir yönü olarak görürler. Bilgilere istekleri dışında erişilir veya açıklanırsa, bireylerin refahını etkileyebilir ve haklarını ihlal edebilir. İnsanların mahremiyetine saygı duymak, onlara birey olarak saygı duyulduğunu göstermektir." (4. sayfa *"The value of privacy"* başlığı) (Nuffield Council on Bioethics, 2015).

GDPR'ın mahremiyet ve gizlilikle ilgili 32, 33, 34 ve 44. maddeleri ekte verilmiştir (EK-1).

Tez kapsamında tanımlanan mahremiyet ve gizlilik ilkesi: Minimum veri ilkesi gözetilmeli, anonimleştirme ilkesine özen gösterilmeli ve gizliliğe dayalı şeffaflık ilkesi korunmalıdır. Bilgiye yalnızca yetkili kişiler onam alarak erişim sağlamalı ve bilgilerin üçüncü taraflarla paylaşılmayacağı güvence altına alınmalıdır.

Mahremiyet ve gizlilik birbirinden farklı iki kavramdır. Tez kapsamında mahremiyet, sadece bilgi ile sınırlı olmayan, bireylerin özel alanında tanımladığı ve başkasının görmesini istemediği her şeydir. Buna sadece kişinin kendisi karar verebilir. Gizlilik ise kişi hakkında işlenen bilgilerin gizli tutulmasıdır. Buna göre gizlilik, bilgi ve belgelerin güvenli bir şekilde saklanması ve başkalarının yetkisiz erişiminden korunması eylemlerini ifade etmektedir. Buna göre gizlilikle ilgili olarak; bir kişi hakkında yasal olarak toplanan veriler, kayıp, bozulma, yetkisiz imha, kullanım, değiştirme veya ifşaya karşı tüm makul ve uygun önlemlerle korunmalıdır. Veri tabanlarında şifreleme olmalı, veri sızıntılarına yönelik siber güvenlik önlemleri alınmalıdır. Veri güvenliğini artırmak için tanımlanan dört aşama uygulanmalıdır: 1) Bireylerin korunması: Hassas olmayan verileri de mümkün olduğunca hassas veriler için kabul edilen önlemlere genişletilmeli. Büyük Veri kullanımının risklerine ve bunun bireyler ve toplum üzerindeki etkilerine ilişkin önleyici politikalar benimsenmelidir. 2) Şeffaflık: Veri tabanları ile ilgili her türlü bilgi kamuya açık olmalıdır. 3) Katılım ve kapsayıcılık: Veri tabanlarının kullanılması için bireylere ve

topluluklara danışılmalı ve onlarla iletişim kurmalıdır. 4) Hesap verebilirlik: Veri tabanları tüm tarafların erişimine açık ve duyarlı olmalı, veri denetleyicileri, anonimleştirilmiş bir veri kümesinin bireyler üzerinde hala bir etkisi olabileceğinin farkında olmalı ve veri sorumlusu tanımlanmalıdır.

Mobil Uygulamaların Analizi: Pandemi döneminde kullanılmaya başlanan temas takip uygulamaları, genel sağlık verisi yerine bulaşıcı hastalık gibi toplum sağlığını etkileyen durumlara karşı işlenen kişisel veriler açısından incelenmiştir. İnceleme yapılabilmesi için "Guidance on Apps supporting the fight against COVID-19 pandemic in relation to data protection" (Veri Koruma ile İlişkili COVID-19 Salgınına Karşı Mücadeleyi Destekleyen Uygulamalar/Aplikasyonlar Üzerine Kılavuz) kılavuzu temel alınmıştır (European Commission, 2019). Buna göre kılavuzda bulunan temel ilkeler aşağıdaki şekilde özetlenmiştir:

- Uygulamanın cihaza yüklenmesi gönüllü olmalı ve uygulamayı indirmemeye /kullanmamaya karar veren kişi için herhangi bir olumsuz sonuç doğurmamalıdır (Md.3.2)
- Farklı uygulama işlevleri (örn. bilgi, semptom kontrol, temas izleme ve uyarı işlevleri), bireyin her bir işlev için özel olarak kendi onayını verebilmesi için bir araya getirilmemelidir. Bu, sağlayıcı tarafından bir seçenek olarak sunuluyorsa, kullanıcının farklı uygulama işlevlerini birleştirmesini engellememelidir (Md.3.2).
- Yakınlık verileri kullanılıyorsa (Bluetooth servisi) bunlar kişinin cihazında saklanmalıdır. Bu veriler sağlık yetkilileriyle paylaşılacaksa, ancak ilgili kişinin COVID-19 ile enfekte olduğu teyit edildikten sonra ve bunu yapmayı seçmesi şartıyla paylaşılmalıdır. Sağlık yetkilileri, enfeksiyon riski taşıyan kişilerle iletişim kurabilmeleri için yalnızca virüs bulaşmış bir kişinin cihazından gelen yakınlık verilerine erişebilmelidir (Md.3.2).
- Sağlık yetkilileri, bireylere kişisel verilerinin işlenmesiyle ilgili tüm gerekli bilgileri sağlamalıdır (Md.3.2).
- Birey GDPR kapsamındaki haklarını (özellikle erişim, düzeltme, silme) kullanabilmelidir (Md.3.2).

- Uygulamalar en geç pandeminin kontrol altına alındığı ilan edildiğinde devre dışı bırakılmalıdır; devre dışı bırakma, kullanıcı tarafından kurulumun kaldırılmasına bağlı olmamalıdır (Md.3.2).
- Uygulamaların yüklenmesi ve kullanıcının cihazında bilgilerin saklanması: kullanıcının cihazında bilgilerin depolanmasına veya halihazırda saklanan bilgilere erişim sağlanmasına yalnızca (i) kullanıcının onay vermesi veya (ii) depolama ve/veya erişim izni vermesi durumunda izin verilir (Md.3.3).
- Onam, "özgürce verilmiş", "spesifik", "açık" ve "aydınlatılmış" olmalıdır. Bireyin net bir olumlu eylemiyle ifade edilmelidir. Enfekte kişi, potansiyel olarak temasta bulunduğu ve uyarılacak kişilerin kimliği hakkında bilgilendirilmemelidir. Enfekte kişinin kimliği, temasta bulunduğu kişilere açıklanmamalıdır. Son 16 gün içinde enfekte bir kişiyle temas halinde olduklarını kendilerine iletmeleri yeterlidir. Bu tür temasların zamanı ve yeri ile ilgili veriler saklanmamalıdır. Enfekte olduğu tespit edilen bir uygulama kullanıcısının temaslarını izlemek için, ulusal sağlık yetkilileri yalnızca, semptomların başlamasından 48 saat öncesinden 14 güne kadar enfekte kişinin temas halinde olduğu kişinin kimliği hakkında bilgilendirilmelidir (Md.3.3; Md.3.5).
- Veri işlemenin yasal dayanağı: Herhangi bir ulusal yasa, veri öznelerinin hak ve özgürlüklerini korumak için özel ve uygun önlemler sağlamalıdır. Genel bir kural olarak, bireylerin özgürlükleri üzerindeki etki ne kadar güçlüyse, ilgili kanunda buna karşılık gelen güvenceler de o kadar güçlü olmalıdır. Veri işlemede Covid-19, toplum sağlığının korunması için yasal bir dayanak oluşturur. (Md.3.3).
- Uygulama kaldırıldığında kullanıcılar için hiçbir olumsuz sonuç ortaya çıkmamalıdır (Md.3.3).
- Veri minimizasyonu: Kişisel verinin işlenmesi sınırlı, amaçla bağlantılı ve ölçülü olmalıdır. Yalnızca gerekli olan bilgi işlenmeli, bir gerekçe olmadıkça sağlık yetkilileri hiçbir bilgiye erişememelidir. Semptom denetleyici ve tele-tıp işlevleri için ilgili mevzuatta işlenen kişisel veriler listelenmelidir (Md.3.4).
- Enfeksiyon zincirinin kırılması için Bluetooth gibi yakınlık verileri, yalnızca gerçek bir enfeksiyon riski varsa oluşturulmalı ve kullanılmalıdır (Md.3.4).
- Temas izlemek için konum verileri kullanılmamalıdır (Md.3.4).

- Bir uygulamanın her işlevi için bir amaç olmalıdır. İşlenen veriler Covid-19 ile mücadele kapsamı dışında kullanılmamalıdır (Md.3.5).
- Kişisel veriler gereğinden uzun süre saklanmamalıdır. Semptom belirlemeye yönelik uygulamalarda toplanan veriler, sağlık yetkilileri tarafından en fazla bir ay veya kişi test edildikten ve sonuç negatif çıktıktan sonra silinmelidir. Sağlık yetkilileri, anonimleştirilmiş bir biçimde olması koşuluyla, verileri sürveyans raporlaması ve araştırma için daha uzun süre saklayabilir. Kişisel cihazdan ulusal sağlık yetkililerine yapılan tüm aktarımlar şifrelenmelidir (Md.3.5).
- Veriler, kullanıcının cihazında saklanmalı ve yalnızca kullanıcılar tarafından iletilen ve amacı yerine getirmek için gerekli olan veriler, bu seçeneğin seçildiği durumlarda sağlık yetkililerinin erişimine açık olan sunucuya yüklenmelidir. Verilerin merkezi bir sunucuda saklanması durumunda, yönetici erişimi de dahil olmak üzere erişim kayıt altına alınmalıdır (Md.3.8).
- Yakınlık verileri yalnızca bireyin cihazında şifreli ve takma adlarla oluşturulmuş biçimde oluşturulmalı ve saklanmalıdır. Üçüncü tarafların takibinin hariç tutulduğundan emin olmak için, diğer konum servislerini etkinleştirmek zorunda kalmadan Bluetooth'un etkinleştirilmesi mümkün olmalıdır (Md.3.8).
- İşlenen kişisel verilerin doğruluğu sağlanmalıdır. Temasın daha kesin bir şekilde değerlendirilmesine izin veren teknolojiler kullanılmalıdır (Bluetooth gibi) (Md.3.9).
- Veri Koruma Yetkilileri, uygulamanın geliştirilmesi sürecinde tam olarak yer almalı ve uygulamayı inceleme altında tutmalıdır (Md.3.10).

Oluşturulan bu ilkelerden hareketle iki aşamalı bir analiz gerçekleştirilmiştir.

3.1.2. Birinci aşama: Ulusal düzenlemelerin belirlenmesi

Birinci aşamada Türkiye'deki kişisel sağlık verileri ile ilgili incelenebilecek yasal düzenlemeler belirlenmiş ve bu düzenlemeler etik ilkelere göre karşılaştırılmıştır. Yasal düzenlemelerin taranması için KVK Kurumu'nun temel metinlerinde belirtilen düzenlemeler ve Resmi Gazete'de "kişisel veri", "kişisel sağlık verisi", "veri", "sağlık" kavramları girilerek arama yapılmış, aşağıdaki kriterleri karşılayanlar çalışma kapsamına alınmıştır.

Yasal düzenlemelerin seçilme kriterleri;

- Kişisel sağlık bilgileri ile doğrudan ilgili olması veya ilgili maddelerinin bulunması
- Sağlık çalışanlarının herhangi bir etik ikilemle karşılaştıklarında başvuracakları düzenlemeler olabilmesi
- Sağlık hizmetlerinde kullanılan veri tabanları için kayıtların tutulmasındaki usul ve esasları belirlemesi
- Kişisel verilerin güvenliği açısından dayanak oluşturması
- Kişisel verilerin korunması ile ilgili yasal bağlayıcılığı olabilecek metin olması
- Yukarıdaki gerekçelerden en az ikisini karşılaması

Analiz edilen düzenleme metinleri ve genel özellikleri:

Tablo 3. Analiz edilen düzenlemeler ve özellikleri

Düzenlemeler/Özellikleri	**Resmi Gazete Tarihi**	**Türü**	**Hedef grubu (Kapsamı)**	**Kişisel verilerle ilgi düzeyi***
Tıbbi Deontoloji Nizamnamesi	1960	Tüzük	Madde (Md.) 1. Tabip odalarına kayıtlı bulunan hekim ve diş hekimleri	Maddeleri ilgili
Organ ve Doku Alınması, Saklanması, Aşılanması ve Nakli Hakkında Kanun	1979	Kanun		Maddeleri ilgili
T.C. Anayasası	1982			Maddeleri ilgili
Nüfus Planlaması Hakkında Kanun	1983	Kanun		Maddeleri ilgili
Yataklı Tedavi Kurumları İşletme Yönetmeliği	1983	Yönetmelik	Md.2. Ağız ve diş sağlığı merkezleri ve sağlık kurumları	Maddeleri ilgili
Sağlık Hizmetleri Temel Kanunu	1987	Kanun	Md.2. Milli Savunma Bakanlığı hariç, bütün kamu kurum ve kuruluşları ile özel hukuk tüzel kişilerini ve gerçek kişileri	Maddeleri ilgili

Tablo 3. Analiz edilen düzenlemeler ve özellikleri (devamı)

Düzenlemeler/Özellikleri	Resmi Gazete Tarihi	Türü	Hedef grubu (Kapsamı)	Kişisel verilerle ilgi düzeyi*
Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Hakları ve İnsan Haysiyetinin Korunması Sözleşmesi: İnsan Hakları ve Biyotıp Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun	1997 (Türkiye'de kabul tarihi: 2003)	Ulusal üstü düzenleme	Md.1. Sözleşmeyi imzalayan ülkelerin vatandaşları	Maddeleri ilgili
Hasta Hakları Yönetmeliği	1998	Yönetmelik	Md.2. sağlık hizmeti verilen resmi ve özel bütün kurum ve kuruluşları, bu kurum ve kuruluşlarda veya bunların dışında hizmete katılan her kademedeki ve unvandaki ilgilileri	Maddeleri ilgili
TTB Hekimlik Meslek Etiği Kuralları	1999	TTB düzenlemesi	Md.3. Tüm hekimler	Maddeleri ilgili
Türk Medeni Kanunu	2001	Kanun		Maddeleri ilgili
Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arşiv Hizmetleri Yönergesi	2001	Yönerge	Sağlık Bakanlığı'na bağlı yataklı tedavi kurumlarını ve bu kurumlardaki tıbbî kayıt ve arşiv hizmetleri	Doğrudan ilgili
Özel Hastaneler Yönetmeliği	2002	Yönetmelik	Gerçek kişiler ve özel hukuk tüzel kişilerine ait hastaneler	Maddeleri ilgili
Bilgi Edinme Hakkı Kanunu	2003	Kanun		Doğrudan ilgili
İş Kanunu	2003	Kanun		Maddeleri ilgili
Türk Tabipleri Birliği Disiplin Yönetmeliği	2004	Yönetmelik		Maddeleri ilgili
Aile Hekimliği Kanunu	2004	Kanun	Aile Hekimliğinde görevli sağlık personeli	Maddeleri ilgili
Elektronik İmza Kanunu	2004	Kanun		Maddeleri ilgili
Türk Ceza Kanunu	2004	Kanun		Maddeleri ilgili
Ceza Muhakemesi Kanunu	2004	Kanun		Maddeleri ilgili

Tablo 3. Analiz edilen düzenlemeler ve özellikleri (devamı)

Düzenlemeler/Özellikleri	Resmi Gazete Tarihi	Türü	Hedef grubu (Kapsamı)	Kişisel verilerle ilgi düzeyi*
Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu	2006	Kanun	Sosyal sigortalar ile genel sağlık sigortasından yararlanacak kişileri, işverenleri, sağlık hizmeti sunucularını, tüzel ve gerçek kişileri	Maddeleri ilgili
Kan ve Kan Ürünleri Kanunu	2007	Kanun	Bakanlıkça izin verilmiş gerçek kişiler ile özel hukuk tüzel kişileri	Maddeleri ilgili
İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun	2007	Kanun		Maddeleri ilgili
Ayakta Teşhis ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmelik	2008	Yönetmelik	Ayakta teşhis ve tedavi hizmeti sunulan özel sağlık kuruluşları ve bu kuruluşların işletenleri	Maddeleri ilgili
Elektronik Haberleşme Kanunu	2008	Kanun		Maddeleri ilgili
Türk Borçlar Kanunu	2011	Kanun		Maddeleri ilgili
Sağlık Alanında Bazı Düzenlemeler Hakkında KHK	2011	Kanun Hükmünde Kararname	Sağlık Bakanlığı ve bağlı kuruluşları	Maddeleri ilgili
Genel Sağlık Sigortası Verilerinin Güvenliği ve Paylaşımına İlişkin Yönetmelik	2012	Yönetmelik	Md.1. Sosyal Güvenlik Kurumu ve sözleşmeli sağlık hizmet sunucuları, kamu kurum ve kuruluşları, gerçek ve tüzel kişiler	Doğrudan ilgili
Sağlık Hizmetleri Lisans Yönetmeliği	2012	Yönetmelik	Md.2. Sağlık hizmet sunucusu tüm gerçek ve tüzel kişileri	Maddeleri ilgili
Aile Hekimliği Uygulama Yönetmeliği	2013	Yönetmelik	Md.1. Aile hekimi ve aile sağlığı elemanları	Maddeleri ilgili
Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği	2015	Yönetmelik		Maddeleri ilgili

Tablo 3. Analiz edilen düzenlemeler ve özellikleri (devamı)

Düzenlemeler/Özellikleri	Resmi Gazete Tarihi	Türü	Hedef grubu (Kapsamı)	Kişisel verilerle ilgi düzeyi*
Kişisel Verilerin Korunması Kanunu	2016	Kanun	Md.2. Kişisel verileri işlenecek gerçek kişiler, bir veri kayıt sisteminin parçası olan, otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler	Doğrudan ilgili
Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik	2017	Yönetmelik	Md.2. Veri sorumluları	Doğrudan ilgili
Kişisel Verileri Koruma Kurulu Çalışma Usul ve Esaslarına Dair Yönetmelik	2017	Yönetmelik	Md.1. Kurulda çalışanlar	Doğrudan ilgili
Veri Sorumluları Sicili Hakkında Yönetmelik	2017	KVK Kurumu'ndan Yönetmelik	Md.2. Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek ve tüzel kişileri	Doğrudan ilgili
Kişisel Verileri Koruma Kurumu Teşkilat Yönetmeliği	2018	Yönetmelik	Md.1. Kurulda çalışanlar	Doğrudan ilgili
Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ	2018	KVK Kurumu	Md.1. veri sorumluları veya yetkilendirdiği kişiler	Doğrudan ilgili
Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ	2018	KVK Kurumu		Doğrudan ilgili
Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler	2018	KVK Kurumu	Veri sorumluları	Doğrudan ilgili
Kişisel Sağlık Verileri Hakkında Yönetmelik	2019	Yönetmelik	Md.1. Sağlık hizmeti sunucuları ile bağlı ve ilgili kuruluşları	Doğrudan ilgili
Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğin Korunması Yönetmeliği	2020	Yönetmelik	Md.1 Haberleşme sektöründeki işletmecileri	Doğrudan ilgili

Tablo 3. Analiz edilen düzenlemeler ve özellikleri (devamı)

Düzenlemeler/Özellikleri	Resmi Gazete Tarihi	Türü	Hedef grubu (Kapsamı)	Kişisel verilerle ilgi düzeyi*
Sır Niteliğindeki Bilgilerin Paylaşılması Hakkında Yönetmelik	2021	Yönetmelik		Doğrudan ilgili
Uzaktan Sağlık Hizmetlerinin Sunumu Hakkında Yönetmelik	2022	Yönetmelik	Md.2 Uzaktan sağlık hizmeti sunan tüm sağlık tesisleri ve sağlık meslek mensupları ve hizmeti almak isteyen gerçek kişiler	Doğrudan ilgili
Sağlık Bilgi Yönetim Sistemleri Hakkında Yönetmelik[1]	2022	Yönetmelik	Md.2 Sağlık bilgi yönetim sistemi hizmeti sağlayıcıları ile bu hizmetten yararlanan sağlık bilgi yönetim sistemi hizmet alıcıları	Doğrudan ilgili

*Kişisel veri ve kişisel sağlık verileri ile ilgili düzenlemeler doğrudan ilgili düzenlemeler, sağlıkla ve kişilik hakları ile ilgili düzenlemeler ise maddeleri ilgili düzenlemeler biçiminde ayrılmıştır.

"Kişisel Verileri Koruma Kurumu Personeli Görevde Yükselme ve Unvan Değişikliği Yönetmeliği", "Kişisel Verileri Koruma Kurumu Disiplin Amirleri Yönetmeliği" ve "Kişisel Verileri Koruma Uzmanlığı Yönetmeliği" kişisel verilerle doğrudan ilgili olsa da hedef grup ve amaçları açısından analiz dışında bırakılmıştır. Ayrıca Kişisel Veri Güvenliği Rehberi (2018) yasal bağlayıcılığı olmadığı halde KVK Kurumu çıkarmış olduğu için incelenmiştir.

Analizde karşılaştırma yaparken düzenlemeler ve veri kayıt sistemlerinde ileri sürülen amacın ilkelere uygunluğu değerlendirilmiş, tartışmada düzenlemeler ve veri kayıt sistemlerinin ilkelerle uyumlu olup olmadığı, uygulanma biçimi yönünden yaratabileceği riskler ele alınmıştır.

3.1.3. İkinci aşama: Veri tabanları ve mobil sağlık uygulamalarının seçimi ve analizi

Sağlık hizmetlerinin bütün basamaklarını temsil eden veri tabanları seçilmiştir. Buna göre birinci basamak sağlık hizmetleri için Türkiye genelinde kullanılan veri

[1]Tez yazım sürecinde (25 Ağu. 22) yürürlüğe koyulan bu yönetmelik, Bulgular'da analize dahil edilmemiş, ancak Tartışma'da ulusal düzenlemelerde saptanan sorunlara karşı ve belirtilen boşlukları tamamlaması açılarından değerlendirilmiştir.

tabanı Aile Hekimliği Bilgi Sistemidir. Aile Hekimliği Bilgi Sistemi örneği olarak Bursa Ertuğrul 36 nolu Eğitim Aile Sağlığı Merkezi'nde kullanılan Hızır AHBS uygulaması incelenmiştir. İkinci ve üçüncü basamak sağlık hizmetlerinde Hastane Bilgi Yönetim Sistemi (HBYS) kullanılmaktadır. HBYS için yataklı tedavi kurumlarını temsilen Bursa Uludağ Üniversitesi Sağlık Uygulama ve Araştırma Merkezi (SUAM) kayıt sistemi olan MİA MED veri tabanı incelenmiştir. Kişisel sağlık kaydı olarak kullanılan e-Nabız, veri kayıt sistemi olduğu için incelemeye alınmıştır. Covid-19 pandemisi ile mücadele kapsamında uygulamaya koyulan Hayat Eve Sığar (HES) ve Korona Önlem mobil uygulamaları, olağandışı durumlarda işlenen kişisel veriler açısından incelenmek üzere seçilmiştir. Bu veri kayıt sistemlerinin etik açısından analizi için ilk aşamada hangi sağlık bilgilerinin toplandığı ve uygulamaların özellikleri veya işlevleri incelenmiştir. Bu inceleme Hızır AHBS için Bursa Ertuğrul 36 nolu Eğitim Aile Sağlığı Merkezi'nde ve MİA MED için Bursa Uludağ Üniversitesi Tıp Fakültesi Aile Hekimliği polikliniğinden yazar adına kayıt açılarak gerçekleştirilmiştir. Diğer uygulamalar olan e-Nabız, HES ve Korona Önlem uygulamalarını araştırmacı kendi kişisel bilgilerini kullanılarak oluşturduğu hasta profilinden incelemiştir.

Analiz: Veri tabanlarını (E-Nabız, Hızır AHBS ve MİA MED) ilkelere göre karşılaştırırken hassas veri ilkesi dışarıda tutulmuştur. Çünkü bu ilke yasal düzenleme metinlerinde sağlık verisine yaklaşımı ifade etmektedir. Bununla birlikte tez kapsamında sağlıkla ilgili tüm veriler hassas kabul edildiği için ayrıca veri tabanlarına işlenen verilerin hassas olup olmadığı şeklinde bir değerlendirme yapılmamıştır.

Analizde karşılaştırma yaparken ilgili düzenlemeler ve veri tabanlarında ileri sürülen amacın ilkelere uygunluğu değerlendirilmiş, tartışma bölümünde gerek düzenleme ve veri tabanlarının amaç yönünden ilkelere uygun olup olmadığı, gerekse de amaca uygun olsa dahi, uygulanma biçimi yönünden yaratabileceği riskler ele alınmıştır.

3.1.4. Tanım ve ölçütler

Veri tabanı: Çalışma kapsamında "veri tabanı" sözcüğü bilgilerin toplandığı, depolandığı, yönetildiği ve kullanıldığı veri kaynaklarını ifade eden anlamıyla kullanılmıştır. Bu tanımdan hareketle kişisel sağlık verilerini çeşitli amaçlarla toplayan

mobil sağlık uygulamaları da veri tabanı olarak kabul edilmiştir.

Sağlık verileri konusunda tıbbi kayıt, elektronik sağlık kayıtları, elektronik hasta kaydı vs. gibi çeşitli kavramlar kullanılmaktadır. Bu çalışma kapsamında sağlık durumu ile yakın bir bağlantıya sahip olan tüm veriler, sağlık verisi olarak kabul edilmiştir.

İnceleme sırasında Sağlık Bakanlığı'nın veri tabanlarında kullanılan değişkenlerin neyi temsil ettiğini gösterdiği ve hangi bilginin neden toplandığını gerekçelendirdiği için "Ulusal Sağlık Veri Sözlüğü (USVS) 2.2" sürümü referans olarak alınmıştır (Sağlık Bakanlığı, 2014b). Sözlük, birinci basamak kapsamında Sağlık Bakanlığı'nın hangi sağlık verisini hangi gerekçe ile topladığı bilgisine yer vermektedir. Bu nedenle veri tabanlarının minimum veri ilkesi ile uyumlu olup olmadıklarının tartışılmasında bu Sözlük'ten yararlanılmıştır.

3.2. Çalışmanın Sınırlılıkları

Konunun genişliği ve disiplinler arası bir nitelik taşıması çalışmanın sınırlarını belirlemeyi gerektirmektedir. Kişisel sağlık verilerini toplayan/kaydeden veri tabanlarının güvenliği, bilişim teknolojileri uzmanlık alanı ile birlikte değerlendirilmesi gereken bir konudur. Bu değerlendirmenin yapılabilmesi için konunun teknik boyutu, gerektirdiği ölçüde ele alınmış ve çoğunlukla konunun sınırları dışında tutulmuştur.

Teknolojinin hızla gelişen yapısı nedeniyle veri tabanlarının güncellenebilir, benzer özelliklere sahip başka bir uygulama ile değiştirilebilir olma gibi özellikleri bulunmaktadır. Bu özellikler, yeni etik sorun alanları oluşturabilir. Bu nedenle yapılan analiz, söz konusu teknolojinin hızlı gelişen doğası nedeniyle sürekli geçerli kalmayabilecektir. Modern tıbbın dinamik yapısının yanı sıra kişisel verilerin korunmasıyla ilgili mevzuatın da sürekli olarak gelişebilmesi söz konusudur. Bu nedenle kişisel verilerin korunmasıyla ilgili olabilecek düzenlemeler de eksik kalabilmektedir.

Bulgular her ne kadar standart referanslar temel alınarak elde edildiyse de, araştırmacının bakışı ile oluşturulduğundan bir dereceye de kadar olsa öznellik içermektedir.

Tezin yazılması sırasında 2022 yılına ait iki yeni yönetmelik yürürlüğe koyulmuştur (Tablo 3). Kişisel verilerin korunması ile ilgili ulusal mevzuattaki boşluk nedeniyle, yeni düzenlemeler yayımlanabilmekte, var olan düzenlemelere yeni maddeler eklenebilmektedir. Dolayısıyla ulusal mevzuatın bu konudaki dinamik yapısı, çalışmanın önemli sınırlılıklarından birini oluşturmaktadır.

3.3.İzin ve Onaylar

Araştırmanın etik açısından uygunluğu Uludağ Üniversitesi Tıp Fakültesi Klinik Araştırmalar Etik Kurulu 2011-KAEK-26, 11 Ağustos 2021 tarih ve 2021-11/1 nolu kararıyla onaylanmıştır (EK-4).

Yataklı tedavi kurumu örneği olarak seçilen MİA MED uygulamasının incelenmesi için Bursa Uludağ Üniversitesi Sağlık Uygulama ve Araştırma Merkezi Müdürlüğü'nden 21/06/2021 tarih ve E-73115338-000-17561 sayılı karar ile izin alınmıştır (EK-5).

Birinci basamak sağlık hizmetleri kapsamında kullanılan Aile Hekimliği Bilgi Sistemi veri kayıt sisteminin incelenmesi için Bursa Sağlık Müdürlüğü Halk Sağlığı Hizmetleri Başkanlığı'ndan 06/09/2021 tarih ve E-72873149-604.02 sayılı karar ile izin alınmıştır (EK-6).

3.4.Zamanlama

	Mart 2020	Nisan 2020	Mayıs 2020	Haziran 2020	Temmuz 2020	Ağustos 2020	Eylül 2020	Ekim 2020	Kasım 2020	Aralık 2020	Ocak 2021	Şubat 2021	Mart 2021	Nisan 2021	Mayıs 2021
Yazın tarama/okuma															
Planlama ve Tez önerisinin hazırlanması															
Tez önerisinin sunumu															
Çalışmanın düzeltilmesi															
TİK'e ilk 6 aylık çalışmanın sunumu															
TİK'e çalışmanın ikinci sunumu															

	Haziran 2021	Temmuz 2021	Ağustos 2021	Eylül 2021	Ekim 2021	Kasım 2021	Aralık 2021	Ocak 2022	Şubat 2022	Mart 2022	Nisan 2022	Mayıs 2022	Haziran 2022	Temmuz 2022	Eylül 2022	Ekim 2022	Kasım 2022	Aralık 2022	Ocak 2023
Yazın tarama/okuma																			
TİK'e üçüncü 6 aylık çalışmanın sunumu																			
TİK'e dördüncü ve beşinci 6 aylık çalışmanın sunumu																			
Veri toplama ve verilerin analizi																			
Tezin yazımı																			
Tezin sunulması																			

4. BULGULAR

4.1.Düzenlemelerin Etik İlkelere Göre Analizi

Türkiye Anayasası başta olmak üzere kişisel verilerle ilgili kanun, tüzük, yönetmelik, yönerge, Hekimlik Meslek Etiği Kuralları (HMEK) ve Kişisel Verileri Koruma Kurulu'nun rehberleri olmak üzere toplam 44 düzenleme belirlenmiş ve ilkelere göre incelenmiştir.

4.1.1. Toplum yararı ilkesi

Toplum yararı ilkesine göre toplanan veriler halk sağlığı hedeflerine katkıda bulunmalı ve ortak yol gösterici etik değerler korunmalıdır. Toplum yararı amacıyla veri toplanırken ayrıca insan haklarına saygılı olunmalı, verilerin nasıl kullanıldığı konusunda bireylerin söz sahibi olmaları sağlanmalıdır. Bu kriterlere göre ilgili düzenlemeler incelendiğinde, KVK Kanunu'nda bu ilkenin sınırları 28. madde ile şu şekilde çizilmektedir (Kişisel Verilerin Korunması Kanunu, 2016);

> "İstisnalar Madde 28- (1) Bu Kanun hükümleri aşağıdaki hâllerde uygulanmaz: … 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 ihlal 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 istihbari faaliyetler kapsamında işlenmesi. d) Kişisel verilerin soruşturma, kovuşturma, yargılama veya infaz işlemlerine ilişkin olarak yargı makamları veya infaz mercileri tarafından işlenmesi."

Kanunun bu maddesinde, veri işlemenin istisnası olarak araştırma, planlama, istatistik, kamu düzeni, milli savunma ve güvenlik, ekonomik güvenlik gibi nedenlerle verinin "kanunla görev ve yetki verilmiş kamu kurum ve kuruluşları" tarafından işlenebileceği belirtilmektedir.

Toplum yararı ilkesi ile ilişkili olarak kişisel verilerin bilimsel amaçlarla işlenmesinin usul ve esasları, KSV Yönetmeliği'nin 16. maddesinde düzenlenmiştir (Kişisel Sağlık Verileri Hakkında Yönetmelik, 2019).

> "Bilimsel amaçlarla işleme MADDE 16 – (1) Kanunun 28 inci maddesinin birinci fıkrasının (b) bendi kapsamında veri sorumlusu tarafından anonim hâle getirilen kişisel sağlık verileri ile bilimsel çalışma yapılabilir. (2) Kanunun 28 inci maddesinin birinci fıkrasının (c) bendi kapsamında kişisel sağlık verileri, ilgili kişilerin özel hayatın gizliliğini veya kişilik haklarını ihlâl etmemek ya da suç teşkil etmemek kaydıyla alınacak teknik ve idari tedbirler çerçevesinde, bilimsel amaçlarla işlenebilir."

Maddenin birinci fıkrasında verinin bilimsel amaçlarla işlenebilmesi için anonim hale getirilmesi koşulu belirtilmektedir. İkinci fıkrada kanunda belirtilen veri işlemenin istisnaları kamu düzeni, milli savunma ve güvenlik, ekonomik güvenlik biçiminde belirtilmektedir.

Kişisel sağlık verilerinin bilimsel amaçlarla işlenmesi, Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği'nde de düzenlenmektedir (Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği, 2015).

> "Kayıt ve istatistik MADDE 10 – (1) TSM'nin kayıt ve istatistiğe ilişkin görevleri şunlardır: a) Bakanlığın belirlemiş olduğu standartlara uygun olarak bölgedeki sağlık hizmeti sunucularından veri toplamak, yürütülen hizmetlerin kayıt ve istatistiklerini elektronik veya basılı ortamda tutmak, olağanüstü durumlarda bölgedeki sağlık hizmeti sunucularından yazılı olarak da veri toplamak, topladığı verileri zamanında müdürlüğe iletmek."

Yönetmeliğin bu maddesinde, toplum sağlığı merkezlerinin kayıt ve istatistiğe ilişkin görevleri belirtilmekte ve olağandışı durumlarda veri toplanması ve toplanan verilerin müdürlüğe iletilmesi görevleri ile toplum sağlığının korunması amaçlanmaktadır.

Toplum yararı ilkesinin koşullarından biri, toplum yararı amacıyla veri toplanırken, insan haklarına saygılı olunması adına verilerin nasıl kullanıldığı konusunda bireylerin söz sahibi olmalarının sağlanması gerekliliğidir. Buna göre insan haklarının korunabilmesi için, kişisel verilerin korunması bir insan hakkı olarak tanınması gerekir. İnsan hakları en genel ifadeyle insan onuruna saygı ilkesini korumayı amaçlar. İlgili düzenlemeler incelendiğinde kişisel verinin korunması hakkı, özel hayatın

gizliliği kapsamında düzenlenmektedir. Anayasa'nın özel hayatın gizliliğini düzenleyen 20. maddesine eklenen ek fıkra ile kişisel verinin korunması hakkı tanımlanmıştır (T.C. Anayasası, 1982);

> "(Ek fıkra: 7/5/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

Ulus üstü düzenlemelerden biri olan İnsan Hakları ve Biyotıp Sözleşmesi'nin 10. maddesi özel yaşam ve bilgilendirme hakkı başlığı altında kişisel sağlık verilerinin korunması hakkını tanımlamıştır (Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Hakları ve İnsan Haysiyetinin Korunması Sözleşmesi: İnsan Hakları ve Biyotıp Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun, 2003);

> "Özel Yaşam ve Bilgilendirme Madde 10 - Özel yaşam ve bilgilendirme hakkı 1.Herkes, kendi sağlığıyla ilgili bilgiler bakımından, özel yaşamına saygı gösterilmesini isteme hakkına sahiptir. 2. Herkes, kendi sağlığı hakkında toplanmış herhangi bir bilgiyi öğrenme hakkına sahiptir. Bununla beraber, bireylerin, bilgilendirilmeme istekleri de gözetilecektir."

Borçlar Kanunu'nun 58. maddesi ile kişilik hakları zedelenen kişiler güvence altına alınmaktadır (Türk Borçlar Kanunu, 2011).

> "Kişilik hakkının zedelenmesi MADDE 58- Kişilik hakkının zedelenmesinden zarar gören, uğradığı manevi zarara karşılık manevi tazminat adı altında bir miktar para ödenmesini isteyebilir. Hâkim, bu tazminatın ödenmesi yerine, diğer bir giderim biçimi kararlaştırabilir veya bu tazminata ekleyebilir; özellikle saldırıyı kınayan bir karar verebilir ve bu kararın yayımlanmasına hükmedebilir."

Toplum yararı amacıyla veri toplanırken, insan haklarına saygılı olunması gerektiği, kişisel verilerin korunması hakkı bağlamında değerlendirilebilirken, verilerin nasıl kullanıldığına ilişkin bireylerin söz sahibi olmalarının sağlanması, sadece Anayasa'da düzenlenmektedir.

4.1.2. Minimum veri ilkesi

Minimum veri ilkesine göre kişisel veri işlendiği amaçla bağlantılı, sınırlı ve ölçülü olmalıdır. Kişisel verilerin işlenmesi gerekliliğinin ve bu kişisel verilerin uygunluğunun değerlendirilmesi, takip edilen amaç(lar) ışığında yapılmalıdır.

KVK Kanunu'nda minimum veri ilkesine, "Kişisel Verilerin İşlenmesi Genel ilkeler MADDE 4- … b) Doğru ve gerektiğinde güncel olma. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme." biçiminde yer vermektedir.

Kişisel Verileri Koruma Kurumu'nun yayımladığı Kişisel Veri Güvenliği Rehberi'nde bu ilkeye "Verilerin Mümkün Olduğunca Azaltılması" başlığı altında yer verilmektedir. Buna göre ilgili ifade şu şekildedir (KVKK, 2018b):

> "Kişisel Verilerin Mümkün Olduğunca Azaltılması Kanunun 4 üncü maddesinin ikinci fıkrasının (b) ve (d) bentleri uyarınca kişisel veriler, gerektiğinde doğru ve güncel olmalı, ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilmelidir. Ancak, özellikle uzun süredir faaliyet gösteren veri sorumluları, çok fazla miktarda kişisel veri toplamakta olduğundan söz konusu kişisel verilerin bir kısmı zamanla doğru olmayan, güncelliğini yitirmiş ve herhangi bir amaca hizmet etmeyen veriler haline gelebilmektedir. Bunun önüne geçebilmek için, veri sorumlularınca işleme amaçları bakımından anılan kişisel verilere hala ihtiyaç olup olmadığının değerlendirilmesi ve kişisel verilerin doğru yerde muhafaza edildiğinden emin olunması gerekmektedir…"

KVK Kanunu ve Kurum'un çıkarmış olduğu rehberde minimum veri ilkesi tanımlanırken, kişisel sağlık verileriyle doğrudan ilgili olan temel düzenleme KSV Yönetmeliği'nde tanımlanmadığı saptanmıştır.

4.1.3. Hassas veri ilkesi

Hassas veri ilkesi, KVK Kanunu ve KSV Yönetmeliği'nde "özel nitelikli veri" başlığı altında yer almaktadır. Kanunu'nun 6. maddesi, hassas veriyi özel nitelikli veri kategorisinde tanımlamakta ve bu tür verilerin işlenme koşullarını belirtmektedir. KSV Yönetmeliği'nde hassas veri ilkesi ayrıca tanımlanmamış, aynı anlamı taşıyan "özel nitelikli kişisel veri" ifadesi doğrudan kullanılmıştır. Bu yönetmeliğe göre kişisel

sağlık verisi "hassas veri" kategorisindedir (Kişisel Sağlık Verileri Hakkında Yönetmelik, 2019).

> "Özel nitelikli kişisel verilerin işlenme şartları Madde 6 (1) Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri özel nitelikli kişisel veridir."

KVK Kanunu'nun 2018 yılı kararı olarak resmi gazetede yayımlanan Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler kararında kişisel sağlık verileri, özel nitelikli kişisel veri biçiminde tanımlanmaktadır.

Aile Hekimliği Uygulama Yönetmeliği'nin 30. maddesi, kişisel sağlık verilerini "resmi kayıt ve evrak" niteliğinde kabul etmektedir (Aile Hekimliği Uygulama Yönetmeliği, 2013).

> "Tutulacak kayıtlar MADDE 30 – (1) Aile hekimlerinin kullandığı basılı veya elektronik ortamda tutulan kayıtlar, kişilerin sağlık dosyaları ile raporlar, sevk belgesi ve reçete gibi belgeler resmî kayıt ve evrak niteliğindedir."

Genel olarak doğrudan ilgili düzenlemeler (KVK Kanunu ve KSV Yönetmeliği) kişisel sağlık verilerini "hassas veri ilkesi" kapsamında değerlendirmektedir. Diğer düzenlemelerin ilgili maddelerinde hassas veri ilkesini tanımlayan bir ifade saptanmamış, yalnızca Aile Hekimliği Uygulama Yönetmeliği'nde farklı bir yaklaşım olarak sağlık kayıtları resmi evraklar olarak nitelendirildiği saptanmıştır.

4.1.4. Eşitlik ve adalet ilkesi

Eşitlik ve adalet ilkesine göre sağlık hakkı kapsamında sağlık veri tabanlarına herkes erişilebilir olmalı, veri kayıt sistemleriyle ilgili sosyoekonomik, coğrafi ve etnik ayrımcılık yapılmamalı ve veri kayıt sistemleri damgalanmaya yol açmamalıdır. Bununla birlikte bilgi ve iletişim teknolojilerine erişim, kültür, dil, gelir düzeyi ve yaş gibi değişkenler açısından sağlanmalı ve dezavantajlı grupların menfaatleri ve hakları korunmalıdır. Bu ilkeye göre düzenlemeler incelendiğinde KSV Yönetmeliği'nin 6. maddesi, e-Nabız hesabı bulunmayan kişilerin haklarını düzenlemektedir (Kişisel

Sağlık Verileri Hakkında Yönetmelik, 2019):

> "Sağlık personelinin verilere erişimi MADDE 6 – … (3) e-Nabız hesabı bulunmayan kişilerin sağlık verilerine ise Kanunun 6 ncı maddesinin üçüncü fıkrasında yer alan istisnai amaçlarla sınırlı olmak üzere ancak; a) Kişinin kayıtlı olduğu aile hekimi tarafından herhangi bir süre sınırı olmaksızın, b) Kişinin sağlık hizmeti almak üzere randevu aldığı hekim tarafından, randevunun alındığı gün ile sınırlı olmak kaydıyla ve alınan sağlık hizmeti ile doğrudan bağlantılı işlemler sonlanana kadar, c) Kişinin sağlık hizmeti almak üzere giriş yaptığı sağlık hizmeti sunucusunda görev yapan hekimler tarafından, yirmi dört saat süre ile sınırlı olmak kaydıyla, ç) Hastanın yatışının yapıldığı sağlık hizmeti sunucusunda görev yapan hekimler tarafından, hasta sağlık hizmeti sunucusundan taburcu olana kadar, erişilebilir."

Yönetmeliğin 8. maddesinde, ayrıt etme gücüne sahip çocukların, e-Nabız kaydına erişim için ebeveynlerini izne tabi tutma hakları bulunmaktadır (Kişisel Sağlık Verileri Hakkında Yönetmelik, 2019).

> "Çocukların sağlık verilerine erişim MADDE 8 – (1) Ebeveynler, çocuklarına ilişkin sağlık kayıtlarına herhangi bir onaya ihtiyaç duyulmaksızın e-Nabız üzerinden erişebilir. Ayırt etme gücüne sahip çocuklar, sağlık geçmişlerine ebeveynlerinin erişimini e-Nabız üzerinden izne tabi tutabilir. (2) Anne ve babanın boşanması hâlinde velâyet hakkı üzerinde bırakılmayan taraf, çocuk ile velinin faydası gözetilmek suretiyle kişisel verilerin korunması mevzuatına uygun şekilde ve Genel Müdürlükçe belirlenen sınırlar çerçevesinde çocuğa ilişkin sağlık verilerine erişebilir."

Yönetmeliğin 11. Maddesi, ölen kişilerin sağlık verilerine erişimi düzenlemektedir (Kişisel Sağlık Verileri Hakkında Yönetmelik, 2019).

> "Ölünün sağlık verilerine erişim MADDE 11 – (1) Ölmüş bir kimsenin sağlık verilerini almaya, veraset ilamını ibraz etmek suretiyle murisin yasal mirasçıları münferit olarak yetkilidir. (2) Ölmüş bir kimsenin sağlık verileri, en az 20 yıl süre ile saklanır."

Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği'nin "AÇS-AP birimi MADDE 40 – AÇS-AP biriminin görevleri… ı) Kadın, ana, çocuk, ergen ve üreme sağlığı konuları ile ilgili yürüttüğü hizmetlerin kayıt ve bildirimlerini yapmak." biçimindeki 40. maddesi, kadınların, çocukların, ergenlerin ve üreme sağlığı ile ilgili kayıtların

tutulmasını sağlık hizmetine erişim hakkı kapsamında ele almaktadır (Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği, 2015).

Özel Hastaneler Yönetmeliği'nin 52. maddesi sağlık kayıtlarının ücretsiz bir şekilde hastaya verilmesi hakkını ele almaktadır (Özel Hastaneler Yönetmeliği, 2022);

> "Hastalara verilecek belgeler Madde 52- Özel hastaneler, hastalar tarafından istenildiğinde, aşağıda belirtilen belgeleri ücretsiz olarak vermek zorundadırlar: a) Özel hastanede kullanılıp bedeli hastadan alınan ilaç ve sarf malzemesinin tür ve miktarlarını gösteren liste, b) (Değişik:RG-22/3/2017-30015)Adlî vakalara ilişkin olanların asılları verilmemek kaydıyla, özel hastanede veya dışarıda yapılan ve bedeli hasta tarafından ödenen her türlü tetkik, tahlil ve görüntüleme sonuçları, c) Dışarıdan satın alınan ilaç ve malzemenin reçeteleri, d) Hastaların klinik ve laboratuvar bulguları, hastalığın teşhisi, seyri, yapılan incelemeler ile tedavi ve sonucuna ilişkin tedaviyi yapan tabip tarafından düzenlenecek çıkış özeti."

HMEK'in 43. maddesi bilimsel araştırmalarda deneğin kimliğinin gizli tutulmasını vurgulamakta ve deneğin kişisel verilerinin korunması hakkını belirtmektedir. Buna göre ilgili madde şu şekildedir: "Deneğin Korunması Madde 43 - İnsan üzerinde yapılan tıbbi araştırmalarda… Deneğin özel yaşamına saygı gösterilmesi ve kişisel bilgilerin gizliliği sağlanır. Bilimsel araştırma ve yayınlar ile akademik-bilimsel amaçlı sunuşlarda deneğin kimliği gizli tutulur." (TTB, 2012). Aynı düzenlemenin 35. maddesi tutuklu ve hükümlülerin gizlilik haklarının korunması gerektiğini belirterek hükümlünün kişisel verilerini korunmaktadır (TTB, 2012).

> "Tutuklu ve Hükümlülere Verilecek Tıbbi Yardım Madde 35 - Tutuklu ve hükümlülerin muayenesi de öteki hastalarınki gibi, kişilik haklarına saygılı, hekimlik sanatını uygulamaya elverişli koşullarda yapılır ve onların gizlilik hakları korunur. Hekimin, bu koşulların sağlanması için ilgililerden istekte bulunma hakkı ve sorumluluğu vardır. Muayene sonucu düzenlenecek belge veya raporlarda hekimin adı, soyadı, diploma numarası ve imzası mutlaka bulunur. Belge ve raporun bir örneği kişiye verilir. Belge ve rapor baskı altında yazılmış ise, hekim bu durumu en kısa zamanda meslek örgütüne bildirir."

Bu iki madde savunmasız gruplar olarak deneklerin ve tutuklu veya hükümlülerin kişisel verisinin korunması hakkını gözetmesi bakımından eşitlik ve adalet ilkesi ile ilgilidir.

4.1.5. Özerklik ilkesi

Özerklik ilkesi için her bireyin profiline ve veri denetleyicisinin kendileri hakkında sahip olduğu tüm bilgilere erişimi olmalı; profil oluşturma veya karar verme için temel olarak hangi algoritmaların kullanıldığı bilgisine erişimi olmalı; bireyler, verilerin kullanımı hakkında bilgi talep edebilmeli, bunlarla ilgili hata veya eksikliklerin düzeltilmesini isteyebilmeli, uygulamayı devre dışı bırakabilmeli ve tanımlanabilir verileri silebilmelidir.

KVK Kanunu'nun 11. maddesi özerklikle ilgilidir (Kişisel Verilerin Korunması Kanunu, 2016);

> "İlgili kişinin hakları Madde 11- (1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili; a) Kişisel veri işlenip işlenmediğini öğrenme, b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme. c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme. ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme. d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini istem. e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme, f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme. g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme. ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir."

KSV Yönetmeliği'nin 6. maddesi özerklikle ilgilidir (Kişisel Sağlık Verileri Hakkında Yönetmelik, 2019);

> "Sağlık personelinin verilere erişimi MADDE 6 – (2) e-Nabız hesabı bulunan kişilerin sağlık verilerine, kendi gizlilik tercihleri çerçevesinde erişim sağlanır. İlgili *kişiler,* gizlilik tercihleri ve sonuçları konusunda ayrıntılı şekilde bilgilendirilir. Gizlilik tercihi ve geçmiş sağlık verilerinin görüntülenememesi nedeniyle sağlık hizmeti sunumunda meydana gelebilecek aksaklık ve zararlardan Bakanlık sorumlu olmaz. (5) Geçmiş sağlık verilerinin herhangi bir kimse tarafından erişilmesini istemeyen kişilere ilgili gizlilik tercihi e-Nabız üzerinden sunulur. Bu gizlilik tercihini kullanan kişilerin geçmiş sağlık verilerine ancak kişinin kendisi tarafından beyan edilen telefon numarasına gönderilecek olan kodun hekim ile paylaşılması ve hekim tarafından sisteme girilmesi halinde erişilebilir."

Bu maddeye göre kişilerin e-Nabız ile ilgili gizlilik tercihi konusunda bilgilendirilme ve uygulamaya erişim konusunda gizlilik tercihinde bulunulabilme hakları tanımlanmaktadır. Bununla birlikte hekimin hastanın e-Nabız kaydına erişim sağlayabilmesi için hastaya gelen kodun hekim ile paylaşılabilmesi gerektiğini bildirmektedir. Yönetmeliğin 13. maddesi, kişisel sağlık verilerinin düzeltilmesi hususunu düzenleyerek özerklikle ilgiliyken, 14. madde kişisel verilerin imha edilmesini düzenlemesi açısından özerklik kapsamındadır (Kişisel Sağlık Verileri Hakkında Yönetmelik, 2019):

> "Kişisel sağlık verilerinin düzeltilmesi MADDE 13 – (1) İlgili kişi, kendisi hakkında sehven oluşturulan sağlık verilerinin düzeltilmesi hususunda sağlık verisinin oluşturulduğu sağlık hizmeti sunucusunun bağlı bulunduğu il sağlık müdürlüğüne başvurur. İl sağlık müdürlüğü, ilgili sağlık hizmeti sunucusunda yapacağı araştırma neticesinde sağlık verisinin sehven oluşturulduğu bilgisine ulaşırsa resmi yazı ile Genel Müdürlüğe başvurur ve sehven oluşturulan sağlık verisinin düzeltilmesini ister. (2) Genel Müdürlük tarafından tesis edilecek işlem, sağlık hizmeti sunucusunun kendi veri tabanında da gerçekleştirilir. (3) Genel Müdürlük, sağlık hizmeti sunucuları tarafından oluşturulan sağlık verilerinin kendileri tarafından düzeltilebileceği tarihi belirler ve bu tarihi ihtiyaca göre günceller. Genel Müdürlükçe belirlenen bu tarihten sonra oluşturulan sağlık verileri ilgili sağlık hizmeti sunucusu tarafından; bu tarihten önce oluşturulan sağlık verileri ise ilgili il sağlık müdürlüğünün talebi üzerine Genel Müdürlükçe düzeltilir. Kişisel sağlık verilerinin imha edilmesi MADDE 14 – (1) Kişisel verilerin imha edilmesinde, Kanunun 7 nci maddesi ile Kurum tarafından hazırlanarak 28/10/2017 tarihli ve 30224 sayılı Resmî Gazete'de yayımlanan Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik hükümlerine riayet edilir."

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in 8. maddesi, kişisel sağlık verilerinin silinmesini, 9. maddesi verilerin yok edilmesini ve 12. maddesi talep edilmesi durumunda kişisel verilerin silme ve yok edilmesini düzenlemesi bakımından doğrudan özerklik ile ilgilidir (Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik, 2017).

> "Kişisel verilerin silinmesi MADDE 8 – (1)Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. (2) Veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür."

Yönetmeliğin 9. maddesi verilerin yok edilmesini düzenlemektedir (Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, 2017).

> "Kişisel verilerin yok edilmesi MADDE 9 – (1) Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. (2) Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür."

Kişisel verilerin ilgili kişinin talep etmesi durumunda silinmesi ve yok edilmesi süreleri, Yönetmeliğin 12. maddesi ile düzenlenmektedir (Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, 2017).

> "Kişisel verileri ilgili kişinin talep etmesi durumunda silme ve yok etme süreleri MADDE 12 – (1) İlgili kişi, Kanunun 13 üncü maddesine istinaden veri sorumlusuna başvurarak kendisine ait kişisel verilerin silinmesini veya yok edilmesini talep ettiğinde; a) Kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa; veri sorumlusu talebe konu kişisel verileri siler, yok eder veya anonim hale getirir. Veri sorumlusu, ilgili kişinin talebini en geç otuz gün içinde sonuçlandırır ve ilgili kişiye bilgi verir. b) Kişisel verileri işleme şartlarının tamamı ortadan kalkmış ve talebe konu olan kişisel veriler üçüncü kişilere aktarılmışsa veri sorumlusu bu durumu üçüncü kişiye bildirir; üçüncü kişi nezdinde bu Yönetmelik kapsamında gerekli işlemlerin yapılmasını temin eder. c) Kişisel verileri işleme şartlarının tamamı ortadan kalkmamışsa, bu talep veri sorumlusunca Kanunun 13 üncü maddesinin üçüncü fıkrası uyarınca gerekçesi açıklanarak reddedilebilir ve ret cevabı ilgili kişiye en geç otuz gün içinde yazılı olarak ya da elektronik ortamda bildirilir."

Yönetmeliğin bu maddesine göre, ilgili kişinin talebi halinde verilerin silinmesi veya yok edilmesi koşula bağlanmıştır. (a) bendinde belirtildiği üzere verinin silinmesi veya yok edilebilmesi için işlenme şartlarının tamamının ortadan kalkması gerekmektedir.

Hasta Hakları Yönetmeliği'nin 16. ve 17. maddeleri özerklikle ilgilidir (Hasta Hakları Yönetmeliği, 1998);

> "Kayıtları İnceleme Madde 16- Hasta, sağlık durumu ile ilgili bilgiler bulunan dosyayı ve kayıtları, doğrudan veya vekili veya kanuni temsilcisi vasıtası ile inceleyebilir ve bir suretini alabilir. Bu kayıtlar, sadece hastanın tedavisi ile doğrudan ilgili olanlar tarafından görülebilir. Kayıtların Düzeltilmesini İsteme Madde 17- Hasta; sağlık kurum ve kuruluşları nezdinde bulunan kayıtlarında eksik, belirsiz ve hatalı tıbbi ve şahsi bilgilerin tamamlanmasını, açıklanmasını,

> düzeltilmesini ve nihai sağlık durumu ve şahsi durumuna uygun hale getirilmesini isteyebilir. Bu hak, hastanın sağlık durumu ile ilgili raporlara itiraz ve aynı veya başka kurum ve kuruluşlarda sağlık durumu hakkında yeni rapor düzenlenmesini isteme haklarını da kapsar."

Yönetmeliğin 16. maddesine göre veri ilgilisinin kayıtları inceleme hakkı, 17. maddesine göre kayıtların düzeltilmesini isteme hakları bulunmaktadır. Yönetmeliğe göre bireyin kayıtları inceleme ve düzeltilmesini isteme hakları bulunurken, kayıtların silinmesi veya silinmesini isteme hakkının düzenlenmediği saptanmıştır.

Aile Hekimliği Uygulama Yönetmeliği'nin "Kayıtların tutulma şekli ve muhafazası MADDE 31 – (3) Kişi, kendisi ile ilgili tutulan kayıtların bir nüshasını aile hekiminden talep edebilir." biçimindeki 31. maddesi özerklikle ilgilidir (Aile Hekimliği Uygulama Yönetmeliği, 2013). Kayıtlı bilgileri talep etme hakkı HMEK'in 31. maddesi ile düzenlenmektedir. Buna göre; "Hastayla İlgili Bilgilerin Hastaya Verilmesi ve Kullanımı Madde 31 - Hasta dosyalarındaki bilgilerin geniş bir özeti ile bilgi ve belgelerin örnekleri, isteği durumunda hastaya verilir..." (TTB, 2012).

Özerklik ilkesi özel sağlık kuruluşlarındaki yeri açısından incelendiğinde, Özel Hastaneler Yönetmeliği'nin 52. maddesinin hastaların kişisel verilerine ücretsiz erişim hakkını ele aldığı saptanmıştır (Özel Hastaneler Yönetmeliği, 2002).

> "Hastalara verilecek belgeler Madde 52- Özel hastaneler, hastalar tarafından istenildiğinde, aşağıda belirtilen belgeleri ücretsiz olarak vermek zorundadırlar: a) Özel hastanede kullanılıp bedeli hastadan alınan ilaç ve sarf malzemesinin tür ve miktarlarını gösteren liste, b) (Değişik:RG-22/3/2017-30015)Adlî vakalara ilişkin olanların asılları verilmemek kaydıyla, özel hastanede veya dışarıda yapılan ve bedeli hasta tarafından ödenen her türlü tetkik, tahlil ve görüntüleme sonuçları, c) Dışarıdan satın alınan ilaç ve malzemenin reçeteleri, d) Hastaların klinik ve laboratuvar bulguları, hastalığın teşhisi, seyri, yapılan incelemeler ile tedavi ve sonucuna ilişkin tedaviyi yapan tabip tarafından düzenlenecek çıkış özeti."

Bilgi Edinme Hakkı Kanunu'nun 4. maddesi, bilgi edinme hakkını; 5. maddesi, kurum ve kuruluşların bilgi verme yükümlülüğünü; 6, 7 ve 8. maddeleri bilgi edinme başvurusunun nasıl yapılacağını; 10 ve 11. maddeleri verilere erişim ve erişim süreleri ile ilgili bilgileri düzenlemektedir. Kanunun bu maddeleri özerklik ve onam ile ilgilidir (Bilgi Edinme Hakkı Kanunu, 2003);

> “Bilgi edinme hakkı Madde 4- Herkes bilgi edinme hakkına sahiptir. Türkiye'de ikamet eden yabancılar ile Türkiye'de faaliyette bulunan yabancı tüzel kişiler, isteyecekleri bilgi kendileriyle veya faaliyet alanlarıyla ilgili olmak kaydıyla ve karşılıklılık ilkesi çerçevesinde, bu Kanun hükümlerinden yararlanırlar. Bilgi verme yükümlülüğü Madde 5- Kurum ve kuruluşlar, bu Kanunda yer alan istisnalar dışındaki her türlü bilgi veya belgeyi başvuranların yararlanmasına sunmak ve bilgi edinme başvurularını etkin, süratli ve doğru sonuçlandırmak üzere, gerekli idarî ve teknik tedbirleri almakla yükümlüdürler. Bu Kanun yürürlüğe girdiği tarihten itibaren diğer kanunların bu Kanuna aykırı hükümleri uygulanmaz. Bilgi veya belgeye erişim Madde 10- Kurum ve kuruluşlar, başvuru sahibine istenen belgenin onaylı bir kopyasını verirler. Bilgi veya belgenin niteliği gereği kopyasının verilmesinin mümkün olmadığı veya kopya çıkarılmasının aslına zarar vereceği hâllerde, kurum ve kuruluşlar ilgilinin; a) Yazılı veya basılı belgeler için, söz konusu belgenin aslını incelemesi ve not alabilmesini, b) Ses kaydı şeklindeki bilgi veya belgelerde bunları dinleyebilmesini, c) Görüntü kaydı şeklindeki bilgi veya belgelerde bunları izleyebilmesini, sağlarlar. Bilgi veya belgenin yukarıda belirtilenlerden farklı bir şekilde elde edilmesi mümkün ise, belgeye zarar vermemek koşuluyla bu olanak sağlanır. Başvurunun yapıldığı kurum ve kuruluş, erişimine olanak sağladığı bilgi veya belgeler için başvuru sahibinden erişimin gerektirdiği maliyet tutarı kadar bir ücreti bütçeye gelir kaydedilmek üzere tahsil edebilir. Bilgi veya belgeye erişim süreleri Madde 11- Kurum ve kuruluşlar, başvuru üzerine istenen bilgi veya belgeye erişimi onbeş iş günü içinde sağlarlar. Ancak istenen bilgi veya belgenin, başvurulan kurum ve kuruluş içindeki başka bir birimden sağlanması; başvuru ile ilgili olarak bir başka kurum ve kuruluşun görüşünün alınmasının gerekmesi veya başvuru içeriğinin birden fazla kurum ve kuruluşu ilgilendirmesi durumlarında bilgi veya belgeye erişim otuz iş günü içinde sağlanır. Bu durumda, sürenin uzatılması ve bunun gerekçesi başvuru sahibine yazılı olarak ve onbeş iş günlük sürenin bitiminden önce bildirilir. 10 uncu maddede belirtilen bilgi veya belgelere erişim için gereken maliyet tutarının idare tarafından başvuru sahibine bildirilmesiyle onbeş iş günlük süre kesilir. Başvuru sahibi onbeş iş günü içinde ücreti ödemezse talebinden vazgeçmiş sayılır. Başvuruların cevaplandırılması Madde 12- Kurum ve kuruluşlar, bilgi edinme başvurularıyla ilgili cevaplarını yazılı olarak veya elektronik ortamda başvuru sahibine bildirirler. Başvurunun reddedilmesi hâlinde bu kararın gerekçesi ve buna karşı başvuru yolları belirtilir.”

Bilgi Edinme Kanunu’nun 21. maddesinde özel hayatın gizliliği gözetilerek bilgi edinme hakkı sınırlandırılmaktadır (Bilgi Edinme Hakkı Kanunu, 2003).

> “Bilgi Edinme Hakkının Sınırları Özel hayatın gizliliği Madde 21- Kişinin izin verdiği hâller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması hâlinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve haysiyetine, meslekî ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır. Kamu yararının gerektirdiği hâllerde, kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir.”

Özerklik ceza hukuku açısından incelendiğinde Türk Ceza Kanunu özerkliği, bireyin şikayetine bağlı olarak korumaktadır (Türk Ceza Kanunu, 2004);

> “Şikayet Madde 139- (1) Kişisel verilerin kaydedilmesi, verileri hukuka aykırı olarak verme veya ele geçirme ve verileri yok etmeme hariç, bu bölümde yer alan suçların soruşturulması ve kovuşturulması şikayete bağlıdır.”

Özerklik kişilik hakkı ile doğrudan ilgili olduğu için Borçlar Kanunun 58. maddesinde kişilik hakkının zedelenmesi başlığında ele alınmaktadır (Türk Borçlar Kanunu, 2011);

> “3. Kişilik hakkının zedelenmesi MADDE 58- Kişilik hakkının zedelenmesinden zarar gören, uğradığı manevi zarara karşılık manevi tazminat adı altında bir miktar para ödenmesini isteyebilir. Hâkim, bu tazminatın ödenmesi yerine, diğer bir giderim biçimi kararlaştırabilir veya bu tazminata ekleyebilir; özellikle saldırıyı kınayan bir karar verebilir ve bu kararın yayımlanmasına hükmedebilir.”

Özerklik Anayasası’nın 20. maddesi ve İnsan Hakları ve Biyotıp Sözleşmesi’nin 10. maddesinde özel yaşamın gizliliği kapsamında da korunmaktadır.

Özerklik ilkesinin korunabilmesi için bir diğer koşul aydınlatılmış onam alınmasıdır. Bu onam, kişinin bazı noktalarda aydınlatılmasına dayanmalıdır (Bkz. s.58). Yöntem bölümünde belirtilen onam ile ilgili koşullara göre ilgili düzenlemeler incelendiğinde KVK Kanunu’nun 10. ve 11. maddeleri aydınlatılmış onamı düzenlemektedir (Kişisel Verilerin Korunması Kanunu, 2016);

> “Veri sorumlusunun aydınlatma yükümlülüğü Madde 10- (1) Kişisel verilerin elde edilmesi sırasında veri sorumlusu veya yetkilendirdiği kişi, ilgili kişilere; a) Veri sorumlusunun ve varsa temsilcisinin kimliği. b) Kişisel verilerin hangi amaçla işleneceği. c) İşlenen kişisel verilerin kimlere ve hangi amaçla aktarılabileceği. ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi. d) 11 inci

maddede sayılan diğer hakları, konusunda bilgi vermekle yükümlüdür. İlgili kişinin hakları Madde 11- (1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili; a) Kişisel veri işlenip işlenmediğini öğrenme. b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme. c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme. ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme. d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme. e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme. f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme. g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme. ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir."

Aydınlatılmış onam KSV Yönetmeliği'nin 5. maddesinde belirtilmekte ve bu maddede kurul tarafından yayımlanan Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ başlıklı düzenlemenin hükümlerine riayet edileceği ifade edilmektedir. Bu tebliğin 5. maddesinde onamın koşulları şu şekilde açıklanmaktadır (KVKK, 2018a).

"Usul ve esaslar MADDE 5 – (1) Veri sorumlusu ya da yetkilendirdiği kişi tarafından sözlü, yazılı, ses kaydı, çağrı merkezi gibi fiziksel veya elektronik ortam kullanılmak suretiyle aydınlatma yükümlülüğünün yerine getirilmesi esnasında aşağıda sayılan usul ve esaslara uyulması gerekmektedir: a) İlgili kişinin açık rızasına veya Kanundaki diğer işleme şartlarına bağlı olarak kişisel veri işlendiği her durumda aydınlatma yükümlülüğü yerine getirilmelidir. b) Kişisel veri işleme amacı değiştiğinde, veri işleme faaliyetinden önce bu amaç için aydınlatma yükümlülüğü ayrıca yerine getirilmelidir. c) Veri sorumlusunun farklı birimlerinde kişisel veriler farklı amaçlarla işleniyorsa, aydınlatma yükümlülüğü her bir birim nezdinde ayrıca yerine getirilmelidir. ç) Sicile kayıt yükümlülüğünün bulunması durumunda, aydınlatma yükümlülüğü çerçevesinde ilgili kişiye verilecek bilgiler, Sicile açıklanan bilgilerle uyumlu olmalıdır. d) Aydınlatma yükümlülüğünün yerine getirilmesi, ilgili kişinin talebine bağlı değildir. e) Aydınlatma yükümlülüğünün yerine getirildiğinin ispatı veri sorumlusuna aittir. f) Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir. g) Aydınlatma yükümlülüğü kapsamında açıklanacak kişisel veri işleme amacının belirli, açık ve meşru olması gerekir. Aydınlatma yükümlülüğü yerine getirilirken, genel nitelikte ve muğlak ifadelere yer verilmemelidir. Gündeme

gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaatini uyandıran ifadeler kullanılmamalıdır. ğ) Aydınlatma yükümlülüğü kapsamında ilgili kişiye yapılacak bildirimin anlaşılır, açık ve sade bir dil kullanılarak gerçekleştirilmesi gerekmektedir. h) Kanunun 10 uncu maddesinin birinci fıkrasının (ç) bendinde yer alan "hukuki sebep" ten kasıt, aydınlatma yükümlülüğü kapsamında kişisel verilerin Kanunun 5 ve 6 ncı maddelerinde belirtilen işleme şartlarından hangisine dayanılarak işlendiğidir. Aydınlatma yükümlülüğünün yerine getirilmesi esnasında hukuki sebebin açıkça belirtilmesi gerekmektedir. ı) Aydınlatma yükümlülüğü kapsamında, kişisel verilerin aktarılma amacı ve aktarılacak alıcı grupları belirtilmelidir. i) Aydınlatma yükümlülüğü kapsamında kişisel verilerin, tamamen veya kısmen otomatik yollarla ya da veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yöntemlerden hangisiyle elde edildiği açık bir şekilde belirtilmelidir. j) Aydınlatma yükümlülüğü yerine getirilirken eksik, ilgili kişileri yanıltıcı ve yanlış bilgilere yer verilmemelidir."

4.1.6. Mahremiyet ve gizlilik ilkesi

Mahremiyet ve gizlilik ilkesinin korunabilmesi için yöntem bölümünde tanımlandığı üzere toplum yararı ve minimum veri ilkeleri gözetilmeli, anonimleştirme ilkesine özen gösterilmeli ve gizliliğe dayalı şeffaflık ilkesi korunmalıdır. Bilgiye yalnızca yetkili kişiler onam alarak erişim sağlamalı ve bilgilerin üçüncü taraflarla paylaşılmayacağı güvence altına alınmalıdır. Mahremiyet ve gizlilik ilkesinin korunmasının en önemli koşulu veri güvenliğinin sağlanmasıdır. Sınırsız bir veri güvenliğinden söz edilebilmesi oldukça güç olduğundan veri güvenliğini artırabilmek için önerilen dört aşamanın uygulanması gerekmektedir (Bkz. s.61).

Anayasanın 20. maddesi mahremiyeti, özel hayatın gizliliğini tanımlayarak ele almaktadır (T.C. Anayasası, 1982);

> "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz. …Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir..."

KVK Kanunu'nun 12. maddesi, veri güvenliğine ilişkin yükümlülükleri tanımlamaktadır (Kişisel Verilerin Korunması Kanunu, 2016);

> "Veri güvenliğine ilişkin yükümlülükler, Madde 12- (1) Veri sorumlusu; a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek. b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek. c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır. (2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur. (3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır. (4) Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder. (5) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir."

Kanunun bu maddesi, veri güvenliğinin sağlanabilmesi için gerekli olan koşulları belirtmektedir. Mahremiyet ve gizlilik ilkesinin korunabilmesi için toplanan verinin üçüncü taraflarla paylaşılmaması gerekmektedir. KVK Kanunu kapsamında kişisel verilerin yurt içi ve yurt dışına aktarımı 8. ve 9. maddelerde belirtilmektedir. Bu iki madde, kişisel verinin gerekli önlemlerin alınması koşuluyla aktarımını mümkün kılmaktadır. Kanunun 8. maddesi;

> "Kişisel verilerin aktarılması MADDE 8- (1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz. (2) Kişisel veriler; a) 5 inci maddenin ikinci fıkrasında, b) Yeterli önlemler alınmak kaydıyla, 6 ncı maddenin üçüncü fıkrasında, belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir. (3) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır."

Sekizinci maddenin ikinci fıkrasında kanunun 6. maddesinde belirtilen şartlardan birinin bulunması halinde açık rıza aranmaksızın verinin aktarılacağı belirtilmektedir. İlgili maddenin üçüncü fıkrası şu şekildedir (Kişisel Verilerin Korunması Kanunu, 2016);

> “MADDE 6 - (3) Birinci fıkrada sayılan 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.”

Kanunun 9. maddesinde verinin yurt dışına aktarımı için gerekli koşullar belirtilmektedir;

> “Kişisel verilerin yurt dışına aktarılması MADDE 9- (1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz. (2) Kişisel veriler, 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede; a) Yeterli korumanın bulunması, b) Yeterli korumanın bulunmaması durumunda Türkiye’deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması, kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir. (3) Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilir. (4) Kurul yabancı ülkede yeterli koruma bulunup bulunmadığına ve ikinci fıkranın (b) bendi uyarınca izin verilip verilmeyeceğine; a) Türkiye’nin taraf olduğu uluslararası sözleşmeleri, b) Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu, c) Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç ve süresini, ç) Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını, d) Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri, değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verir. (5) Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye’nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir. (6) Kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.”

Bu maddeye göre yurt dışı aktarım için altıncı maddenin üçüncü fıkrasına ek olarak beşinci maddenin ikinci fıkrasında belirtilen şartların varlığı halinde verinin yurt dışına aktarımı mümkündür;

> "(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür: a) Kanunlarda açıkça öngörülmesi. b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki 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. ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması. d) İlgili kişinin kendisi tarafından alenileştirilmiş olması. e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması. f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması."

KSV Yönetmeliği'nin 5., 6., 7. ve 12. maddeleri kişisel sağlık verilerinin mahremiyet ve gizliliğini korumakla ilgilidir (Kişisel Sağlık Verileri Hakkında Yönetmelik, 2019);

> "Genel ilke ve esaslar MADDE 5 – (1) Kişisel verilerin işlenmesinde Kanunun 4 üncü maddesinde yer alan genel ilkeler başta olmak üzere, Kanunda yer alan bütün esaslara riayet edilir. (2) Herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi maksadıyla, Bakanlık ile bağlı ve ilgili kuruluşlarınca gerekli kayıt ve bildirim sistemi kurulur. Bu sistem, e-Devlet uygulamalarına uygun olarak elektronik ortamda da oluşturulabilir. Bu amaçla Bakanlık tarafından, bağlı ve ilgili kuruluşları da kapsayacak şekilde ülke çapında bilişim sistemleri kurulabilir. (3) Hiç kimse, sağlık hizmeti sunumu için gerekli olan durumlar haricinde geçmiş sağlık verilerinin dökümünü sunmaya veya göstermeye zorlanamaz. (5) Sağlık hizmeti sunucuları, tahlil ve tetkik sonuçları gibi hastaya ait kişisel sağlık verilerini içeren basılı materyal üzerinde gerekli kısmî kimliksizleştirme veya maskeleme tedbirlerini uygular ve söz konusu materyalin yetkisiz kişilerin eline geçmesi hâlinde kime ait olduğunun tespit edilmesini zorlaştıracak diğer tedbirleri alır. Sağlık personelinin verilere erişimi MADDE 6 – (3) e-Nabız hesabı bulunmayan kişilerin sağlık verilerine ise Kanunun 6 ncı maddesinin üçüncü fıkrasında yer alan istisnai amaçlarla sınırlı olmak üzere ancak; a) Kişinin kayıtlı olduğu aile hekimi tarafından herhangi bir süre sınırı olmaksızın, b) Kişinin sağlık hizmeti almak üzere randevu aldığı hekim tarafından, randevunun alındığı gün ile sınırlı olmak kaydıyla ve alınan sağlık hizmeti ile doğrudan bağlantılı işlemler sonlanana kadar, c) Kişinin sağlık hizmeti almak üzere giriş yaptığı sağlık hizmeti sunucusunda görev yapan hekimler tarafından, yirmi dört saat süre ile sınırlı olmak kaydıyla, ç) Hastanın yatışının yapıldığı sağlık hizmeti sunucusunda görev yapan hekimler tarafından, hasta sağlık hizmeti sunucusundan taburcu olana kadar, erişilebilir. (6) Mahremiyet düzeyi daha yüksek olan, başkaları tarafından görülmesi ve

bilinmesi halinde kişilerin sosyal hayatını ve ruh sağlığını olumsuz etkileme riski taşıyan kişisel sağlık verileri Bakanlıkça belirlenir ve sağlık personelinin bu verilere erişimine ölçülü kısıtlar getirilebilir. Bakanlık birimlerinin verilere erişimi MADDE 7 – (1) Sağlık hizmeti sunucuları tarafından merkezi sağlık veri sistemine kimliksizleştirilerek gönderilen sağlık verilerini, ilişkisel veri tabanı aracılığı ile ait oldukları kişilerle eşleştirmeye yetkili kişileri Bakanlığın birim amirleri ayrı ayrı belirler ve Genel Müdürlükten bu kişilerin yetkilendirilmesini talep eder. Her birimin amiri, kendi biriminden en fazla üç kişinin yetkilendirilmesini talep edebilir. Kişisel sağlık verilerinin gizlenmesi MADDE 12 – (1) Hakkında gizlilik kararı verilen kişilere ait verilerin gizlenmesi için yargı makamları tarafından gönderilen müzekkerenin gereği il sağlık müdürlüğü tarafından yerine getirilir. İl sağlık müdürlüğü tarafından tesis edilen işlem doğrudan Kimlik Paylaşım Sistemine de yansır. Gizlilik kararlarının sadece görevi gereği bilmesi gereken kişiler tarafından bilinmesini sağlamak üzere gerekli her türlü teknik ve idari tedbirler alınır."

Yönetmeliğin 17. maddesi, mahremiyet ve gizlilik ilkesinin korunabilmesi için belirtilen şeffaflık ve hesap verebilirliğin sağlanması yönünde "açık sağlık verisi" kavramını tanımlamaktadır;

"Açık sağlık verisi MADDE 17 – (1) Genel Müdürlük tarafından, Bakanlığın merkez ve taşra teşkilatı ile bağlı ve ilgili kuruluşlarında kullanılan sistemlerde yer alan verilerin, veri mahremiyeti ile veri güvenliğine ilişkin düzenlemeler göz önünde bulundurularak, sağlık sisteminde şeffaflığı ve hesap verilebilirliği temin etmek, sağlık hizmeti sunumuna ilişkin politika ve stratejilere yön vermek, sağlık alanında yapılacak bilimsel araştırmalara destek olmak ve sağlığa ilişkin ürün ve hizmetlerin geliştirilmesini sağlamak amaçlarıyla, bu konuya özel olarak tahsis edilen bir internet sitesi üzerinden herkesin erişimine açılmasına ilişkin usûl ve esaslar Bakanlıkça belirlenir. Veri güvenliğine ilişkin yükümlülükler MADDE 18 – (1) Kanunun 12 nci maddesinde yer alan veri güvenliğine ilişkin yükümlülüklere riayet edilir. Teknik ve idari tedbirlerin alınmasında, Kurum tarafından hazırlanan Kişisel Veri Güvenliği Rehberi esas alınır. (2) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde veri sorumlusu tarafından Kurula yapılacak bildirimde Kanun hükümleri ile Kurulun bu hususa ilişkin düzenleyici işlemleri esas alınır. Yeterli önlemler MADDE 20 – (1) Özel nitelikli kişisel verilerin işlenmesinde ayrıca, Kanunun 6 ncı maddesinin dördüncü fıkrası ile 22 nci maddesinin birinci fıkrasının (ç) bendi uyarınca Kişisel Verileri Koruma Kurulu tarafından yapılan ikincil düzenlemelerde yer alan yeterli önlemlere riayet edilir." Yönetmeliğin 21. maddesi kişisel sağlık verilerinin merkezi sağlık veri sistemine gönderilmesini zorunlu tutmaktadır. "Yaptırım MADDE 21 – (3) Merkezi sağlık veri sistemine Bakanlıkça belirlenen usul ve esaslara

uygun bir şekilde veri gönderimi yapmayan sağlık hizmeti sunucularına, 3359 sayılı Sağlık Hizmetleri Temel Kanununun Ek 11 inci maddesinin üçüncü fıkrasına göre işlem tesis edilir."

Kişisel sağlık verilerinin mahremiyeti ve gizliliğini korumayı amaçlayan bir diğer düzenleme GSS Verilerinin Güvenliği ve Paylaşımına İlişkin Yön.'in 5. ve 10. maddeleridir (Genel Sağlık Sigortası Verilerinin Güvenliği Ve Paylaşımına İlişkin Yönetmelik, 2012).

"Sağlık Verilerinin Güvenliği, Kişisel ve ticari sır niteliğindeki verilerin korunması MADDE 5 – (1) Genel sağlık sigortalısına ait sağlık bilgilerinin gizliliği esastır. Sağlık verilerinin paylaşımında; Anayasada, kanunlarda ve uluslararası sözleşmelerde yer alan özel hayatın gizliliğine ve ticari sır niteliğindeki verilerin korunmasına ilişkin hükümler esas alınır. Kurum veri tabanında yer alan bilgilerin güvenliğinin sağlanması MADDE 6 – (1) Kurum, veri tabanında tutulan sağlık verilerinin her türlü tehlikeye karşı güvenliğinin sağlanması amacıyla, güvenlik politikalarının hazırlanmasını, uygulamaya konulmasını, güncellenmesini ve denetlenmesini sağlamakla yükümlüdür. (2) Kurumda yazılım geliştirme üzerine çalışan personel, verilecek özel izin dışında veri tabanına erişemez. (3) Veri talebinde bulunan kamu kurum ve kuruluşları, özel sektör kuruluşları ve gerçek ve tüzel kişilerin kurum veri tabanının tamamına doğrudan erişimine izin verilmez. Talep edilen verinin aktarımı sağlanır. Paylaşılmayacak veriler MADDE 10 – (1) Genel sağlık sigortalısına ve sağlık hizmet sunucularına ait verilerin gizliliği esastır. Bu verilerin paylaşımında uluslararası sözleşmeler, Anayasa, kanunlar ve diğer mevzuatta yer alan özel hayatın gizliliğine ve ticari sır niteliğindeki verilerin korunmasına ilişkin hükümler esas alınır. (2) Aşağıda yer alan bilgiler paylaşılmaz: a) Paylaşılması ulusal güvenliği tehdit edebilecek nitelikte olan bilgiler, b) Milli İstihbarat Teşkilatı Müsteşarlığı personeli ile bakmakla yükümlü oldukları kişilere ait her türlü veriler, c) Genel sağlık sigortalısına ait kişisel bilgileri içeren veriler, ç) Rekabet hukuku ilkelerine aykırılık teşkil eden firma, ürün, marka ve ilgili diğer bilgileri içeren veriler. (3) Sağlık hizmet sunucularına ait veriler, ancak kurum adı belirtilmeden, doğrudan veya dolaylı tanımlamaya yol açmayacak şekilde bölge veya alan adı olarak verilebilir."

Kişisel sağlık verilerinin mahremiyeti ve gizliliğini konu edinen bir diğer önemli düzenleme KVK Kurumu'nun yayınladığı Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'tir. Yönetmeliğin 8. maddesi, verilerin silinmesi, 9. maddesi, verilerin yok edilmesi ve 10. maddesi verilerin anonim

hale getirilmesini düzenlemektedir (Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, 2017);

> "Kişisel verilerin silinmesi MADDE 8 – (1)Kişisel verilerin silinmesi, kişisel verilerin ilgili kullanıcılar için hiçbir şekilde erişilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. (2) Veri sorumlusu, silinen kişisel verilerin ilgili kullanıcılar için erişilemez ve tekrar kullanılamaz olması için gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür. Kişisel verilerin yok edilmesi MADDE 9 – (1) Kişisel verilerin yok edilmesi, kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir. (2) Veri sorumlusu, kişisel verilerin yok edilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür. Kişisel verilerin anonim hale getirilmesi MADDE 10 – (1) Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. (2) Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir. (3) Veri sorumlusu, kişisel verilerin anonim hale getirilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür."

Bu üç madde, hem özerklik ilkesi hem de mahremiyet ve gizlilik ilkesi açısından öne çıkmaktadır.

Mahremiyet ve gizliliğin korunmasıyla ilgili Hasta Hakları Yönetmeliği'nin 5. maddesinin f bendinde "Kanun ile müsaade edilen haller ile tıbbi zorunluluklar dışında, hastanın özel hayatının ve aile hayatının gizliliğine dokunulamaz." ibaresi bulunmaktadır. Yönetmeliğin 21. maddesi hastanın mahremiyetine saygı gösterilmesi hakkını tanımlarken, 23. maddesi hasta mahremiyetine vurgu yapmaktadır (Hasta Hakları Yönetmeliği, 1998).

> "Mahremiyete Saygı Gösterilmesi Madde 21- 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. Eğitim verilen sağlık kurum ve kuruluşlarında, hastanın tedavisi ile doğrudan ilgili olmayanların tıbbi müdahale sırasında bulunması gerekli ise; önceden veya tedavi sırasında bunun için hastanın ayrıca rızası alınır." Yönetmeliğin 23. maddesi gizliliğe vurgu yapmaktadır. Buna göre; "Bilgilerin Gizli Tutulması Madde 23- Sağlık hizmetinin verilmesi sebebiyle edinilen bilgiler, kanun ile müsaade edilen haller dışında, hiçbir şekilde açıklanamaz. Kişinin rızasına dayansa bile, kişilik haklarından bütünüyle vazgeçilmesi, bu hakların başkalarına devri veya aşırı şekilde sınırlanması neticesini doğuran hallerde bilginin açıklanması, bunları açıklayanın hukuki sorumluluğunu kaldırmaz. Hukuki ve ahlaki yönden geçerli ve haklı bir sebebe dayanmaksızın hastaya zarar verme ihtimali bulunan bilginin ifşa edilmesi, personelin ve diğer kimselerin hukuki ve cezai sorumluluğunu da gerektirir. Araştırma ve eğitim amacı ile yapılan faaliyetlerde de hastanın kimlik bilgileri, rızası olmaksızın açıklanamaz."

Kişisel sağlık verilerinin korunmasında maddeleri bakımından ilgili bir diğer düzenleme Tıbbi Deontoloji Nizamnamesidir. Nizamnamenin 4. ve 31. maddelerinde, hasta-hekim ilişkisi bağlamında hasta mahremiyeti ele alınmaktadır (Tıbbi Deontoloji Nizamnamesi, 1960);

> "Madde 4 – Tabip ve diş tabibi, meslek ve sanatının icrası vesilesiyle muttali olduğu sırları, kanuni mecburiyet olmadıkça, ifşa edemez. Tıbbi toplantılarda takdim edilen veya yayınlarda bahis konusu olan vakalarda, hastanın hüviyeti açıklanamaz.
>
> Hastayla İlgili Bilgilerin Hastaya Verilmesi ve Kullanımı Madde 31 - Hasta dosyalarındaki bilgilerin geniş bir özeti ile bilgi ve belgelerin örnekleri, isteği durumunda hastaya verilir. Hekim, yasal zorunluluk olmadıkça, bu bilgileri başkasına veremez. Hekim, hastanın kimlik bilgilerini saklı tutmak koşuluyla, bu bilgileri dosya üzerinden yapacağı araştırmalarda kullanabilir."

Bu madde, hekimin hastasının kimlik bilgilerini gizli tutması koşuluyla hastanın sağlık verilerini araştırmalarda kullanabileceğini belirtmektedir. Nizamname'nin 35. maddesi dezavantajlı gruplar olarak tutuklu ve hükümlülerin mahremiyetlerinin korunması hakkını düzenlemektedir;

> "Tutuklu ve Hükümlülere Verilecek Tıbbi Yardım Madde 35 - Tutuklu ve hükümlülerin muayenesi de öteki hastalarınki gibi, kişilik haklarına saygılı, hekimlik sanatını uygulamaya elverişli koşullarda yapılır ve onların gizlilik hakları korunur. Hekimin, bu koşulların sağlanması için ilgililerden istekte bulunma hakkı ve sorumluluğu vardır. Muayene sonucu düzenlenecek belge veya raporlarda hekimin adı, soyadı, diploma numarası ve imzası mutlaka bulunur. Belge ve raporun bir örneği kişiye verilir. Belge ve rapor baskı altında yazılmış ise, hekim bu durumu en kısa zamanda meslek örgütüne bildirir."

Bir diğer dezavantajlı grup olarak deneklerin mahremiyetinin korunması 43. madde ile ifade edilmektedir;

> "Deneğin Korunması Madde 43 - İnsan üzerinde yapılan tıbbi araştırmalarda… Deneğin özel yaşamına saygı gösterilmesi ve kişisel bilgilerin gizliliği sağlanır. Bilimsel araştırma ve yayınlar ile akademik-bilimsel amaçlı sunuşlarda deneğin kimliği gizli tutulur."

Hekimin meslek ahlakı kurallarını düzenleyen HMEK'te mahremiyet ve gizlilik, hekimin sır saklama yükümlülüğü başlığı altında 9. madde ile korunmaktadır. Bu maddeye göre hekim ile hastası arasındaki her türlü bilgi sır kapsamında kabul edilmektedir (TTB, 2012);

> "Sır Saklama Yükümlülüğü Madde 9 - Hekim, hastasından mesleğini uygularken öğrendiği sırları açıklayamaz. Hastanın ölmesi ya da o hekimle ilişkisinin sona ermesi, hekimin bu yükümlülüğünü ortadan kaldırmaz. Hastanın onam vermesi ya da sırrın saklanmasının hasta ya da öteki insanların yaşamını tehlikeye sokması durumunda, hastanın kişilik haklarının zedelenmemesi koşuluyla, hekim bu sırrı saklamakla yükümlü değildir. Yasal zorunluluk durumlarında hekimin rapor düzenlemesi de, meslek sırrının açıklanması anlamına gelmez. Hekim, tanık ya da bilirkişi olarak mahkemeye çağrıldığında olayın meslek sırrı olduğunu ileri sürerek bu görevlerinden çekilebilir."

Kan ve Kan Ürünleri Kanunu'nun 3. maddesi, kan, kan bileşenleri ve ürünleriyle ilgili bilgilerin kaydedilmesi ve saklanması sürecini düzenlemektedir. Buna göre kaydedilen bilgilerin otuz yıl süreyle saklanması gerekmektedir (Kan ve Kan Ürünleri Kanunu, 2007);

> "MADDE 3 – (1) c) Kan, kan bileşenleri ve ürünlerinin alınmasında ve verilmesinde bağışçı ve alıcının sağlığının tehlikeye düşürülmemesi, tıbbî risklere karşı korunması, transfüzyonun güvenle yapılması ve transfüzyon

sonrası bağışçı ve alıcının izlenmesi şarttır. Alıcı ve vericide ortaya çıkabilecek komplikasyonların bildirilmesi zorunludur. Kan, kan bileşenleri ve ürünlerinin alınması, kaydı, analizi, işlenmesi, depolanması, kullanılır hale getirilmesi, dağıtım ve kullanımını ilgilendiren kan bağışı, kan bağışçısı, hazırlayan kuruluş, kullanım yeri ve alıcı ile ilgili bütün verilerin yazılı veya elektronik ortamda kaydedilmesi ve otuz yıl süreyle saklanması zorunludur. Kan istek formu ve bağışçı sorgulama formlarının asılları ile kan bağışçısından alınan kan örneklerinin şahit numuneleri bir yıldan az olmamak üzere Bakanlıkça belirlenecek süreyle saklanır."

Özel Hastaneler Yönetmeliği'nin 49. ve 50. maddeleri tıbbi kayıtlarla ilgilidir. Buna göre yönetmeliğe eklenen maddeler ile özel hastanede tutulan hasta dosyalarının yirmi yıl süre ile saklanacağı belirtilmiş, KVK Kanunu'na vurgu yapılmış ve ortak kullanım alanları kamera kayıt sistemlerinin iki ay süre ile saklanacağı değişikliği eklenmiştir. (Özel Hastaneler Yönetmeliği, 2002);

"Tıbbî arşiv ve Bakanlığa yapılacak bildirimler Madde 49– Özel hastanelerde, muayene, teşhis ve tedavi amacıyla başvuran hasta, yaralı, acil ve adlî vakalar ile ilgili olarak yapılan tıbbî ve idarî işlemlere ilişkin kayıtların, düzenlenen ve kullanılan belgelerin toplanması ve bunların müteakip başvurular ile denetim ve adlî mercilerce her istenildiğinde hazır bulundurulması amacıyla tasnif ve muhafazaya uygun bir merkezî tıbbî arşiv kurulması zorunludur. (Ek cümle:RG-22/3/2017- 30015) Merkezi tıbbi arşivin hastane bünyesinde bulunması zorunlu değildir. İlgili diğer mevzuat hükümleri saklı kalmak kaydıyla, özel hastanede tutulan hasta dosyaları, en az yirmi yıl süre ile saklanır. Faaliyeti sona eren özel hastanelerin arşiv belgeleri, bir tutanağa bağlanarak müdürlüğe teslim edilir. (Değişik dördüncü fıkra:RG-31/5/2019-30790) Özel hastaneler tarafından kayıt altına alınan kişisel sağlık verileri, 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ikincil düzenlemelere uygun bir şekilde Bakanlıkça belirlenen usul ve esaslar çerçevesinde merkezi sağlık veri sistemine aktarılır ve işlenir. Bakanlık tarafından kurulan kayıt ve bildirim sistemine ve Bakanlıkça yapılacak diğer iş ve işlemlere esas olmak üzere, istenilen bilgi ve belgelerin Bakanlığa gönderilmesi zorunludur. (Ek fıkra:RG-23/9/2010-27708) Özel hastaneler, kliniklerinde takip ettikleri gebeler, yenidoğan ve bebeklerin izlenmesi ve kontrolü için Bakanlıkça istenilen kayıt ve bildirimleri istenilen formatta ve sürelerde Bakanlıkça belirlenen birime bildirir. (Ek fıkra:RG-23/9/2010-27708) (Değişik:RG-1/7/2014-29047)Hasta mahremiyeti dikkate alınmak kaydıyla, ortak kullanım alanları kamera kayıt sistemi ile kayıt altına alınır ve kamera görüntüleri en az iki ay süre ile saklanır."

Yönetmeliğin 50. maddesinde olası suiistimallere karşı gerekli idari ve teknik tedbirlerin alınmasından mesul müdür sorumlu tutulmuştur. Maddeye eklenen son cümle ile elektronik imzalı tıbbi kayıtlar resmi kayıt olarak kabul edilmiştir.

> "Kayıtların bilgisayar ortamında tutulması Madde 50- (Değişik:RG-21/10/2006-26326) Özel hastanelerde, bu Yönetmelikte belirtilmiş her türlü kayıt işlemi, bilgisayar ortamında ve/veya ihtiyaca göre yazılı kayıt sistemi ile tutulabilir... Bu kayıtların bilgisayar ortamında saklanmasının, değiştirilmesinin ve silinmesinin önlenmesi, gizliliğin ihlal edilmemesi amacıyla fizikî, manyetik veya elektronik müdahalelere ve olası suistimallere karşı gerekli idarî ve teknik tedbirlerin alınmasından ve periyodik olarak denetlenmesinden mesul müdür sorumludur. Mevcut yedekleme sisteminden günlük, haftalık, aylık ve yıllık olmak üzere veriler yedeklenir. Adli vakalara ve adli raporlara ait kayıtların gizliliği ve güvenliği açısından vakayı takip eden tabip dışında vaka hakkında veri girişi yapılamaması ya da adli raporu tanzim eden tabibin onayından sonra kendisi dahil hiç kimsenin rapor ile ilgili değişiklik yapamaması için gerekli düzenlemeler yapılır. Adli vaka kayıtlarına mesul müdür veya yetkilendirdiği kişiler erişebilir. Ancak, yetkililerin rapor üzerinde hiçbir şekilde değişiklik yapmasına izin verilmez. …Bu raporlar ile ilgili sorumluluk mesul müdüre ve hastane sahibine aittir. Güvenli dijital hasta kaydına geçilmeyen hastanelerde bilgisayar ortamında kayıt tutulması, yazılı kayıt sisteminin gereklerini ortadan kaldırmaz. (Ek cümle:RG-27/5/2012-28305)15/1/2004 tarihli ve 5070 sayılı Elektronik İmza Kanunu hükümlerine uygun elektronik imza ile imzalanmış tıbbi kayıtlar, resmi kayıt olarak kabul edilir ve ilgili mevzuata göre yedekleme ve arşivlemesi yapılır."

Birinci basamak sağlık hizmetlerindeki kişisel sağlık kayıtlarıyla ilgili bir diğer düzenleme Aile Hekimliği Uygulama Yönetmeliği'dir. Bu yönetmeliğin 30, 31. ve 32. maddeleri sağlık kayıtları ile ilgilidir (Aile Hekimliği Uygulama Yönetmeliği, 2013);

> "Tutulacak kayıtlar MADDE 30 – (1) Aile hekimlerinin kullandığı basılı veya elektronik ortamda tutulan kayıtlar**,** kişilerin sağlık dosyaları ile raporlar, sevk belgesi ve reçete gibi belgeler resmî kayıt ve evrak niteliğindedir. (2) Kayıtlı kişi sayısı, yapılan hizmetlerin listesi, muayene edilen ve sevk edilen hasta sayısı, kodları ile birlikte konulan teşhisler, reçete içeriği, aşılama, gebe ve lohusa izlemi, bebek ve çocuk izlemi, üreme sağlığı ve bulaşıcı hastalıklar ile ilgili veriler ve Kurum tarafından belirlenen benzeri veriler evrak kayıt kriterlerine göre belirli aralıklarla düzenli olarak basılı veya elektronik ortamda Kuruma bildirilir."

Yönetmeliğin 31. maddesi sağlık kayıtlarının tutulması ve muhafaza edilmesini düzenlemektedir. Buna göre kişisel sağlık verilerini tutmakla yükümlü olan aile hekimi, kişisel sağlık verilerinin gizliliği, bütünlüğü, güvenliği ve mahremiyetini sağlamakla görevlendirilmektedir.

> "Kayıtların tutulma şekli ve muhafazası MADDE 31 – (1) Aile hekimi kendisine kayıtlı kişilerin kişisel sağlık dosyalarını tutmakla yükümlüdür. Kayıtların güvenliği ve mahremiyeti aile hekiminin sorumluluğundadır. (2) Denetim sırasında talep edilmesi halinde, aile hekimi hasta haklarına riayet etmek suretiyle kendisine kayıtlı kişilerin dosyalarını göstermek zorundadır. (3) Kişi, kendisi ile ilgili tutulan kayıtların bir nüshasını aile hekiminden talep edebilir. (4) Aile hekimlerinin, lisans hakları Bakanlığa ait olan veya Bakanlıkça belirlenip ilan edilen, standartlara haiz bir aile hekimliği bilgi sistemi yazılımı kullanmaları şarttır. (5) Aile hekimleri, bakmakla yükümlü olduğu vatandaşlara ait bilgi sisteminde tuttuğu tüm verilerin ilgili mevzuatı çerçevesinde gizliliğini, bütünlüğünü, güvenliğini ve mahremiyetini sağlamakla yükümlüdür. (6) Herhangi bir vatandaşa ait kişisel veriler ile kişisel sağlık verileri, müdürlük ya da Bakanlık ve Kurum haricindeki herhangi bir kayıt ortamında (bilgisayar, hard disk, cd, dvd, yazılı doküman gibi) yüklenici firma tarafından kaydedilemez. Bu durumun tespiti halinde bu yazılımın kullanımı iptal edilir."

Yönetmeliğin 32. maddesi ise kayıtların devri ile ilgilidir. Buna göre kurumdan ayrılacak aile hekimi, tuttuğu kayıtları yeni aile hekimine devretmelidir.

> "Kayıtların devri MADDE 32 – (1) Bulunduğu bölgeden ayrılacak olan aile hekimi kendisine kayıtlı kişilerin verilerini sorumlu olacak aile hekimine devreder. Devir teslimin yapılamadığı durumlarda ayrılacak olan aile hekimi bu verileri bölgesindeki toplum sağlığı merkezine teslim eder. Ayrılan aile hekiminin hiçbir şekilde verileri devredemediği hallerde toplum sağlığı merkezi gerekli verileri temin ederek sorumlu olacak aile hekimine verir ve devir teslimi yapmayan aile hekimi ile ilgili tutanak tutarak müdürlüğe bildirir."

Bilgi Edinme Hakkı Kanunu'nun 21. maddesinde bilgi edinmenin sınırları belirtilmiş ve özel hayatın gizliliği kapsamında mahremiyet ve gizlilik ilkesi ele alınmıştır (Bilgi Edinme Hakkı Kanunu, 2003);

> "Bilgi Edinme Hakkının Sınırları Özel hayatın gizliliği Madde 21- Kişinin izin verdiği hâller saklı kalmak üzere, özel hayatın gizliliği kapsamında, açıklanması hâlinde kişinin sağlık bilgileri ile özel ve aile hayatına, şeref ve

> haysiyetine, meslekî ve ekonomik değerlerine haksız müdahale oluşturacak bilgi veya belgeler, bilgi edinme hakkı kapsamı dışındadır. Kamu yararının gerektirdiği hâllerde, kişisel bilgi veya belgeler, kurum ve kuruluşlar tarafından, ilgili kişiye en az yedi gün önceden haber verilerek yazılı rızası alınmak koşuluyla açıklanabilir."

Kişisel verilerin mahremiyet ve gizliliğinin korunmasıyla ilgili olarak 663 sayılı KHK'nın 47. maddesi kişisel sağlık verilerinin toplanması, işlenmesi ve paylaşılması ile ilgilidir. Buna göre kişisel sağlık verilerinin toplanması, işlenmesi ve paylaşılması yetkisi ilgili Bakanlık ve bağlı kuruluşlara aittir (Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname, 2011);

> "Bilgi toplama, işleme ve paylaşma yetkisi MADDE 47- (1) Bakanlık ve bağlı kuruluşları, mevzuatla kendilerine verilen görevleri, e-devlet uygulamalarına uygun olarak daha etkin ve hızlı biçimde yerine getirebilmek için, bütün kamu ve özel sağlık kurum ve kuruluşlarından; sağlık hizmeti alanların, aldıkları sağlık hizmetinin gereği olarak ilgili sağlık kurum ve kuruluşuna vermek zorunda oldukları kişisel bilgileri ve bu kimselere verilen hizmete ilişkin bilgileri her türlü vasıtayla toplamaya, işlemeye ve paylaşmaya yetkilidir. (2) Bakanlık ve bağlı kuruluşları işlediği kişisel sağlık verilerini ilgili üçüncü kişiler ve kamu kurum ve kuruluşları ile ancak bu kişi ve kurumların bu verilere erişebileceği hususunda kanunen yetkili olması halinde ve görevlerini yapmalarına yetecek derecede paylaşabilir. (3) Bakanlık ve bağlı kuruluşları, mevzuatla kendilerine verilen görevleri yerine getirebilmek için gereken bilgileri, kamu ve özel ilgili bütün kişi ve kuruluşlardan istemeye yetkilidir. İlgili kişi ve kuruluşlar istenilen bilgileri vermekle yükümlüdür…"

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 9. maddesi özel hayatın gizliliğini ihlal edebilecek internet ortamındaki içeriklere erişimi düzenlemektedir. Buna göre özel hayatın gizliliğini ihlal edebilecek içeriğe erişimin engellenebilmesi için ilgili kişinin Kuruma doğrudan başvurarak engelleme tedbirinin uygulanmasını talep etmesi gerekmektedir (İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, 2007);

> "Özel hayatın gizliliği nedeniyle içeriğe erişimin engellenmesi MADDE 9/A- (Ek: 6/2/2014-6518/94 md.) (1) İnternet ortamında yapılan yayın içeriği nedeniyle özel hayatının gizliliğinin ihlal edildiğini iddia eden kişiler, Kuruma doğrudan başvurarak içeriğe erişimin engellenmesi tedbirinin uygulanmasını isteyebilir. (2) Yapılan bu istekte; hakkın ihlaline neden olan yayının tam adresi

(URL), hangi açılardan hakkın ihlal edildiğine ilişkin açıklama ve kimlik bilgilerini ispatlayacak bilgilere yer verilir. Bu bilgilerde eksiklik olması hâlinde talep işleme konulmaz. (3) Başkan, kendisine gelen bu talebi uygulanmak üzere derhâl Birliğe bildirir, erişim sağlayıcılar bu tedbir talebini derhâl, en geç dört saat içinde yerine getirir. (4) Erişimin engellenmesi, özel hayatın gizliliğini ihlal eden yayın, kısım, bölüm, resim, video ile ilgili olarak (URL şeklinde) içeriğe erişimin engellenmesi yoluyla uygulanır. (5) Erişimin engellenmesini talep eden kişiler, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edildiğinden bahisle erişimin engellenmesi talebini talepte bulunduğu saatten itibaren yirmi dört saat içinde sulh ceza hâkiminin kararına sunar. Hâkim, internet ortamında yapılan yayın içeriği nedeniyle özel hayatın gizliliğinin ihlal edilip edilmediğini değerlendirerek vereceği kararını en geç kırk sekiz saat içinde açıklar ve doğrudan Kuruma gönderir; aksi hâlde, erişimin engellenmesi tedbiri kendiliğinden kalkar. (6) Hâkim tarafından verilen bu karara karşı Başkan tarafından 5271 sayılı Kanun hükümlerine göre itiraz yoluna gidilebilir. (7) Erişimin engellenmesine konu içeriğin yayından çıkarılmış olması durumunda hâkim kararı kendiliğinden hükümsüz kalır. (8) Özel hayatın gizliliğinin ihlaline bağlı olarak gecikmesinde sakınca bulunan hâllerde doğrudan Başkanın emri üzerine erişimin engellenmesi Kurum tarafından yapılır. (Mülga cümle: 26/2/2014-6527/18 md.) (9) (Ek: 26/2/2014-6527/18 md.) Bu maddenin sekizinci fıkrası kapsamında Başkan tarafından verilen erişimin engellenmesi kararı, (…) yirmi dört saat içinde sulh ceza hâkiminin onayına sunulur. Hâkim, kararını kırk sekiz saat içinde açıklar."

Türk Borçlar Kanunu'nun 419. maddesi, işverenin işçiye ait kişisel bilgilerini kullanma konusunda sınırlama getirmektedir. Buna göre; "Kişisel verilerin kullanılmasında MADDE 419- İşveren, işçiye ait kişisel verileri, ancak işçinin işe yatkınlığıyla ilgili veya hizmet sözleşmesinin ifası için zorunlu olduğu ölçüde kullanabilir. Özel kanun hükümleri saklıdır." (Türk Borçlar Kanunu, 2011).

İşçilerin kişisel verilerinin korunması konusunda İş Kanunu'nun 75. maddesi bulunmaktadır. Buna göre her işçi için tutulan özlük bilgileri, kişisel veri niteliğindedir. Bu verilerin mahremiyet ve gizliliğinin korunmasında işveren sorumludur (İş Kanunu, 2003);

"İşçi özlük dosyası Madde 75 - İşveren çalıştırdığı her işçi için bir özlük dosyası düzenler. İşveren bu dosyada, işçinin kimlik bilgilerinin yanında, bu Kanun ve diğer kanunlar uyarınca düzenlemek zorunda olduğu her türlü belge ve kayıtları saklamak ve bunları istendiği zaman yetkili memur ve mercilere

göstermek zorundadır. İşveren, işçi hakkında edindiği bilgileri dürüstlük kuralları ve hukuka uygun olarak kullanmak ve gizli kalmasında işçinin haklı çıkarı bulunan bilgileri açıklamamakla yükümlüdür."

Ceza Muhakemesi Kanunu'nun 80. maddesi, genetik verilerin gizliliğini düzenlemektedir (Ceza Muhakemesi Kanunu, 2004);

> "Genetik inceleme sonuçlarının gizliliği Madde 80 – (Değişik: 25/5/2005 – 5353/4 md.) (1) 75, 76 ve 78 inci madde hükümlerine göre alınan örnekler üzerinde yapılan inceleme sonuçları, kişisel veri niteliğinde olup, başka bir amaçla kullanılamaz; dosya içeriğini öğrenme yetkisine sahip bulunan kişiler tarafından bir başkasına verilemez. (2) Bu bilgiler, kovuşturmaya yer olmadığı kararına itiraz süresinin dolması, itirazın reddi, beraat veya ceza verilmesine yer olmadığı kararı verilip kesinleşmesi hâllerinde Cumhuriyet savcısının huzurunda derhâl yok edilir ve bu husus dosyasında muhafaza edilmek üzere tutanağa geçirilir"

Bu maddeye göre genetik verilerin gizlilik ve mahremiyeti, "özel veri niteliğinde olma" gerekçesi ile hassas bir koruma düzeyine sahiptir.

GSS Verilerinin Güvenliği ve Paylaşımına İlişkin Yönetmelik'in 6. maddesi, kurum veri tabanında tutulan sağlık verilerinin güvenliğinin nasıl sağlanacağı ile ilgili kurumun yükümlülüklerini bildirmektedir (2012);

> "Kurum veri tabanında yer alan bilgilerin güvenliğinin sağlanması MADDE 6 – (1) Kurum, veri tabanında tutulan sağlık verilerinin her türlü tehlikeye karşı güvenliğinin sağlanması amacıyla, güvenlik politikalarının hazırlanmasını, uygulamaya konulmasını, güncellenmesini ve denetlenmesini sağlamakla yükümlüdür. (2) Kurumda yazılım geliştirme üzerine çalışan personel, verilecek özel izin dışında veri tabanına erişemez. (3) Veri talebinde bulunan kamu kurum ve kuruluşları, özel sektör kuruluşları ve gerçek ve tüzel kişilerin kurum veri tabanının tamamına doğrudan erişimine izin verilmez. Talep edilen verinin aktarımı sağlanır."

Bu maddeye göre Kurum, veri güvenliğinin sağlanması amacıyla güvenlik politikalarının hazırlanmasını, uygulamaya koyulmasını, güncellemesini ve denetlenmesini sağlamakla yükümlü tutulmaktadır. Yönetmeliğin 7. maddesi, sağlık hizmet sunucularında kaydı tutulan kişisel verilerin güvenliğinin nasıl sağlanacağı ile ilgilidir (Genel Sağlık Sigortası Verilerinin Güvenliği ve Paylaşımına İlişkin Yönetmelik, 2012);

> "Sağlık hizmet sunucularında kaydı tutulan verilerin güvenliğinin sağlanması MADDE 7 – (1) Sağlık hizmet sunucularının genel sağlık sigortalısına sunmuş olduğu sağlık hizmetlerine ilişkin kaydı tutulan sağlık verileri dahil her türlü kişisel bilgiler, ilgili mevzuatla izin verilen haller dışında veya kişilerin açıkça rızası olmaksızın, kurum, kuruluş ve üçüncü kişilerle paylaşılmaz. Kişiyi doğrudan veya dolaylı olarak tanımlamayan genel veya anonim veriler paylaşılabilir. (2) Sağlık hizmet sunucularına ait bilgi işlem sistemlerinin yazılım ve donanımını sağlayan gerçek ve tüzel kişiler de yukarıda belirtilen hükümlere tabidir"

Bu maddeye göre kişisel bilgilerin kanunla izin verilen haller ve kişinin açık rızası dışında paylaşılması yasaktır. Ancak anonim hale getirilen veriler paylaşılabilir. Yönetmeliğin 8. maddesi ise veri üreten birimin sorumluluğunu düzenlemektedir.

> "Veri üreten birimin sorumluluğu MADDE 8 – (1) Veri üretimi, kurum veri tabanında yetkilendirilmiş kişiler tarafından yapılır. Veri üreten kişiler kurumca belirlenecek olan yöntemlere göre farklı düzeylerde yetkilendirilebilir. Üretilen veriler sadece veri talebinde bulunan özel sektör veya kamu kurumunun ilgili birimine iletilir. Üretilen verilerin muhafazası ve güvenliği veri üreten ve talep eden birimler tarafından sağlanır. (2) Kurum, paylaşılan verilerin içeriğini kayıt altına almak ve muhafaza etmekten sorumludur."

Yönetmeliğin 9. maddesi, veri alıcısının veri güvenliğini nasıl sağlayacağı ve görevlerini düzenlemektedir.

> "Alıcının sorumluluğu MADDE 9 – (1) Alıcı, kurumdan aldığı verilerin gizliliğini korumakla ve güvenliğini sağlamakla yükümlüdür. Alınan veriler talebe esas gerekçe dışında hiçbir amaçla kullanılamaz. Alıcı tarafın verileri teslim alabilmesi için noter aracılığı ile "Gizlilik Taahhüt Belgesi" imzalaması ve Kuruma vermesi zorunludur. (2) Alıcı, Kurumdan alınan verileri mevzuata aykırı kullanması veya güvenliğini sağlayamaması durumunda doğacak hukuki sonuçlardan sorumludur. Alıcı, verilerin yetkisi olmayan kurum, kuruluş ve üçüncü kişilerin eline geçmemesi için gerekli tüm tedbirleri almakla yükümlüdür."

Bu maddeye göre veri alıcısının veriyi alabilmesi için noter aracılığı ile 'Gizlilik Taahhüt Belgesi' imzalaması zorunludur. Yönetmeliğin 14. maddesi, sözleşme kapsamındaki veri taleplerinin nasıl karşılanacağını düzenlemektedir. İlgili madde; "Sözleşme kapsamındaki veri taleplerinin karşılanması MADDE 14 – (3) Veriler, CD, DVD, sabit disk, taşınabilir bellek gibi elektronik veya manyetik kayıt ortamında

şifrelenerek alıcıya gönderilir. (4) Veri paylaşımı kapsamında edinilen bilgilerin her türlü kullanımında alıcının Kurumu kaynak göstermesi zorunludur." biçimindedir (2012). Bu maddeye göre, verilerin alıcıya şifrelenerek gönderilebileceği ve alıcının verilerin kullanımında Kurumu kaynak göstermesi zorunluluğu bulunmaktadır.

Kişisel verilerin gizlilik ve mahremiyeti, ceza hukuku açısından Türk Ceza Kanunu'nda düzenlenmiştir. Buna göre 134. madde, özel hayatın gizliliğinin ihlaline yönelik suçları; 135. madde kişisel verilerin hukuka aykırı şekilde kaydedilmesi suçlarını; 136. madde, kişisel verileri hukuka aykırı bir şekilde ele geçirme ve yayma suçlarını; 138. madde kişisel verinin yok edilmeme suçunu; 243. madde bilişim sistemine girme suçunu ve 244. madde bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme suçlarını düzenlemektedir. Kanunun 137. maddesi bu suçların nitelikli hallerini tanımlamaktadır. İlgili maddeler şu şekildedir (Türk Ceza Kanunu, 2004);

> "Özel hayatın gizliliğini ihlal[2] Madde 134- (1) Kişilerin özel hayatının gizliliğini ihlal eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlal edilmesi halinde, verilecek ceza bir kat artırılır. (2) (Değişik: 2/7/2012-6352/81 md.) Kişilerin özel hayatına ilişkin görüntü veya sesleri hukuka aykırı olarak ifşa eden kimse iki yıldan beş yıla kadar hapis cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur. Kişisel verilerin kaydedilmesi Madde 135- (1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye bir yıldan üç yıla kadar hapis cezası verilir.[3] (2) Kişisel verinin, kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır.[4] Verileri hukuka aykırı olarak verme veya ele geçirme Madde 136- (1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, iki yıldan dört

[2] 2/7/2012 tarihli ve 6352 sayılı Kanunun 81 inci maddesiyle, bu maddenin birinci fıkrasında yer alan "altı aydan iki yıla kadar hapis veya adlî para" ibaresi "bir yıldan üç yıla kadar hapis" ve "cezanın alt sınırı bir yıldan az olamaz" ibaresi ise "verilecek ceza bir kat artırılır" şeklinde değiştirilmiştir.
[3] 21/2/2014 tarihli ve 6526 sayılı kanunun 3 üncü maddesiyle bu fıkrada yer alan "altı aydan" ibaresi "bir yıldan" şeklinde değiştirilmiştir.
[4] 24/3/2016 tarihli ve 6698 sayılı Kanunun 30 uncu maddesiyle, bu fıkrada yer alan "Kişilerin" ibaresi "Kişisel verinin, kişilerin" şeklinde; "bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır" ibaresi "olması durumunda birinci fıkra uyarınca verilecek ceza yarı oranında artırılır" şeklinde değiştirilmiştir.

yıla kadar hapis cezası ile cezalandırılır.[5] (2) (Ek:17/10/2019-7188/17 md.) Suçun konusunun, Ceza Muhakemesi Kanununun 236 ncı maddesinin beşinci ve altıncı fıkraları uyarınca kayda alınan beyan ve görüntüler olması durumunda verilecek ceza bir kat artırılır. Nitelikli haller Madde 137- (1) Yukarıdaki maddelerde tanımlanan suçların; a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle, b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, İşlenmesi halinde, verilecek ceza yarı oranında artırılır. Verileri yok etmeme Madde 138- (1) Kanunların belirlediği sürelerin geçmiş olmasına karşın verileri sistem içinde yok etmekle yükümlü olanlara görevlerini yerine getirmediklerinde bir yıldan iki yıla kadar hapis cezası verilir.[6] (2) (Ek: 21/2/2014-6526/5 md.) Suçun konusunun Ceza Muhakemesi Kanunu hükümlerine göre ortadan kaldırılması veya yok edilmesi gereken veri olması hâlinde verilecek ceza bir kat artırılır. Bilişim sistemine girme Madde 243- (1) Bir bilişim sisteminin bütününe veya bir kısmına, hukuka aykırı olarak giren veya orada kalmaya devam eden kimseye bir yıla kadar hapis veya adlî para cezası verilir.[7] (2) Yukarıdaki fıkrada tanımlanan fiillerin bedeli karşılığı yararlanılabilen sistemler hakkında işlenmesi halinde, verilecek ceza yarı oranına kadar indirilir. (3) Bu fiil nedeniyle sistemin içerdiği veriler yok olur veya değişirse, altı aydan iki yıla kadar hapis cezasına hükmolunur. (4) (Ek: 24/3/2016-6698/30 md.) Bir bilişim sisteminin kendi içinde veya bilişim sistemleri arasında gerçekleşen veri nakillerini, sisteme girmeksizin teknik araçlarla hukuka aykırı olarak izleyen kişi, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Sistemi engelleme, bozma, verileri yok etme veya değiştirme Madde 244- (1) Bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılır. (2) Bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılır. (3) Bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılır. (4) Yukarıdaki fıkralarda tanımlanan fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması halinde, iki yıldan altı yıla kadar hapis ve beşbin güne kadar adlî para cezasına hükmolunur."

[5] 21/2/2014 tarihli ve 6526 sayılı kanunun 4 üncü maddesiyle bu fıkrada yer alan "bir yıldan" ibaresi "iki yıldan" şeklinde değiştirilmiştir.
[6] 21/2/2014 tarihli ve 6526 sayılı kanunun 5 inci maddesiyle bu fıkrada yer alan "altı aydan bir yıla kadar hapis" ibaresi "bir yıldan iki yıla kadar hapis" şeklinde değiştirilmiştir.
[7] 24/3/2016 tarihli ve 6698 sayılı Kanunun 30 uncu maddesiyle, bu fıkrada yer alan "ve" ibaresi "veya" şeklinde değiştirilmiştir

Cezai yaptırım konusunda hekimlerin disiplin cezası alması ve bu cezaları belirleyen Türk Tabipleri Birliği Disiplin Yönetmeliği'nin 5. maddesi, geçici olarak meslekten alıkoyma cezalarını belirlediği suçlar içerisinde kişisel verinin korunması ve mesleki gizliliğe yer vermektedir (Türk Tabipleri Birliği Disiplin Yönetmeliği, 2004);

> "Geçici Olarak Meslekten Alıkoyma Cezası Madde 5 … c) Mesleğin uygulanması sırasında ve meslek sebebiyle öğrenilen hastalara ait sırları yasal zorunluluk dışında açıklamak. i) Bilimsel araştırma verilerini değerlendirirken ve yayına hazırlarken bilimsel gerçekleri yansıtmamak; çalışmaya fiilen katılmamış kişilerin adlarına yayında yer vermek, kaynak göstermeden veya izin almadan başkalarına ait verileri, olguları veya yazılı eserleri kullanmak ve benzeri suretle bilimsel yayınlarda yayın etiğine aykırı davranmak."

Veri güvenliği konusunda hastanelerin veri kayıt sistemleriyle ilgili düzenlemeler incelendiğinde, Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arşiv Hizmetleri Yönergesinde Değişiklik Yapılmasına Dair Yönerge (2007), oldukça geniş bir şekilde veri güvenliği konusunu ele almaktadır. Bu Yönergede, risk seviyelerine göre acil durum yönetimi, bilgi sistemlerinde yedeklemenin nasıl yapılacağı, veri tabanı güvenliğinin nasıl sağlanacağı, şifreleme yöntemleri, sunucu güvenliğinin nasıl sağlanacağı, kimlik doğrulama ve yetkilendirmenin nasıl yapılacağı ve ayrı bir başlık olarak kişisel sağlık kayıtlarının güvenliği ayrıntılı bir şekilde düzenlenmiştir (EK-2)

Veri güvenliği konusunda ayrıca Kişisel Verileri Koruma Kurulu'nun Kişisel Veri Güvenliği Rehberi bulunmaktadır. Bu rehberde iki bölüm halinde idari ve teknik tedbirlere yer verilmektedir. Rehber, bir kişi hakkındaki yasal olarak toplanan verilerin, kayıp, bozulma, yetkisiz imha, kullanım, değiştirme veya ifşaya karşı tüm makul ve uygun önlemlerle korunması, şifreleme ve veri sızıntı önleyici sistemler konusunda teknik yöntemleri açıklamaktadır. Bu rehberin yanı sıra Kurulun çıkarmış olduğu "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" ve "Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Rehberi" veri güvenliğinin etkin bir şekilde korunabilmesi için gerekli önlemleri açıklamaktadır.

Genel olarak bakıldığında mahremiyet ve gizlilik ilkesinin bireylerin korunması, şeffaflık, katılım ve kapsayıcılık ve hesap verebilirlik bileşenleri ile birlikte ilgili düzenlemelerde teorik olarak korunmaya çalışılmaktadır. KVK Kanunu'nun 8 ve 9.

maddeleri, verilerin yurt içi ve yurt dışı aktarımı için kişinin açık rızası alınmadan paylaşılabileceği yönünde istisnalara yer vermektedir. Bu bakımdan mahremiyet ve gizlilik ilkesinin üçüncü taraflarla paylaşılmaması gerektiği koşulunu taşımamaktadır.

4.2.Veri Kayıt Sistemlerinin Genel Özellikleri

İlkelere göre E-Nabız, AHBS, MİA MED ve mobil sağlık uygulamaları olarak Hayat Eve Sığar (HES) ve Korona Önlem uygulaması analiz edilmiştir. Bu uygulamaların genel özellikleri Tablo 4'te gösterilmiştir.

Basamaklı tedavi hizmetleri açısından e-Nabız uygulaması, birinci, ikinci ve üçüncü basamak sağlık hizmetlerinin tamamını kapsamaktadır. Herhangi bir sağlık kuruluşunda sağlık kaydı oluşturulan hastanın bütün sonuçları kişinin e-Nabız kaydına tanımlanmaktadır. Hızır AHBS, birinci basamak tedavi merkezlerinde kullanılan bir veri tabanıdır. MİA MED veri tabanı yataklı tedavi merkezleri kapsamında incelenmiştir.

Tablo 4. Veri kayıt sistemlerinin özellikleri

Veri tabanları	Çıkış tarihi	Hizmet basamağı	Hedef kullanıcı	Uygulama türü
E-Nabız	2015	Genel	Herkes	Mobil + İnternet
Hızır AHBS	2005	Birinci basamak	Sağlık çalışanları	İntraNet+İnternet
MİA MED	2010	Üçüncü basamak	Sağlık çalışanları	İntraNet+İnternet
Hayat Eve Sığar	2020	Genel	Herkes	Mobil
Korona Önlem	2020	Genel	Herkes	Mobil

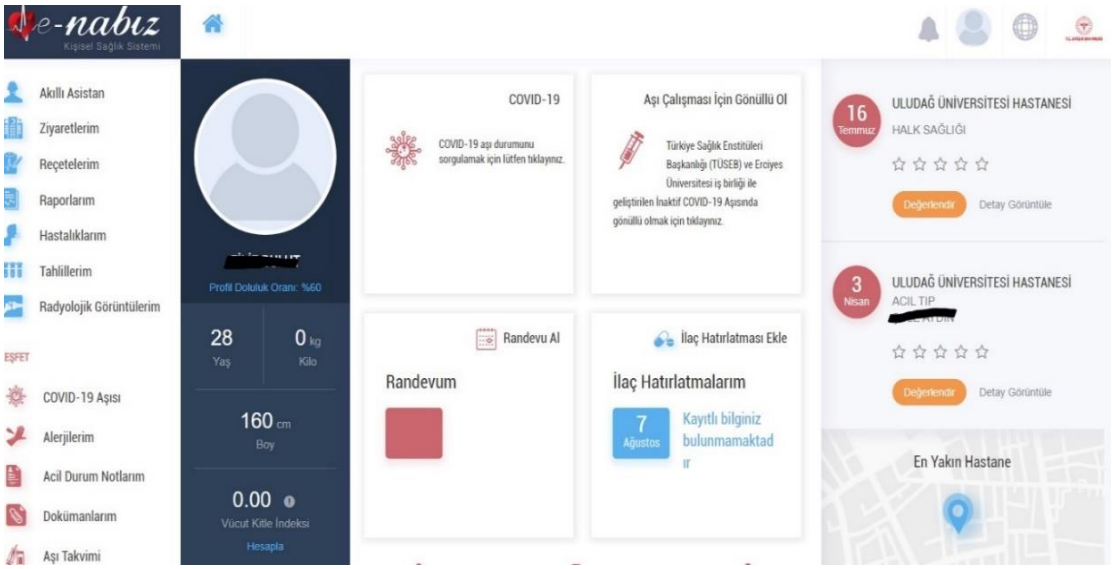
HES ve Korona Önlem Uygulaması Covid-19 pandemisi ile mücadele kapsamında çıkarılmış mobil uygulamalardır ve olağandışı durumlarda işlenen kişisel veriler açısından incelenmiştir.

İncelenen bu uygulamaların kullanım amaçlarına yönelik farklı işlevleri bulunmaktadır. Kullanım amaçlarına özgü olarak sağlık verileri bu uygulamalar aracılığı ile toplanmaktadır.

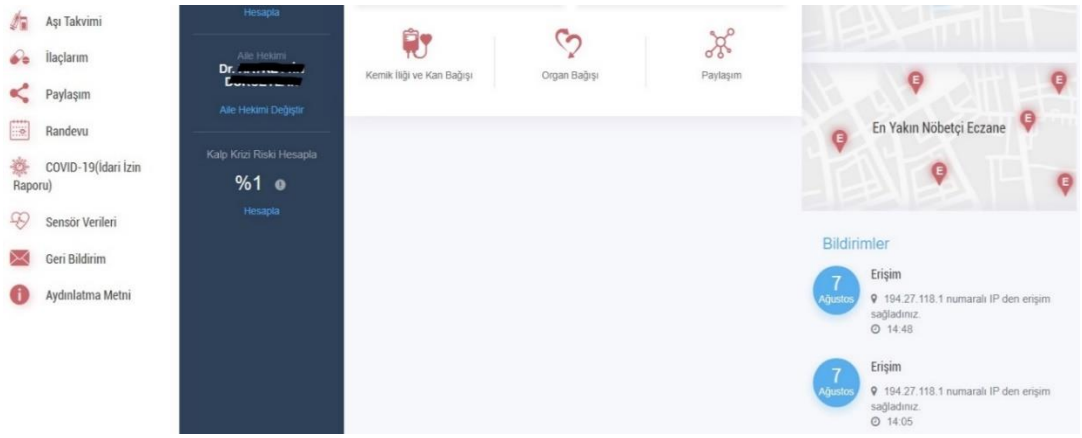
4.2.1. E-Nabız uygulamasının incelenmesi

Ülkemizde kişisel sağlık sistemi olarak e-Nabız uygulaması kullanılmaktadır. Bu uygulama ile kişiler, sağlık kurumlarına yaptıkları tüm ziyaret ve detaylarına, tüm tetkik bilgilerine, güncel sağlık bilgilerine, muayene ve tedavilerine ait tüm sağlık bilgilerine ve çocuklarının sağlık bilgilerine erişim sağlayabilmektedirler.

Uygulamayı kullanabilmek için e-Nabız'a kayıt olmak gerekmektedir. Uygulamaya kayıt olduktan sonra, T.C. kimlik numarası ve kişinin oluşturduğu şifre ile giriş yapılabilmektedir. Uygulamaya e-Devlet üzerinden de erişim sağlanabilmektedir.



Görsel 6. E-Nabız uygulamasına giriş yapıldıktan sonra açılan ana ekran



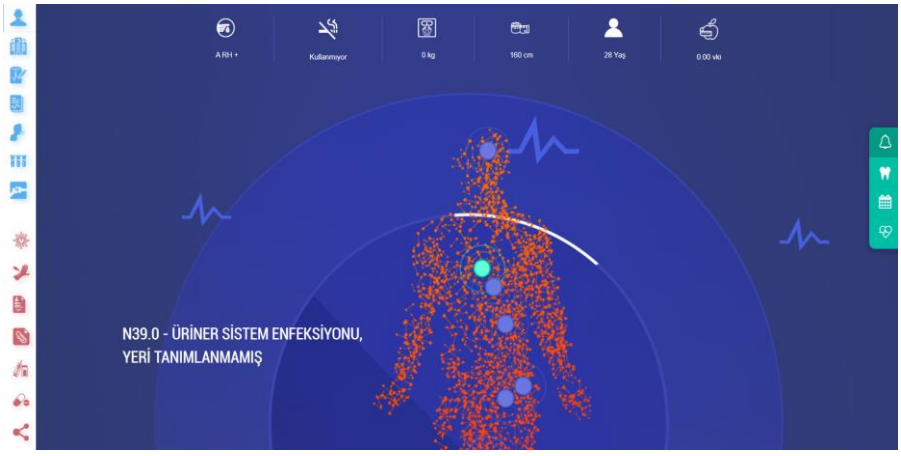
Görsel 7. E-Nabız uygulamasına giriş yapıldıktan sonra açılan ana ekran

E-Nabız kaydına giriş yapıldıktan sonra, uygulamanın ana ekranında "akıllı asistan", "ziyaretlerim", "reçetelerim", "raporlarım", "hastalıklarım", "tahlillerim", "radyolojik

görüntülerim”, “Covid-19”, “alerjilerim”, “acil durum notlarım”, “dokümanlarım”, “aşı takvimi”, “ilaçlarım”, “paylaşım”, “randevu”, “Covid-19 (İdari izin raporu)”, “sensör verileri”, “geri bildirim” ve “aydınlatma metni” işlemlerinin yapılabileceği şekilde sınıflandırma bulunmaktadır (Görsel 6). Ayrıca “Covid-19 ile ilgili bilgilere ulaşma” seçeneği, “influenza risk durumu sorgulama” seçeneği, “randevu al” seçeneği, “aşı çalışması için gönüllü ol” seçeneği, “kemik iliği ve kan bağışı” seçeneği, “organ bağışı” ve “paylaşım” seçenekleri bulunmaktadır. En son gidilen sağlık kurumları, en yakın hastane konumu ve en yakın nöbetçi eczane konumu bilgileri de vardır. Bununla birlikte e-Nabız kaydına erişim sağlanan IP adresi bilgisi, erişim saati bilgisi ile birlikte yer almaktadır. Gidilen sağlık kurumlarını değerlendirme seçeneği de bu ekran üzerinde bir özellik olarak bulunmaktadır (Görsel 7).

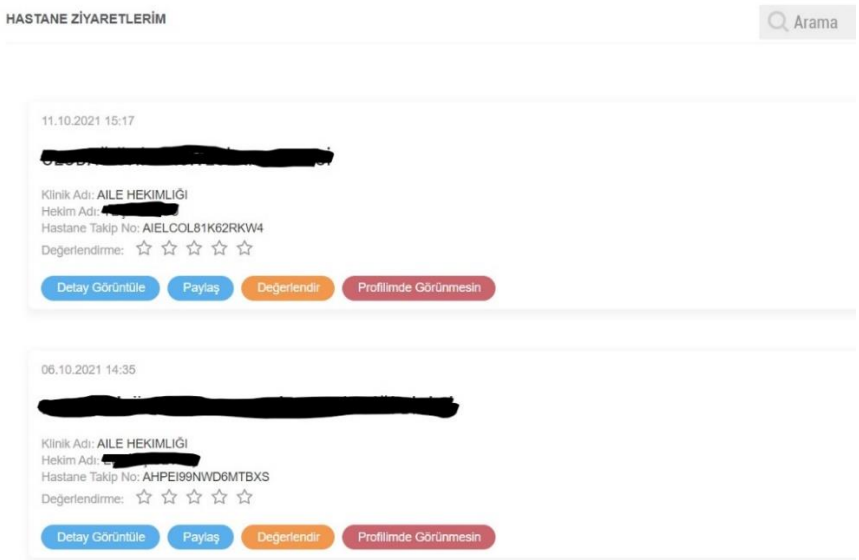
Akıllı asistan ekranı: Akıllı asistan ekranında bulunan kişisel bilgiler; kan grubu, sigara kullanımı, kilo, boy, yaş ve vücut kitle indeksidir. Daha önceki hastalık teşhisleri bu ekranda görüntülenebilmektedir. Ayrıca hasta öneri, diş hastalığı ile ilgili veriler, etkinlik takvimi gibi özellikler bulunmaktadır. Akıllı asistan ekranı Görsel 8’deki gibidir.

Ekran üzerinde bulunan sensör verileri; adım, oksijen doygunluğu, solunum hızı, ağırlık, vücut sıcaklığı, tansiyon, nabız, kan şekeri, vücut kitle endeksi, kalsiyum, gıda kalorisi, düşme sayısı, aktif kalori, çıkılan kat, uyku incelemesi ve bisiklet mesafesi bilgileridir. Sensör verilerine ait bilgiler, manuel olarak kaydedilememektedir.



Görsel 8. Akıllı asistan ekranı

Ziyaretlerim ekranı: Bu ekranda kişinin daha önce yapmış olduğu tüm hastane ziyaretleri, hastane adı, klinik adı, hekim adı ve hastane takip numarası bilgileri listelenmektedir. Kullanıcı bu ekran üzerinde ziyaret ettiği sağlık kurumlarını değerlendirebilmekte, bilgilerini paylaşabilmekte ve "profilimde görünmesin" seçeneği ile akıştaki bilgilerini gizleyebilmekte ve "detay görüntüleme" seçeneği ile bilgilerine daha ayrıntılı bir şekilde erişim sağlayabilmektedir. "Detay görüntüle" seçeneği içinde sağlık kurumunun adı, klinik adı, gidilen tarih ve saat bilgisi, tanı, ek tanılar ve hekim adı bilgileri bulunmaktadır. Hastane ziyaretlerim ekranı Görsel 9'daki gibidir.



Görsel 9. E-Nabız hastane ziyaretlerim ekranı

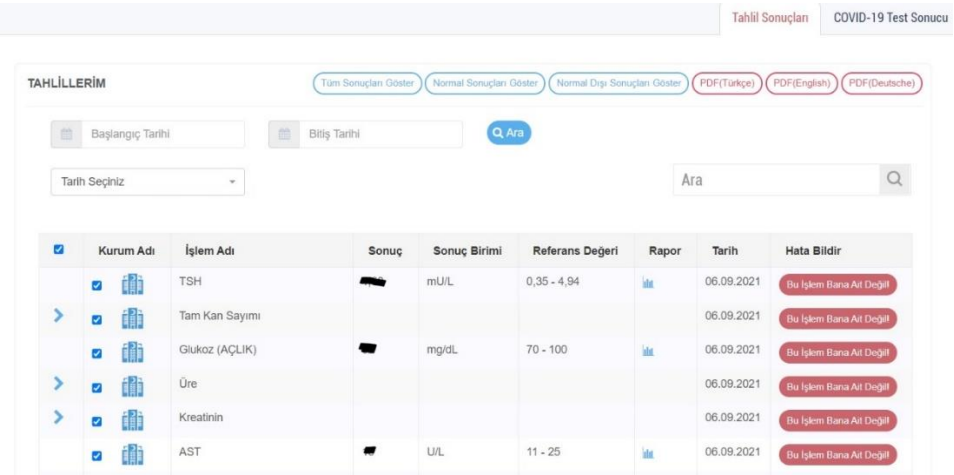
Reçetelerim ekranı: Reçetelerim ekranında kullanıcı için ilaç hatırlatmaları, ilaç kullanım bilgileri, ilaç yan etkileri ve reçete bilgileri vardır. Reçete bilgileri incelediğinde, tarih ve saat, reçete numarası, reçete türü ve hekim bilgileri bulunmaktadır. Reçetelerim ekranında bulunan detay görüntüleme seçeneği tıklandığında ilacın barkod numarası, ilaç adı, açıklama, doz, periyot, kullanım şekli, kullanım sayısı ve kutu adı bilgileri yer almaktadır. Bu ekranda kullanılan ilacın yan etkilerinin manuel olarak eklenebileceği bir seçenek de mevcuttur.

Raporlarım ekranı: Bu ekranda tarih, rapor numarası, rapor takip numarası, rapor türü, başlangıç tarihi, bitiş tarihi ve tanı bilgileri bulunmaktadır. Kullanıcı rapor bilgilerini pdf dosyası biçiminde açabilmektedir. Rapor belgesinde raporun alındığı kurum adı, SGK rapor takip numarası, tarih, adı, soyadı, T.C. numarası, doğum yılı,

açık adres bilgileri, sosyal güvencesi, ICD kodu ve tanıları, teşhisleri, raporun başlama ve bitiş tarihi, ilaçları ve kullanım bilgileri, açıklama ve hekim adı soyadı ile hekimin branşı yazmaktadır.

Hastalıklarım ekranı: Bu ekranda muayene tarihi ve saati, tanı, klinik ve hekim bilgisi bulunmaktadır. Tanı için "detay görüntüle" sekmesi mevcuttur. Bu sekme açıldığında hastalığın ayrıntılı tanısı ile muayene tarih ve saat bilgileri yer almaktadır.

Tahlillerim ekranı: Bu ekran üzerinde kişinin yaptırmış olduğu tüm tahlil sonuçları listelenmektedir.



Görsel 10. E-Nabız tahlillerim ekranı

Bütün tahlilleri görüntüleyebilmek için tarih aralığı seçeneği, "tüm sonuçları göster", "normal sonuçları göster", "normal dışı sonuçları göster" ve "pdf olarak göster" seçenekleri mevcuttur. Yapılan tahlillerin kurum bilgisi, işlemi, sonucu, sonuç birimi, referans değeri, rapor ve tarih bilgileri yer almaktadır. "Hata bildir" sekmesi ile işlemin kişinin kendisine ait olmadığı bildirilmektedir (Görsel 10).

Radyolojik görüntülerim ekranı: Bu ekranda tarih, ön izleme bilgisi, hastane adı, açıklama, rapor, radyolojik görüntüler ve paylaş sekmelerinin kullanılabileceği seçenekler mevcuttur. Radyolojik görüntülerde, "görüntüyü aç" sekmesi tıklanınca ilgili radyolojik görüntü ekranda görüntülenebilmektedir. Görüntüyü kişi isterse "profilimde görünmesin" seçeneğini tıklayarak akışta gizleyebilmektedir.

Covid-19 ekranı: Bu ekran açıldığında kişiye ait aşı bilgileri listelenmektedir. Buna göre aşı adı, aşı üretici firma adı, aşı dozu bilgisi, aşı yapılma yeri ve işlem tarihi bilgileri bulunmaktadır.

Alerjilerim ekranı: Bu ekranda deri prick testleri, alerji tanıları ve alerji bilgileri bulunmaktadır.

Acil durum notlarım ekranı: Bu ekran, acil durumlarda sağlık tesislerinde ve 112 merkezlerinde görünmesi istenilen sağlık bilgilerinden oluşmaktadır. Buraya eklenen bilgilerin sağlık personeli tarafından gerekli müdahale yapılabilmesi için kullanılacağı bilgisi yer almaktadır. Ayrıca bilgilerin doğruluğu ve sorumluluğunun hastaya ait olduğu belirtilmektedir.

Dokümanlarım ekranı: Bu ekran kişinin sağlığı ile ilgili hekiminin görmesini istediği (anlık çıkan yara, döküntü vb.) görselleri yükleyebileceği bir alandır. Yüklenecek görsellerin doğruluğu ve sorumluluğunun hastaya ait olduğu bilgisine yer verilirken, yüklenen görsellerin yasal sorumluluk doğurmayacağı bilgisi de verilmektedir.

Aşı takvimi ekranı: Bu ekranda bulunan "persentil" sekmesi, çocuğun büyüme cetvelini göstermektedir. Çocuğun baş çevresi, boy uzunluğu ve ağırlığı kaydedilmişse görüntülenebilmektedir. Aşılar sekmesinde işlem tarih ve saati, yapılan aşılar, aşı dozu ve yapılma yeri gösterilmektedir. Aşı takvimi sekmesinde genel olarak yapılan Hep-B, Suçiçeği, Hep-A ve BCG gibi çocukluktan itibaren yapılan tüm aşılar, doz sayıları ile birlikte listelenmektedir.

Randevu ekranı: Bu ekranda kişinin almış olduğu randevular, randevu tarih ve saati, kurum bilgisi, klinik, muayene yeri ve hekim bilgilerine göre listelenmektedir.

Covid-19 (İdari izin raporu) ekranı: Bu ekranda idari izin raporları gösterilmekte ve şu uyarı bulunmaktadır: "E-Nabız sisteminden idari izne ilişkin dokümanın alınamaması kronik rahatsızlığınızın bulunmadığı şeklinde anlaşılmamalıdır. İdari izne konu kronik rahatsızlıklar, bakanlığımız ilgili Bilim Kurulları tarafından hazırlanan görüşler doğrultusunda COVID-19 açısından yüksek riskli kronik rahatsızlıklar ilişkilendirilerek belirlenmiştir. Oluşan risk skorunu sistem otomatik hesaplayarak idari izne esas raporu oluşturmaktadır."

İlaçlarım ekranı: Bu ekranda kişiye ait reçetenin tarih ve saati, barkod numarası, reçete numarası bilgileri bulunmakta, yazılan ilaçların adı, dozu, periyotu, kullanım şekli, kullanım sayısı, kutu adedi ve yazılan hastane ve kliniğin adı bilgileri bulunmaktadır. Ayrıca ilaç katılım payı bilgileri de bu ekranda yer almaktadır (Görsel 11).

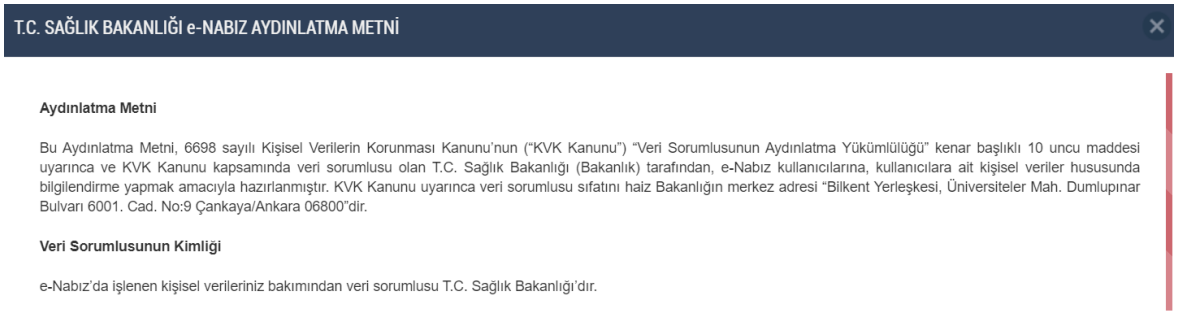
Görsel 11. İlaçlarım ekranı

Paylaşım ekranı: Bu ekran üç grupta sınıflandırılmıştır: "Benimle Paylaşılanlar", "Geçici Paylaştıklarım" ve "Sürekli Paylaştıklarım". Ekranda ayrıca "Çocuklarımı Göremiyorum?" ve "Yakınlarını e-Nabız'a Davet Et" sekmeleri bulunmaktadır.

Sensör verileri ekranı: Bu ekranda tansiyon, nabız, kan şekeri, ağırlık, adım, vücut kitle indeksi, kalsiyum, gıda kalorisi, düşme sayısı, aktif kalori, çıkılan kat, oksijen doygunluğu, solunum hızı, uyku incelemesi, vücut sıcaklığı ve bisiklet mesafesi bilgileri listelenmektedir.

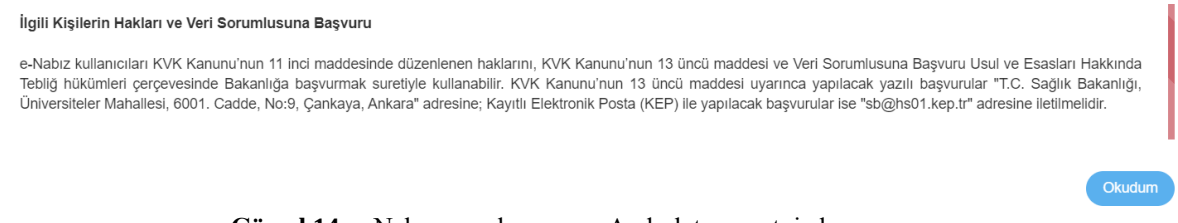
Geri Bildirim ekranı: Bu ekranda "Gönderdiğim Bildirimler", "Güzel Bir Fikriniz Mi Var?" ve "Geri Bildirim" seçenekleri mevcuttur. Bu seçenekler ile uygulama hakkında bildirim alınmakta, kişilerin uygulama ile ilgili görüşleri ve fikirleri sorgulanmaktadır.

Aydınlatma metni ekranı: Uygulamanın Aydınlatma metninde işlenen bilgiler, bilgilerin işlenme amaçları açıklanmakta ve veri sorumlusunun kimliği hakkında bilgi verilmektedir. Görsel 12, Görsel 13 ve Görsel 14 e-Nabız uygulamasının Aydınlatma metnini göstermektedir.



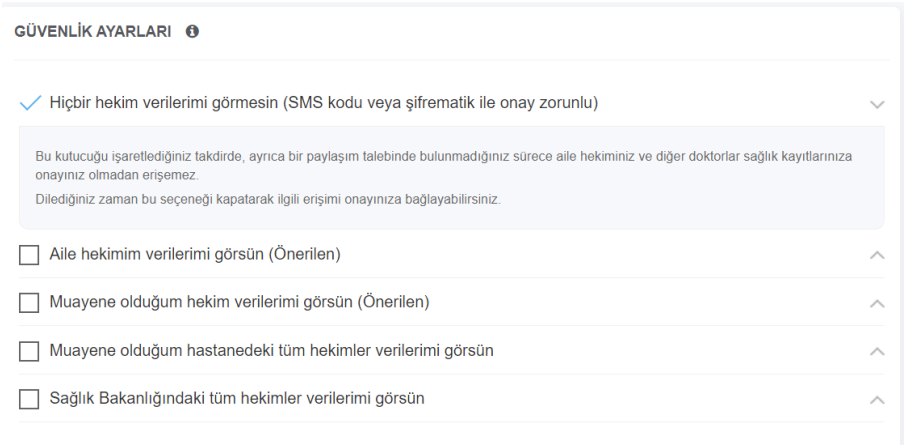
Görsel 12. e-Nabız uygulamasının Aydınlatma metni ekranı

Görsel 13. e-Nabız uygulamasının Aydınlatma metni ekranı



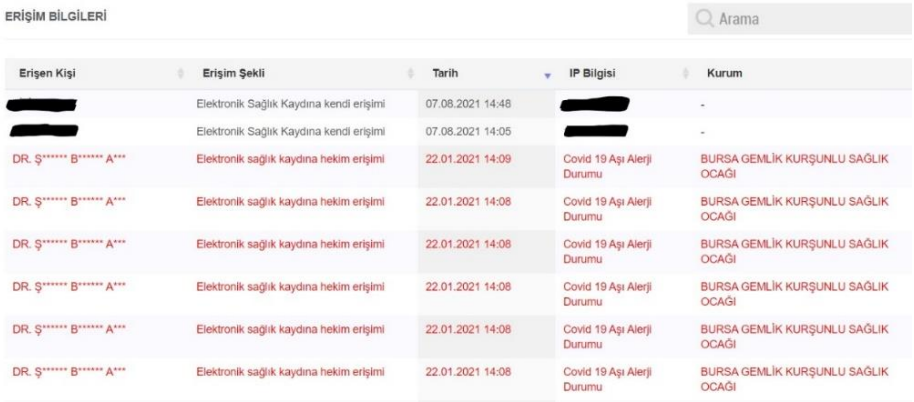
Görsel 14. e-Nabız uygulamasının Aydınlatma metni ekranı

Uygulamanın mahremiyeti korumaya yönelik bir özelliği bulunmaktadır. Buna göre sağlık çalışanlarının verilere erişimi sınırlandırılmaktadır. Kişiler verilerini kimlerin görebileceğini Görsel 15'teki gibi tercih edebilmektedir.



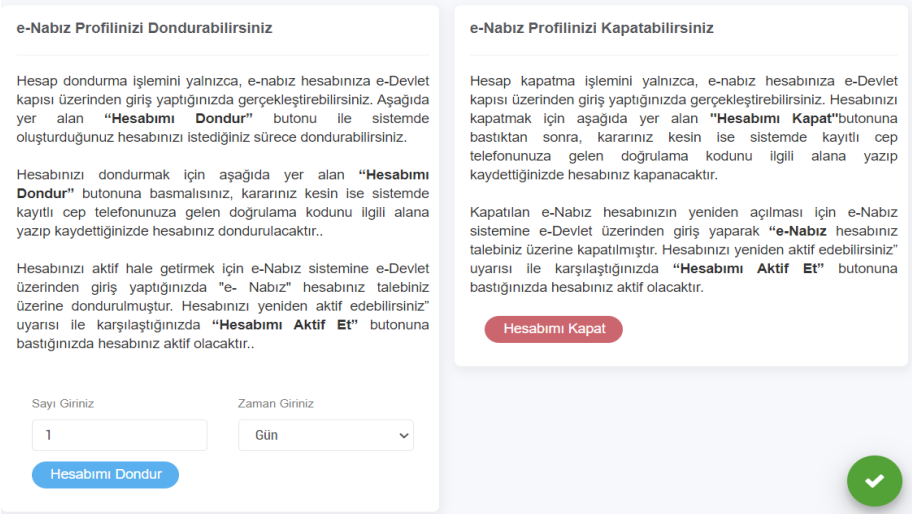
Görsel 15. E-Nabız uygulamasının güvenlik ayarları ekranı

Mahremiyet ve gizlilik açısından uygulamanın "Bildirimler" sekmesinde sisteme kimlerin erişim sağladığı listelenmektedir. Buna göre sisteme erişim sağlayan hekimin adı gizli olacak şekilde, hangi kurumdan erişim sağlandığı, erişim sağlayan hekimin IP bilgisi, erişim tarihi ve erişim şekli bilgileri listelenmektedir (Görsel 16).



Görsel 16. E-nabız erişim bilgileri ekranı

Son olarak e-Nabız kaydında hesap dondurma ve hesap kapatma özellikleri bulunmaktadır.

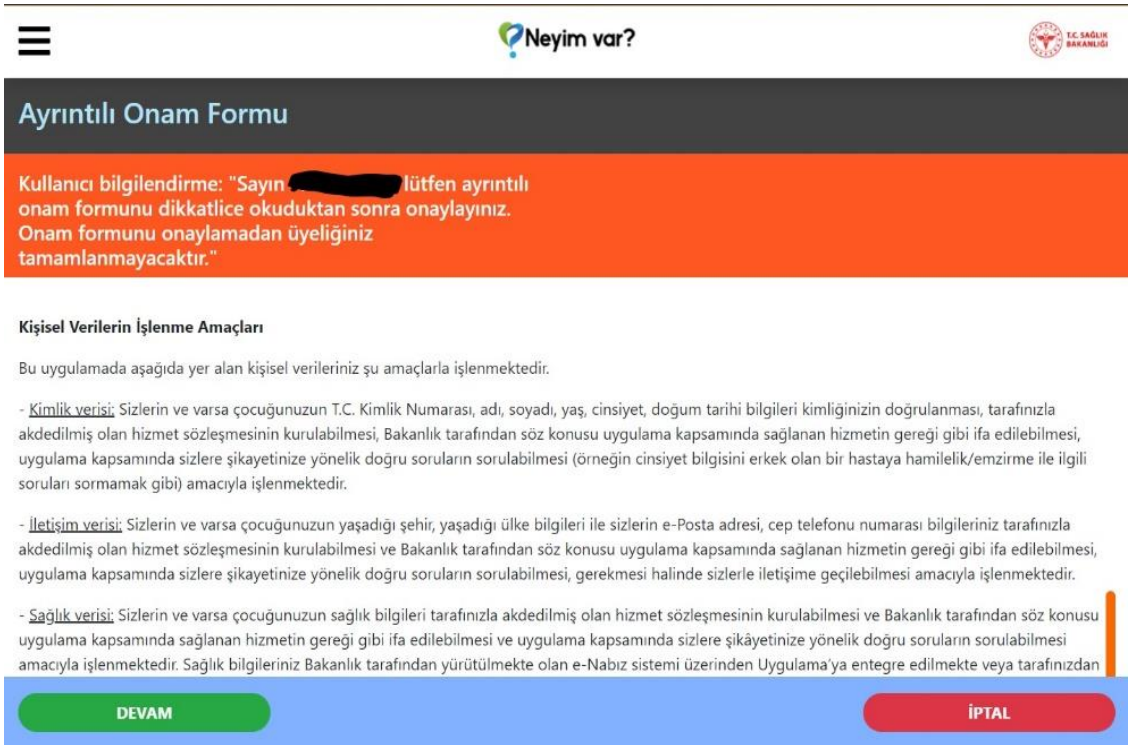


Görsel 17. E-Nabız uygulamasının kayıt dondurma ve hesap kapatma ekranları

4.2.1.1.E-Nabız uygulamasına eklenen "Neyim Var?" uygulaması

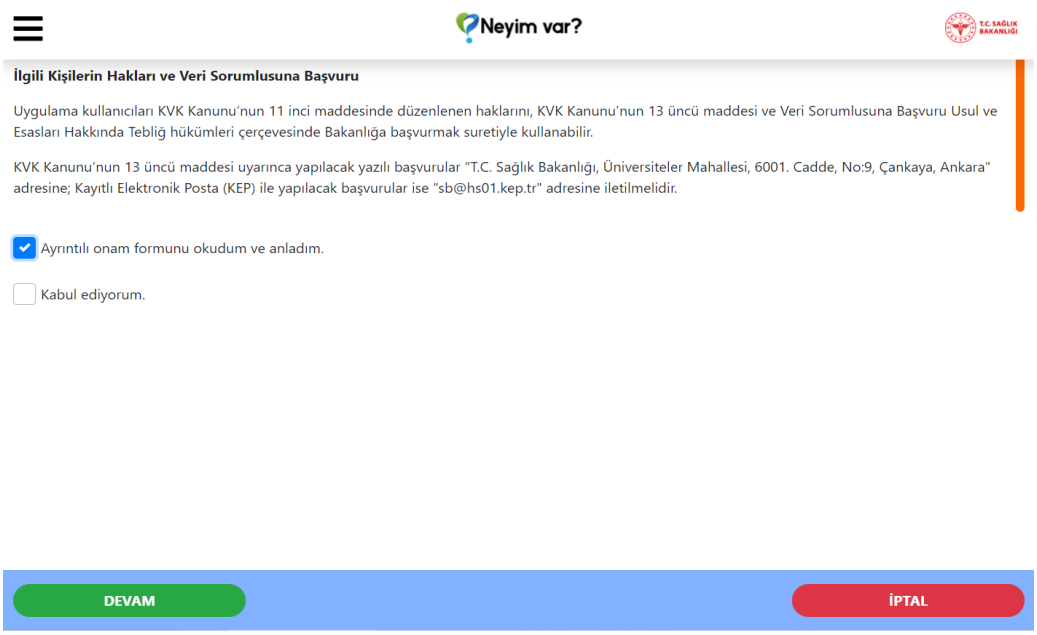
E-Nabız uygulamasına temel bir özellik olarak yapay zeka destekli olduğu bildirilen "Neyim Var?" isimli bir algoritma eklenmiştir. Bu sistem "kullanıcının şikayetlerine ilişkin alınan bilgiler ile kullanıcının geçmiş sağlık verilerini kullanarak zenginleştirilmiş sorgulama süreci başlatıp hastaya gitmesi gereken polikliniği öneren, sorgulama verilerini ve muhtemel tanılarını hastanın gideceği doktorla paylaşabilen yapay zeka destekli bir 'uzman sistem' (expert system)" biçiminde tanımlanmaktadır.

Neyim Var? sistemi için ayrıca bir Aydınlatma metni mevcuttur. Görsel 18, Görsel 19 ve Görsel 20, sistemin Aydınlatma metni ekranını göstermektedir.



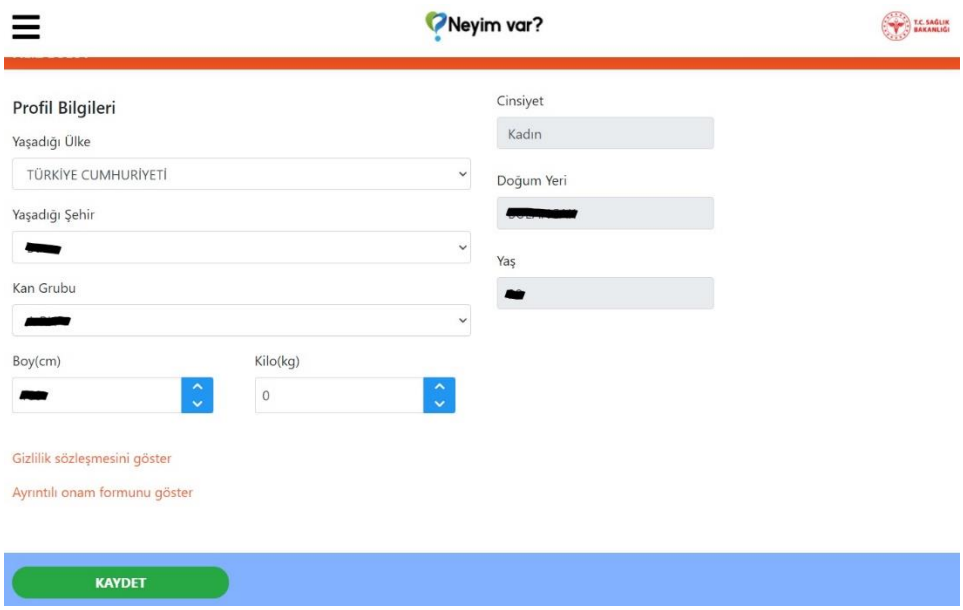
Görsel 18. Neyim Var? uygulamasının Aydınlatma metni ekranı

Görsel 19. Neyim Var? uygulamasının Aydınlatma metni ekranı



Görsel 20. Neyim Var? uygulamasının Aydınlatma metni ekranı

Neyim Var? sistemini kullanabilmek için onam formunun kabul edilmesi gerekmektedir. Onam formu incelendiğinde hangi kişisel verilerin işlendiği bilgileri açıklanmaktadır. Formun sonundaki "Ayrıntılı onam formunu okudum ve anladım" ibaresi ile "Kabul ediyorum" ibaresi işaretlendikten sonra uygulama kullanıma açılmaktadır. Uygulamaya giriş yapıldıktan sonra bazı profil bilgileri otomatik olarak e-Nabız kaydından çekilmektedir.



Görsel 21. Neyim Var? uygulamasının profil bilgileri ekranı

Neyim Var? uygulamasının e-Nabız kaydından çektiği kişisel bilgiler, ülke ve şehir, kan grubu, boy, kilo, cinsiyet, doğum yeri ve yaş bilgileridir.

Uygulamanın temel amacı hastalık tanısı koymak ve kişiyi uygun sağlık polikliniğine yönlendirmektedir. Buna göre kişi hastalığı ile ilgili şikâyetini sisteme yazması gerekir. Kullanıcı hastalığı ile ilgili şikâyetini yazarken karşısına tanımlanmış hastalık bilgileri çıkmaktadır. Ayrıca kullanıcı, üç boyutlu görsel üzerinden de sağlık durumu ile ilgili şikâyetini tanımlayabilmektedir. Görsel 22, kullanıcının şikâyetlerini işaretleyebileceği üç boyutlu ekranı göstermektedir.

Görsel 22. Neyim Var? uygulamasının üç boyutlu şikâyet ekranı

Bir şikâyet yazıldıktan veya üç boyutlu manken üzerinden şikâyet tarifi yapıldıktan sonra uygulama, hastalıkla ile ilgili ek sorular sormaya başlamaktadır. Bu sorular cevaplandıktan sonra, olası teşhisler ve ilgili poliklinik önerileri listelenmektedir. Son olarak sistem hastayı uygun poliklinikten randevu alabilmesi için MHRS ekranına yönlendirmektedir.

Uygulamanın "şikâyet geçmişi" ekranında kişinin daha önce yaptığı şikâyetler listelenmektedir. Uygulama kullanıcıya, şikâyet geçmişini silme ve şikâyetlerinin dokümanını alabilmesi için "pdf olarak tümünü indir" seçeneği sunmaktadır.

4.2.2. Hızır AHBS uygulamasının incelenmesi

Aile Hekimliği Bilgi Sistemleri, birinci basamak ayakta sağlık hizmetlerinin gerçekleştirildiği ve sağlık çalışanlarının hasta bilgilerini kayıt altına aldığı bir veri tabanıdır.

Tez kapsamında incelenen Hızır AHBS sisteminin ana ekranında hekimin genel işlemler yapabildiği "kişi işlemleri", "hasta kabul", "poliklinik defteri", "iş planı", "randevu defteri", "aile işlemleri", "veri işlemleri", "istatistik sorgulama", "aylık çalışma" ve "program ayarları" butonları bulunmaktadır.

4.2.2.1.Genel ekranlar

Kişi işlemleri ekranı: Bu ekranda yeni kişi kaydı, kişi kaydı düzenlemesi ve yeni muayene ekleme işlemleri yapılmaktadır. Ayrıca bu ekranda "tüm aile", "komşular", "diğer işlemler", "Excel'e aktar", "not defteri", "karar destek sayfası", "evrak kayıt", "stok işlemleri", "genel uyarı listesi" ve "özellikli izlem kişi listesi" işlemlerin yapıldığı ekranlar bulunmaktadır.

Görsel 23. Kişi işlemleri ekranı

Kişi işlemleri ekranında bebek ve çocuk listesi, 15-49 yaş kadın listesi, gebe listesi, lohusa listesi, 65 yaş üstü listesi, hükümlüler ve uyarı eklenen kişiler listelenmektedir. Tüm liste ekranı incelendiğinde; kişisel bilgiler olarak kimlik numarası, adı, soyadı, cinsiyeti, resmi doğum tarihi, yaş (ay ve gün), anne adı, baba adı, medeni hali, aile kodu, kan grubu, hasta tipi, telefon, adres, AH (Aile Hekimliği) kayıt tarihi, mevcut AH, kır kent, öncelik, özlük güncelleme tarihi, en son işlem tarihi, ölüm tarihi ve doğum yeri bilgileri bulunmaktadır (Görsel 23). 15-49 yaş kadın listesi ekranında bu bilgilere ek olarak sosyal güvence durumu, gebe listesi ekranında ayrıca gebelik tespit tarihi, son adet tarihi, kaçıncı gebelik olduğu, beklenen doğum tarihi, evlenme yaşı, sık izlem, risk durumu, kullanılan AP (Aile Planlaması) yöntemi, AP kullanmama nedeni ve gebe risk faktörleri bilgileri bulunmaktadır. Hükümlüler ekranında uyruk, doğum sırası, anne ve baba T.C. kimlik numarası, pasaport no, hasta kayıt türü, gelir

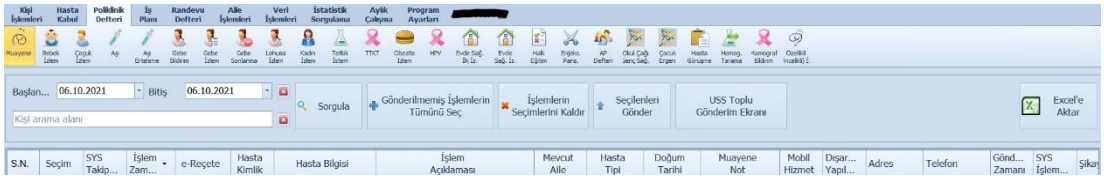
durumu, iş durumu, kan grubu, madde kullanımı, özürlülük durumu, öğrencinin sınıfı, meslek, sosyal güvence durumu, yaralanma geçmişi, alkol kullanımı, ameliyat geçmişi, sigara kullanımı ve kullandığı sigara adedi, öğrenim durumu, e-posta adresi ve ağırlık bilgileri işlenebilmektedir (Görsel 23).

Hasta kabul ekranı: Bu ekranda "dış gösterim kapat", "kişiyi çağır", "kişiyi sona taşı", "kişiyi sil", "tamamlandıya çevir", "bekleyene çevir", "bekleyenleri yönlendirme", "kabul alma ayarları", "hekim seçmeli kabul için hekim fotoğrafı", "kapı üstü ekran ayarları", "dış ekran video listesi" ve "kabul yasaklanan hasta listesi" işlemleri yapılmaktadır (Görsel 24).

Görsel 24. Hasta kabul ekranı

Bununla birlikte hasta kabul ekranında bekleyen hastaların ve MHRS'den randevu alan hastaların bilgileri listelenmektedir. Bekleyen hastaların, hasta tipi (misafir, kesin, ilişik kesik), kimlik numarası, adı, soyadı, doğum tarihi, cinsiyeti, öncelik nedeni, mevcut AH, AH kayıt tarihi, kabul zamanı, telefon ve yaş (ay ve gün) bilgileri bulunmaktadır (Görsel 24).

Poliklinik defteri ekranı: Hekim poliklinik defteri ekranında, muayene, bebek izlem, çocuk izlem, aşı, aşı erteleme, gebe bildirim, gebe izlem, gebe sonlanma, lohusa izlem, kadın izlem, tetkik istem, TTKT (toplum tabanlı kanser tarama), obezite izlem, HPV, evde sağlık ilk izlem, evde sağlık izlem, halk eğitim, enjeksiyon pansuman, AP defteri, okul çağı gençlik sağlığı, çocuk ergen, hasta görüşme, hemoglobin tarama, mamografi bildirim ve özellikli izlem işlemlerini yapmaktadır (Görsel 25).



Görsel 25. Poliklinik defteri ekranı

Ayrıca bu ekran üzerinde hastaların işlem zamanı, e-reçete, hasta kimlik, hasta bilgisi, işlem açıklaması, mevcut aile, hasta tipi, doğum tarihi, mobil hizmet, adres, telefon ve şikayet bilgileri ile hekimin muayene not bilgisi bulunmaktadır (Görsel 25).

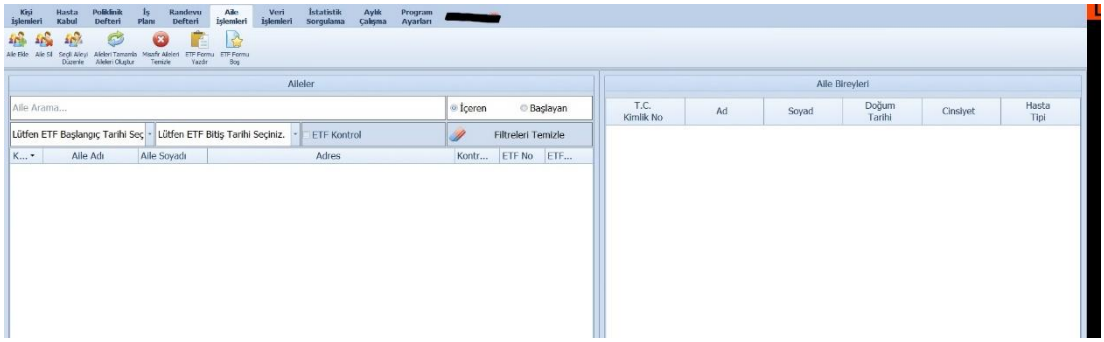
İş planı ekranı: Aile hekimi bu ekranda iş planlarını görüntülemektedir. Ekranda hastaların T.C. kimlik numarası, ad, soyad, doğum tarihi, anne adı, baba adı, bir önceki yapılma tarihi, ATS (Aşı Takip Sistemi) düşüm, aile kodu, işlem başlangıcı, işlem bitişi, adres, telefon, göç dilekçesi, işlem durumu, kalan süre, mahalle, medeni hali, yaş, ay, gün ve gebelik haftası bilgileri listelenmektedir. Ayrıca hastaların hekimin performansına dahil olup olmadığı bilgisi vardır (Görsel 26).

Görsel 26. İş planı ekranı

İş planı ekranında bulunan ‘karar destek sayfası’ tıklandığında, Sağlık Bakanlığı’nın web sayfası açılmaktadır (Görsel 26).

Randevu defteri ekranı: Bu ekran hekimin randevu bilgilerini göstermektedir.

Aile işlemleri ekranı: Bu ekranda aile ekle, aile sil, seçili aileyi düzenle, aileleri tamamla aileleri oluştur ve misafir aileleri temizle işlemleri yapılmaktadır. Bu ekranda ailelerle ilgili, aile adı, aile soyadı, adres ve kontrol tarihi bilgileri bulunmaktadır. Aile bireylerinin T.C. kimlik numarası, ad, soyad, doğum tarihi, cinsiyet ve hasta tipi bilgileri kaydedilebilmektedir (Görsel 27).



Görsel 27. Aile işlemleri ekranı

Veri işlemleri ekranları: Bu ekran üzerinde kişi güncelleme, bakanlıktaki gebe lohusa listesi görüntüleme, toplu HPV-Mamografi sonuç sorgulama, aşı takvimleri, MERNİS (Merkezi Nüfus İdaresi Sistemi) toplu sorgulama, ilaç listeleri, lokasyon ve kurum listeleri sorgulama, tetkik liste güncellemesi, MERNİS eşleştirme geçmişi, evde sağlık hizmet başvuru emirleri ve kişi listesi karşılaştırma işlemleri yapılmaktadır (Görsel 28).

Veri işlemleri ile ilgili olarak kişi güncelleme ekranında hastanın T.C. kimlik numarası, adı, soyadı, cinsiyeti, resmi doğum tarihi, beyan doğum tarihi ve sonuç bilgileri bulunmaktadır (Görsel 28).

Görsel 28. Veri işlemlerinin görüntülendiği bakanlık kişi listesi ekranı

Bakanlık kişi listeleri ekranında özellikli izlem kişi listesi, USS (Ulusal Sağlık Sistemi) özellikli izlem kayıtları, gezici hizmet alanlar listesi, birime ait kişi listesi, mevsimsel influenza aşısı yapılabilir kişi listesi ve birime ait HYP listesi görüntülenmektedir. Bakanlık kişi listesi ekranında ayrıca Aile Hekimliğine kayıtlı bireylerin Covid-19 temaslı veya pozitif olan hasta listesi vardır. Hasta izlemleri T.C. kimlik numarası, adı soyadı, doğum tarihi, aile kodu, bildirim tarihi, telefon numarası, izlem sayısı, temas tipi, süreç durumu, son izlem tarihi, izlem yapılması ve izlem adım süreçleri bilgilerine göre yapılmaktadır (Görsel 28).

Bakanlıktaki gebe lohusa listesi ekranında T.C. kimlik numarası, adı soyadı, son adet tarihi, riskli gebelik detayı ve sonuç bilgileri bulunmaktadır (Görsel 28).

Toplu HPV – Mamografi sonuç sorgulama ekranında T.C. kimlik numarası, adı soyadı, doğum tarihi, sonuç, istem tarihi ve kayıt durumu bilgileri bulunmaktadır (Görsel 28).

Aşı takvimleri ekranı ATS (Aşı Takip Sistemi) ile senkronize bir şekilde çalışmakta ve aşıların hangi tarihler arasında yapılacağı bilgileri listelenmektedir. Hastaların T.C. kimlik numarası, adı soyadı, aşı, dozu, ilk tarihi, yapılma tarihi ve son tarih bilgileri bulunmaktadır. Aynı ekranda bulunan aşı erteleme listesinde doğum tarihi bilgisi yer almaktadır (Görsel 28).

MERNİS toplu sorgulama ekranında MERNİS'ten kişi bilgileri çekilebilmekte ve ölü görünen kişiler sistemde pasif duruma getirilebilmektedir. Sorgulama türüne göre kişiler T.C. kimlik numarası, adı soyadı, cinsiyet, doğum tarihi ve sonuç bilgilerine göre ekranda listelenmektedir (Görsel 28).

İlaç listeleri sorgulama ekranında SKRS'den (Sağlık Kodlama Referans Sunucusu) ilaç listesi güncellenebilmekte, SGK ilaç geri ödeme durumları sorgulanabilmektedir. Yapılan sorgulamada ilaç barkodu, ilaç adı ve sonuç bilgileri bulunmaktadır (Görsel 28).

Lokasyon ve kurum bilgileri sorgulama ekranında yapılan sorgulama il, ilçe, bucak, köy ve mahalle listesi, kodu, adı ve sonuç bilgisine göre listelenmektedir (Görsel 28).

Tetkik liste güncellemesi ekranında laboratuvar kullanıcı adı, laboratuvar kullanıcı şifresi girişi istenmektedir. Bu sayfada tetkik listesi SUT (Sağlık Uygulama Tebliği) kodu, tetkik adı, fiyatı ve laboratuvar hizmet kodu bilgileri görüntülenmektedir (Görsel 28).

Eşleştirme geçmişi ekranında yeni kayda geçen, kesin kayda çevrilen, ilişiği kesilen ve değişiklik yapılan kişiler listelenmektedir. Kişilere ait, T.C. kimlik numarası, adı soyadı, doğum tarihi, kayıt tarihi mevcut AH, işlem sonucu ve eşleştirme tarihi bilgileri bulunmaktadır (Görsel 28).

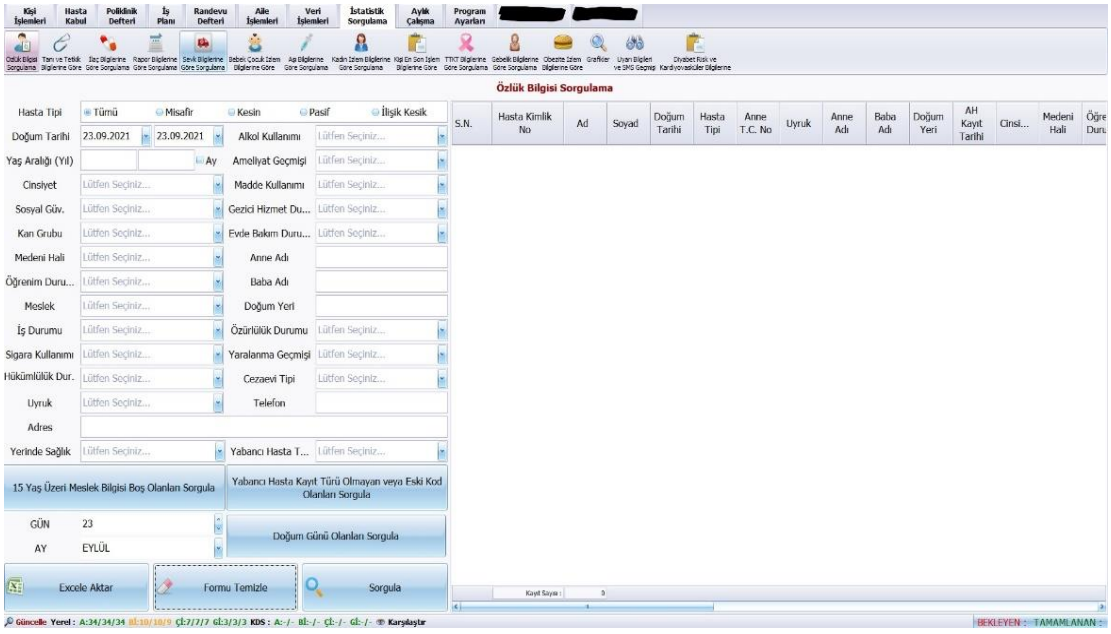
MERNİS eşleştirme geçmişi ekranında hastanın T.C. kimlik numarası, adı, soyadı, doğum tarihi, cinsiyet, hasta tipi, durum ve sonuç bilgileri vardır (Görsel 28).

Evde sağlık hizmet başvuru ve emirleri ekranında hastanın T.C. kimlik numarası, adı, soyadı, doğum tarihi, cinsiyet, işlem zamanı, hizmet emri tarihi, başvuruda bulunan kişinin kimlik numarası, adı soyadı ve telefon numarası bilgileri bulunmaktadır. Ayrıca hastaya dair açıklama, alınan notlar ve adres bilgileri listelenmektedir (Görsel 28).

Veri tabanına kayıtlı bir hasta, aranan kişiler ekranında sorgulanabilmektedir. Yapılan sorgulama kimlik numarası, adı, soyadı, aranma tarihi ve sebebi bilgilerine göre listelenmektedir. Listelenen kişilerin, listeye yeni kişi eklenmesi ve listedeki kişilerin silinmesi işlemleri de bu ekran üzerinde yapılabilmektedir (Görsel 28).

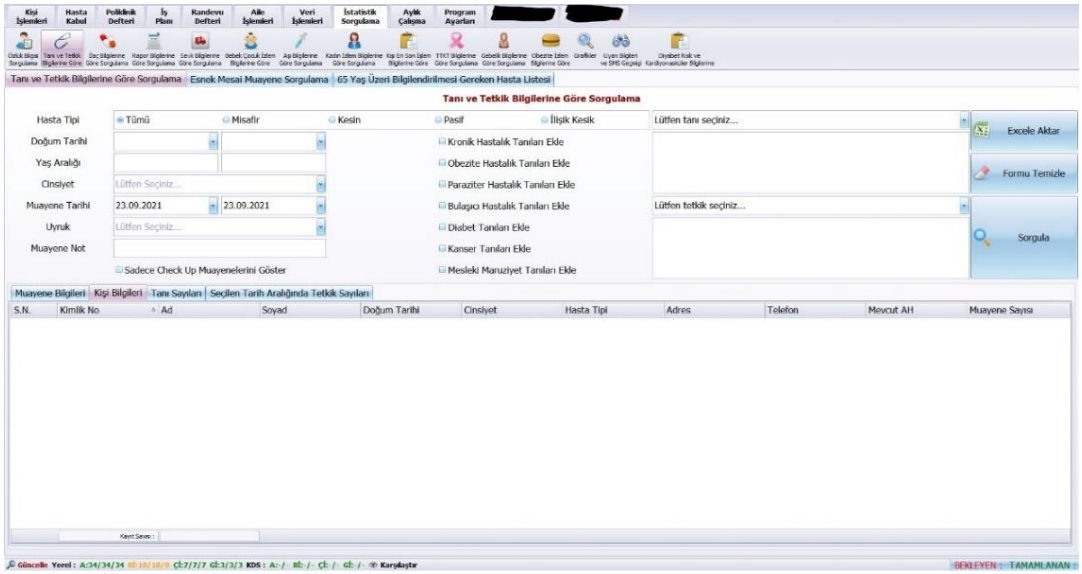
İstatistik sorgulama ekranı: Hastalar bu ekranda özlük bilgisi, tanı ve tetkik, ilaç, rapor, sevk, bebek çocuk izlem, aşı, kadın izlem, TTKT, gebelik ve obezite izlem bilgilerine göre sorgulanmaktadır.

Özlük bilgisi sorgulama ekranı: Özlük bilgilerine göre istatistiksel sorgulamanın yapıldığı bu ekranda hastaların doğum tarihi, yaş aralığı, cinsiyet, sosyal güvence bilgisi, kan grubu, medeni hal, öğrenim durumu, meslek, iş durumu, sigara kullanımı, hükümlülük durumu, uyruk, adres, alkol kullanımı, ameliyat geçmişi, madde kullanımı, gezici hizmet durumu, evde bakım durumu, anne ve baba adı, doğum yeri, özürlülük durumu, yaralanma geçmişi, cezaevi tipi ve telefon bilgileri bulunmaktadır. Bu bilgilere göre yapılabilen sorgulama, hasta kimlik numarası, ad, soyad, doğum tarihi, hasta tipi, anne T.C. kimlik numarası, uyruk, anne adı, baba adı, doğum yeri, aile hekimi kayıt tarihi, cinsiyet, medeni hali ve öğrenim durumu bilgilerine göre listelenmektedir (Görsel 29).



Görsel 29. Özlük bilgisine göre istatistiksel sorgulama ekranı

Tanı ve tetkik bilgilerine göre sorgulama ekranları: Tanı ve tetkik bilgilerine göre yapılan sorgulama ekranında ayrıca esnek mesai muayene sorgulama ve 65 yaş üzeri bilgilendirilmesi gereken hasta listesi ekranları bulunmaktadır (Görsel 30).



Görsel 30. Tanı ve tetkik bilgilerine göre istatistiksel sorgulama ekranı

Tanı ve tetkik bilgilerine göre yapılan sorgulamada, hasta tipi, doğum tarihi, yaş aralığı, cinsiyet, muayene tarihi, uyruk ve muayene notu bilgileri bulunmaktadır. Ayrıca kronik hastalık tanıları, obezite hastalık tanıları, paraziter hastalık tanıları, bulaşıcı hastalık tanıları, diyabet tanıları, kanser tanıları, mesleki maruziyet tanılarından biri veya daha fazlası seçilerek sorgulama yapılabilmektedir. Bu bilgiler

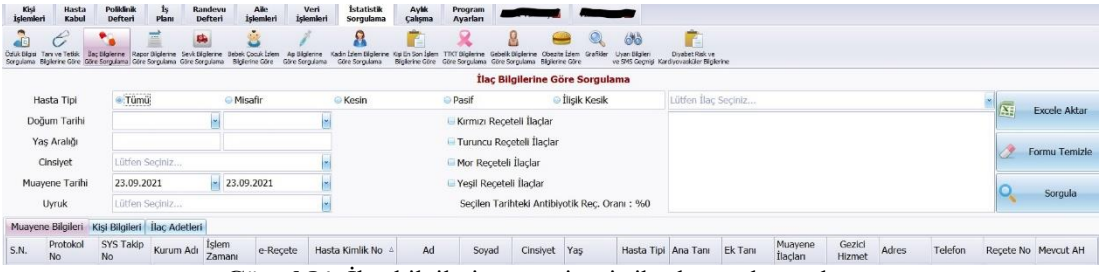
istenilen şekilde doldurulduğunda hastalar, muayene bilgileri, kişi bilgileri, tanı sayıları ve seçilen tarih aralığındaki tetkik sayılarına göre listelenmektedir (Görsel 30).

Muayene bilgileri ekranında Check Up muayenesi, kurum adı, işlem zamanı e-reçete, hasta kimlik numarası, ad, soyad, cinsiyet, yaş, hasta tipi, ana tanı, ek tanı, muayene ilaçları, gezici hizmet, adres, telefon, diastolik, sistolik, ağırlık, boy, nabız, ateş, şikayeti, hikayesi, bulgu, muayene not, mesleki maruziyet durumu, mevcut AH ve bulaşıcı hastalık bildirim bilgileri yer almaktadır.

Kişi bilgileri ekranında kimlik numarası, ad, soyad, doğum tarihi, cinsiyet, hasta tipi, adres, telefon, mevcut aile hekimi ve muayene sayısı bilgileri vardır.

Atmış beş yaş üstü hasta listesi ekranında bilgilendirilmesi gereken ve bilgilendirme yapılmış hastalar listelenmektedir. Listelenen hastaların, kimlik numarası, adı, soyadı, cinsiyet, doğum tarihi, aile kodu, muayene tarihi, varsayılan telefon, diğer telefon ve adres bilgileri bulunmaktadır.

İlaç bilgilerine göre sorgulama ekranları: Bu ekranda sorgulama yapılabilmesi için hasta tipi, doğum tarihi, yaş aralığı, cinsiyet, muayene tarihi, uyruğu, kullandığı ilacı ve hangi tür reçeteli ilaç kullandığı bilgilerinden tercih edilenlerin işaretlenmesi gerekmektedir (Görsel 31).



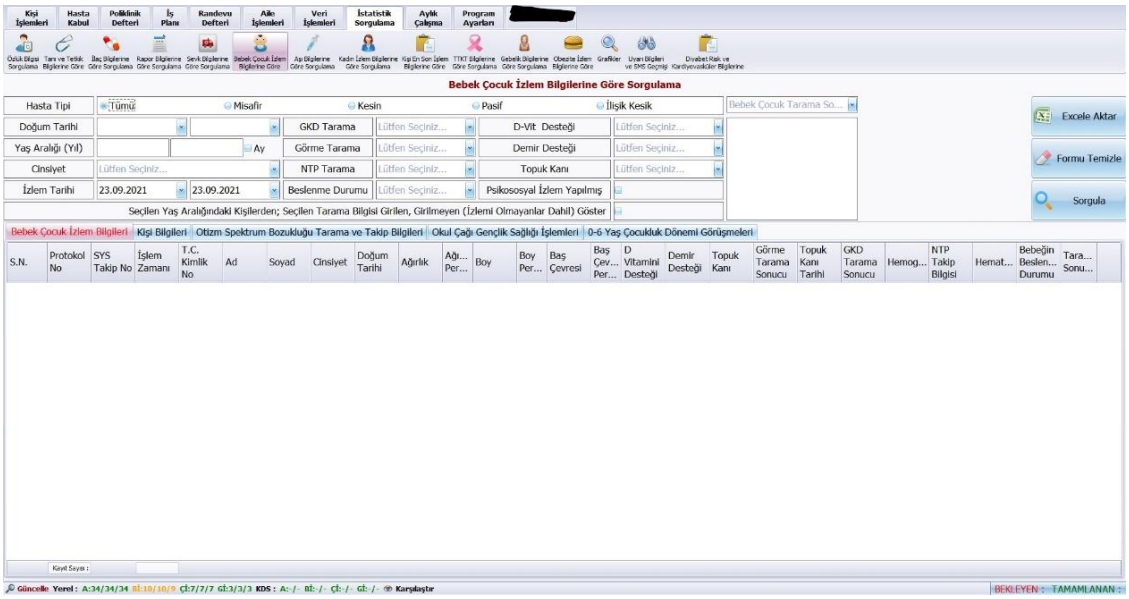
Görsel 31. İlaç bilgilerine göre istatistiksel sorgulama ekranı

Yapılan sorgulama, muayene bilgileri, kişi bilgileri ve ilaç adetlerine göre listelenmektedir. Muayene bilgilerinde kurum adı, işlem zamanı, e-reçete, hasta kimlik numarası, adı, soyadı, cinsiyet, yaş, hasta tipi, tanı, ek tanı, muayene ilaçları, adres, telefon reçete no ve mevcut AH bilgileri yer almaktadır. Kişi bilgileri ekranında kimlik numarası, adı, soyadı, doğum tarihi, cinsiyet, hasta tipi, adres, telefon ve mevcut AH bilgileri bulunmaktadır. İlaç adetleri ekranında ilaç adı ve adedi bilgileri listelenmektedir (Görsel 31).

Rapor bilgilerine göre sorgulama ekranı: İstatistiksel sorgulama rapor bilgilerine göre yapıldığında muayene bilgileri ve kişi bilgilerine göre listeleme yapılmaktadır. Muayene bilgileri ekranında işlem zamanı, rapor açıklama, hasta kimlik numarası, ad, soyad, cinsiyet, öğrenim durumu, öğrencinin sınıfı, yaş, hasta tipi, ana tanı, gezici hizmet, adres, telefon ve mevcut aile hekimi bilgileri bulunmaktadır. Kişi bilgileri ekranında ise kimlik numarası, ad, soyad, doğum tarihi, cinsiyet, hasta tipi, adres, telefon ve mevcut AH bilgileri yer almaktadır.

Sevk bilgilerine göre sorgulama ekranı: Sevk bilgilerine göre yapılan sorgulama, muayene bilgileri ve kişi bilgilerine göre listelenmektedir. Muayene bilgileri ekranında işlem zamanı, sevk edilen klinik, hasta kimlik numarası, ad, soyad, cinsiyet, yaş, hasta tipi, ana tanı, gezici hizmet, mevcut aile hekimi, adres ve telefon bilgileri bulunmaktadır. Kişi bilgileri ekranında ise kimlik numarası, ad, soyad, doğum tarihi, cinsiyet, hasta tipi, adres, telefon ve mevcut AH bilgileri bulunmaktadır.

Bebek çocuk izlem bilgilerine göre yapılan sorgulama ekranları: Bebek çocuk izlem ekranında bebek çocuk izlem bilgileri, kişi bilgileri, otizm spektrum bozukluğu tarama ve takip bilgileri, okul çağı gençlik sağlığı işlemleri, 0-6 yaş çocukluk dönemi görüşmeleri ekranları bulunmaktadır (Görsel 32).



Görsel 32. Bebek çocuk izlem bilgilerine göre istatistiksel sorgulama ekranı

Bebek çocuk izlem bilgileri ekranında işlem zamanı, kimlik numarası, ad, soyad, cinsiyet, doğum tarihi, ağırlık, boy, boy persentil, baş çevresi D vitamini desteği, demir

desteği, topuk kanı, görme tarama sonucu, topuk kanı tarihi, GGK (Gaitada Gizli Kan) tarama sonucu, hemoglobin, hematokrit, bebeğin beslenme durumu ve tarama sonuçları bilgileri bulunmaktadır (Görsel 32).

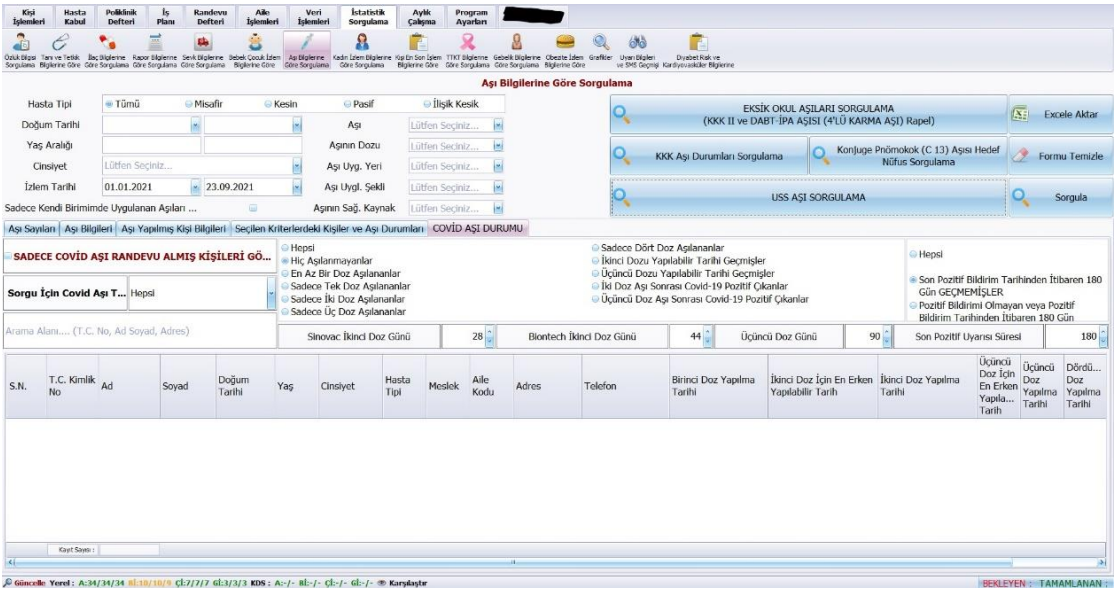
Kişi bilgileri ekranında kimlik numarası, ad, soyad, doğum tarihi, cinsiyet, adres ve telefon bilgileri bulunmaktadır.

Otizm spektrum bozukluğu tarama ve takip bilgileri ekranında kimlik numarası, ad, soyad, cinsiyet, doğum tarihi, işlem zamanı, aile hekimi görüşü, otizm durumu, diğer tanı, irtibat kişi, irtibat telefon ve yaş (ay) bilgileri bulunmaktadır.

Okul çağı gençlik sağlığı işlemleri ekranında işlem zamanı, kaçıncı izlem, kimlik numarası, ad, soyad, cinsiyet, doğum tarihi, görme taraması, okul çağı postür, hemoglobin, hemotokrit, danışmanlık ve muayene not bilgileri bulunmaktadır.

Sıfır-altı yaş çocukluk dönemi görüşmeleri ekranında işlem zamanı, kimlik numarası, ad, soyad, cinsiyet, doğum tarihi, adres ve telefon bilgileri bulunmaktadır.

Aşı bilgilerine göre sorgulama ekranları: Aşı bilgilerine göre yapılan sorgulamada aşı sayıları, aşı bilgileri, aşı yapılmış kişi bilgileri ve aşı durumları ile Covid aşı durumu başlıklarına yönelik bilgiler bulunmaktadır. Eksik okul aşı bilgileri, KKK (kızamık, kızamıkçık ve kabakulak) aşı durumları, konjuge pnömokok aşısı hedef nüfus sorgulama ve USS aşı sorgulama işlemleri bu ekran üzerinden yapılmaktadır (Görsel 33).



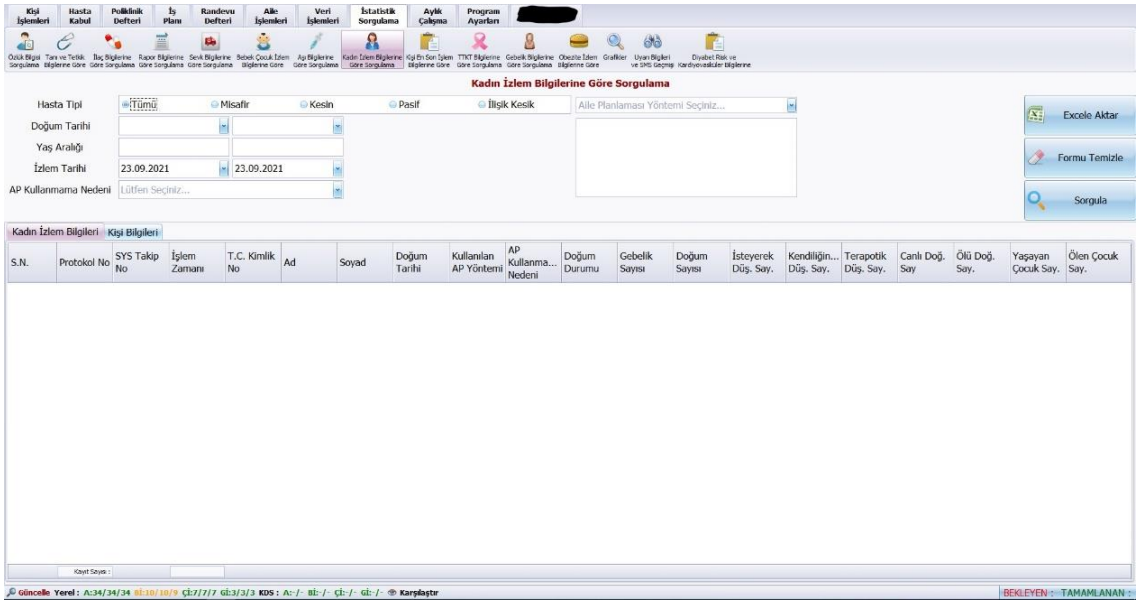
Görsel 33. Aşı bilgilerine göre istatistiksel sorgulama ekranı

Aşı sayıları ekranında aşı adı, aşı dozu ve aşı adedi bilgileri bulunmaktadır.

Aşı bilgileri ekranında işlem zamanı, kimlik numarası, ad, soyad, cinsiyet, doğum tarihi, aşı, aşı dozu, uygulama yeri, uygulama şekli, sağlandığı kaynak ve uyruk bilgileri vardır. Aşı yapılmış kişi bilgileri ekranında kimlik numarası, ad, soyad, cinsiyet, adres ve telefon numarası bilgileri bulunmaktadır. Seçilen kriterdeki kişiler ve aşı durumları ekranında kimlik numarası, ad, soyad, cinsiyet, adres, telefon numarası ve kişiye yapılmış aşıların bilgileri yer almaktadır.

Covid aşı durumu ekranında kimlik numarası, ad, soyad, cinsiyet, doğum tarihi, yaş, cinsiyet, gebe lohusa durumu, hasta tipi, meslek, aile kodu, adres, telefon, birinci doz yapılma tarihi, ikinci doz için en erken yapılabilir tarih, ikinci doz yapılma tarihi, üçüncü doz için en erken yapılma tarihi, üçüncü doz yapılma tarihi, dördüncü doz yapılma tarihi, temas bildirim tarihi ve temaslı tipi bilgileri bulunmaktadır.

Kadın izlem bilgilerine göre sorgulama ekranları: Kadın izlem bilgilerine göre yapılan istatistiksel sorgulama ekranında işlem zamanı, kimlik numarası, ad, soyad, doğum tarihi, kullanılan AP yöntemi, AP kullanma nedeni, doğum durumu, gebelik sayısı, doğum sayısı, isteyerek düşük sayısı, kendiliğinden düşük sayısı, terapotik düşük sayısı, canlı doğum sayısı, ölü doğan sayısı, yaşayan çocuk sayısı ve ölen çocuk sayısı bilgileri bulunmaktadır (Görsel 34).



Görsel 34. Kadın izlem bilgilerine göre istatistiksel sorgulama ekranı

TKT (Toplum Tabanlı Kanser Tarama) bilgilerine göre sorgulama ekranları: TTKT bilgilerine göre yapılan sorgulamada TTKT izlem bilgileri, GGK taraması hedef nüfus, HPV taraması hedef nüfus, meme taraması hedef nüfus ve HPV testi yapılıp TTKT yapılmayanlar ekranları bulunmaktadır.

TTKT izlem bilgileri ekranında işlem zamanı, kimlik numarası, ad, soyad, cinsiyet, GGK testi, kolon görüntüleme yöntemi, HPV testi, PapSmear testi, serviks sitoloji, mamografi, mamografi sonucu, KKMM (kendi kendine meme muayenesi), KMM (klinik meme muayenesi), şimdiki yaşı, işlem zamanındaki yaşı, adres, telefon ve medeni hali bilgileri bulunmaktadır.

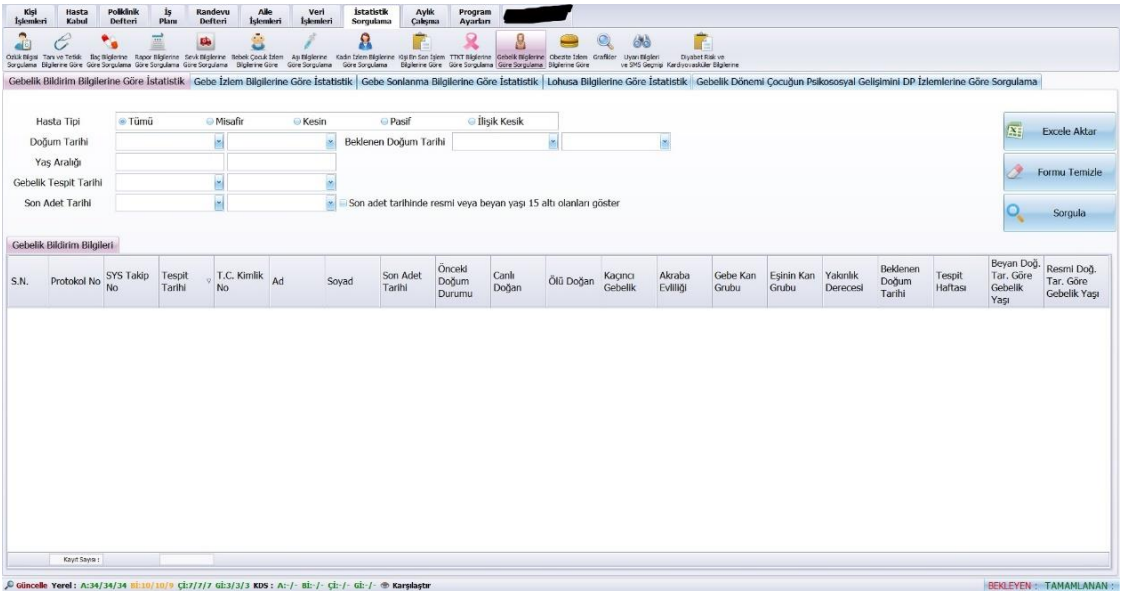
GGK taraması hedef nüfus ekranında kimlik numarası, ad, soyad, doğum tarihi, yaş, cinsiyet, işlem zamanı, GGK sonucu, adres, telefon ve medeni hali bilgileri bulunmaktadır.

HPV taraması hedef nüfus kimlik numarası, ad, soyad, işlem zamanı, yaş, doğum tarihi, cinsiyet, anne adı, baba adı, HPV sonucu, adres, telefon ve medeni hali bilgileri bulunmaktadır.

Meme taraması hedef nüfus ekranında kimlik numarası, ad, soyad, doğum tarihi, yaş, cinsiyet, işlem zamanı, mamografi, adres, telefon ve medeni hali bilgileri bulunmaktadır.

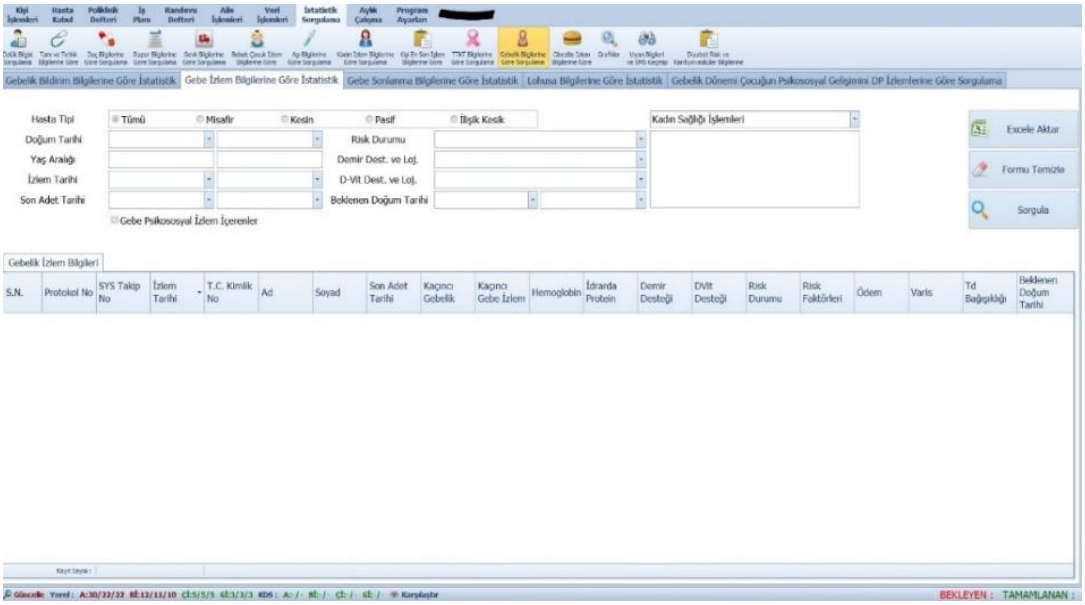
HPV testi yapılıp TTKT yapılmayanlar ekranında kimlik numarası, ad, soyad, doğum tarihi, cinsiyet, HPV işlem zamanı, sonuç ve kayıt durumu bilgileri bulunmaktadır.

Gebelik bilgilerine göre sorgulama ekranları: Gebelik bilgilerine göre istatistiksel sorgulama yapıldığında, gebelik bildirim bilgilerine göre, gebe izlem bilgilerine göre, gebe sonlanma bilgilerine göre, lohusa bilgilerine göre ve gebelik dönemi çocuğun psikososyal gelişimini DP (Destekleme Programı) izlemlerine göre sorgulama yapılarak hastalar listelenmektedir (Görsel 35).



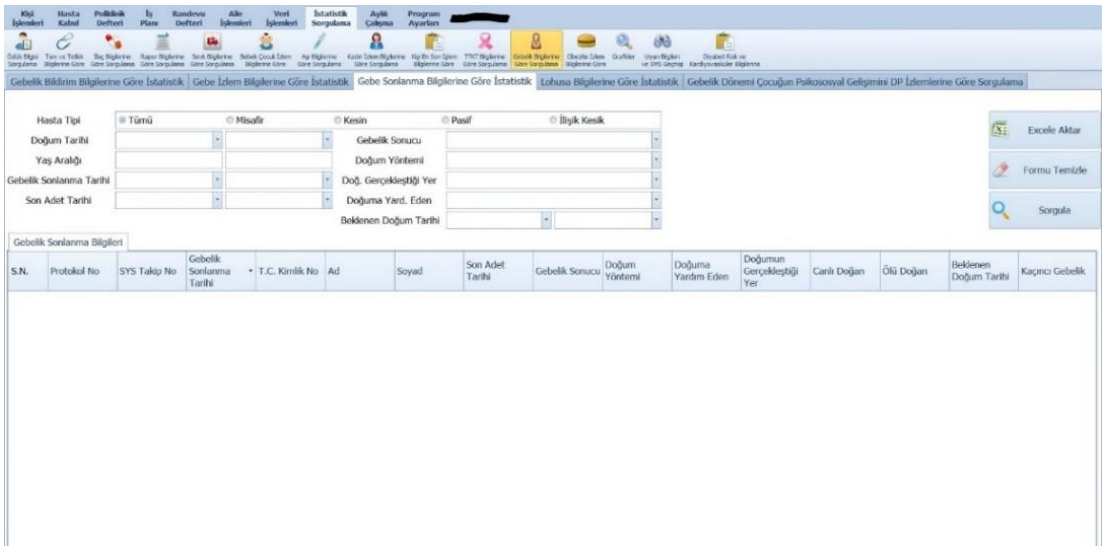
Görsel 35. Gebelik bildirimine göre istatistik hesaplama ekranı

Gebelik bildirimine göre yapılan istatistiksel sorgulama ekranında gebelik tespit tarihi, kimlik numarası, ad, soyad, son adet tarihi, önceki doğum durumu, canlı doğan, ölü doğan, kaçıncı gebelik, akraba evliliği, gebe kan grubu, eşinin kan grubu, yakınlık derecesi, beklenen doğum tarihi, tespit haftası ve beyan edilen doğum tarihine göre gebelik yaşı ile resmi doğum tarihine göre gebelik yaşı bilgileri bulunmaktadır. Ekran üzerinde bilgilerin Excel'e aktarılabileceği bir seçenek de mevcuttur.



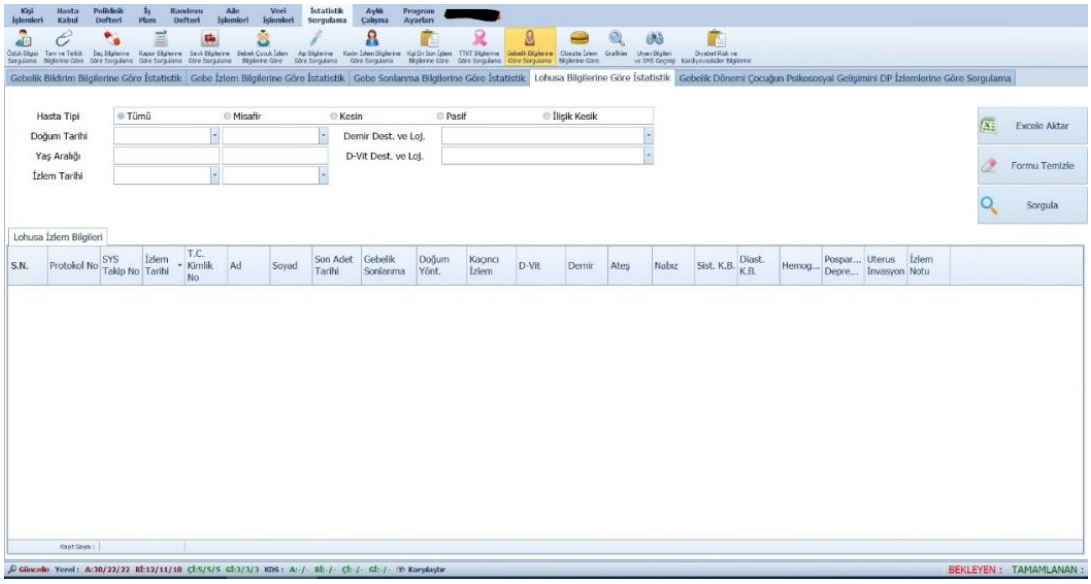
Görsel 36. Gebe izlem bilgilerine göre istatistiksel sorgulama ekranı

Gebe izlem bilgilerine göre yapılan istatistik sorgulamada, izlem tarihi, kimlik numarası, ad, soyad, son adet tarihi, kaçıncı gebelik, kaçıncı gebe izlem, hemoglobin, idrarda protein, demir desteği, D vitamini desteği, risk durumu, risk faktörleri, ödem, varis, Td (tetanoz-difteri aşısı) bağışıklığı ve beklenen doğum tarihi bilgileri bulunmaktadır (Görsel 36).



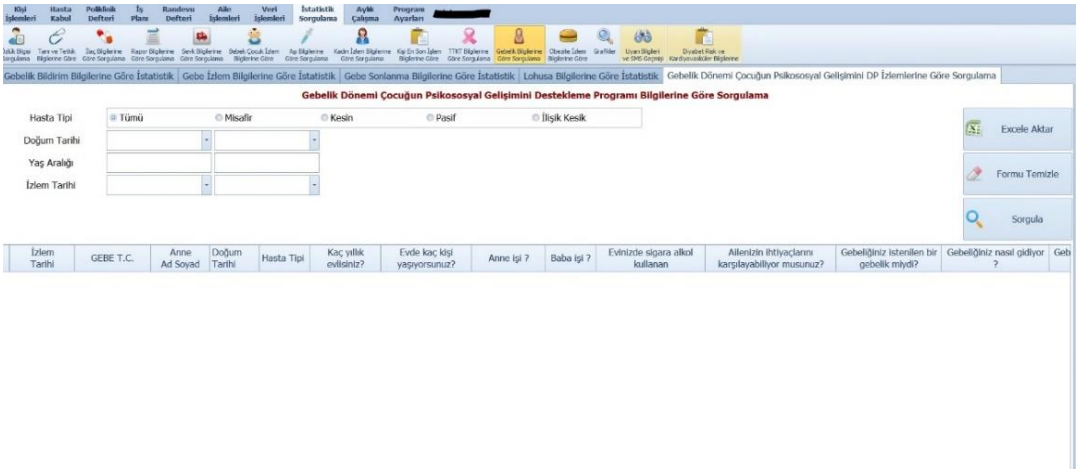
Görsel 37. Gebe sonlanma bilgilerine göre istatistik sorgulama ekranı

Gebe sonlanma bilgilerine göre yapılan istatistik sorgulama ekranında gebelik sonlanma tarihi, kimlik numarası, ad, soyad, son adet tarihi, gebelik sonucu, doğum yöntemi, doğuma yardım eden, doğumun gerçekleştiği yer, canlı doğan, ölü doğan, beklenen doğum tarihi ve kaçıncı gebelik olduğu bilgileri bulunmaktadır (Görsel 37).



Görsel 38. Lohusa bilgilerine göre istatistik sorgulama ekranı

Lohusa bilgilerine göre yapılan istatistik sorgulamada izlem tarihi, kimlik numarası, ad, soyad, son adet tarihi, gebelik sonlanma, doğum yöntemi, kaçıncı izlem, D vitamini, demir, ateş, nabız, sistolik kan basıncı, diastolik kan basıncı, hemoglobin, pospartum depresyon, uterus invasyon ve izlem notu bilgileri bulunmaktadır (Görsel 38).



Görsel 39. Gebelik dönemi çocuğun psikososyal gelişimini DP izlemlerine göre istatistik sorgulama ekranı

Gebelik dönemi çocuğun psikososyal gelişimini DP izlemlerine göre yapılan istatistik sorgulama ekranında, izlem tarihi, gebe T.C. kimlik numarası, anne adı ve soyadı, doğum tarihi ve hasta tipi bilgileri bulunmaktadır. Ayrıca "kaç yıllık evlisiniz?", "evde kaç kişi yaşıyorsunuz?", "anne işi?", "baba işi?", "evinizde sigara alkol kullanan, ailenizin ihtiyaçlarını karşılayabiliyor musunuz?", "gebeliğiniz istenilen bir gebelik

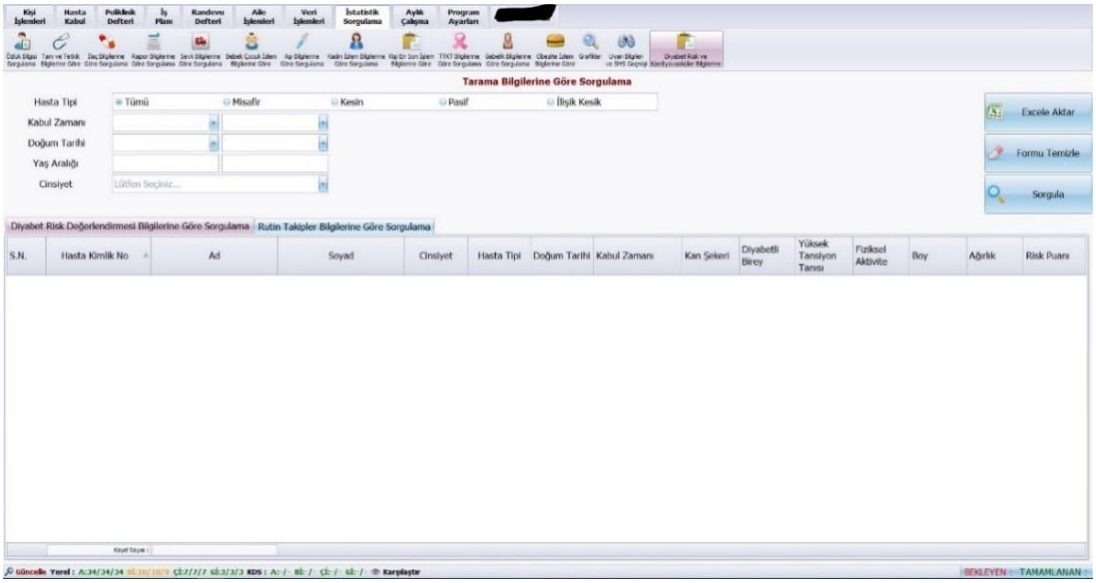
miydi?", "gebeliğiniz nasıl gidiyor?", "nasıl besleniyor, neye dikkat ediyorsunuz?"", son bir haftada aşırı mutsuz hissettiniz mi?", "gebelik sonrası aile planlaması düşünüyor musunuz?", "endişeli ya da kaygılı hissediyor musunuz?", "ne kadar süre ile anne sütü vermeyi planlıyorsunuz?1.görüşme", "ne kadar süre ile anne sütü vermeyi planlıyorsunuz?2.görüşme", "gebede/babada ruhsal bozukluk var mı?1.görüşme" ve "gebede/babada ruhsal bozukluk var mı?2.görüşme" soruları bulunmaktadır (Görsel 39).

Obezite izlem bilgilerine göre sorgulama ekranı: Obezite izlem bilgilerine göre yapılan sorgulama, muayene bilgileri ve kişi bilgilerine göre listelenmektedir. Muayene bilgileri ekranında işlem zamanı, hasta kimlik numarası, ad, soyad, doğum tarihi, cinsiyet, boy, kilo, bel çevresi, kalça çevresi, BKI (beden kitle indeksi), adres, telefon ve kişinin kronik hastalık bilgileri bulunmaktadır. Kişi bilgileri ekranında hasta kimlik numarası, ad, soyad, doğum tarihi, cinsiyet, hasta tipi, adres ve telefon bilgileri bulunmaktadır.

Grafikler ekranı: Grafikler ekranında nüfus piramidi, işlem sayıları grafiği, kadın dağılım grafiği (15 altı, 15-49 kadın, gebe, lohusa, 49 üzeri) ve özlük bilgileri (medeni hali, öğrenim durumu, sosyal güvence durumu, kan grubu, özürlülük durumu, gezici hizmet, sigara kullanımı, alkol kullanımı, madde kullanımı, ameliyat geçmişi, yaralanma geçmişi) grafikleri bulunmaktadır.

Uyarı bilgileri ve SMS geçmişi ekranı: Uyarı bilgileri ve SMS geçmişi ekranında uyarı eklenmiş kişi listesi ve SMS gönderme geçmişi bilgileri listelenmektedir. Uyarı eklenmiş kişi listesi ekranında hasta kimlik no, ad, soyad, cinsiyet, hasta tipi, doğum tarihi, aile kodu, uyarı tipi, uyarı, gösterimi zorunlu, aile uyarısı, uyarı tarihi, adres ve telefon bilgileri bulunmaktadır. SMS gönderme geçmişi ekranında gönderim tarihi, hasta kimlik no, ad, soyad, anne kimlik no, telefon, pasaport ve SMS içeriği bilgileri bulunmaktadır.

Diyabet risk ve kardiyovasküler bilgilerine göre sorgulama ekranı: Diyabet risk ve kardiyovasküler bilgilerine göre sorgulama ekranında diyabet risk değerlendirmesi bilgilerine göre sorgulama yapılmakta ve rutin takip bilgilerine göre hastalar listelenmektedir (Görsel 40).



Görsel 40. Diyabet risk ve kardiyovasküler bilgilere göre istatistik sorgulama ekranı

Diyabet risk değerlendirmesi bilgilerine göre yapılan sorgulama ekranında hasta kimlik numarası, ad, soyad, cinsiyet, hasta tipi, doğum tarihi, kabul zamanı, kan şekeri, diyabetli birey, yüksek tansiyon, fiziksel aktivite, boy, ağırlık ve risk puanı bilgileri bulunmaktadır.

Rutin takip bilgilerine göre yapılan sorgulama ekranında ise hasta kimlik numarası, ad, soyad, cinsiyet, hasta tipi, doğum tarihi, kabul zamanı, nabız, sistolik kan basıncı, diastolik kan basıncı, açlık kan şekeri, tokluk kan şekeri, takip not, ateş, gezici hizmet, total kolesterol, sigara kullanımı ve kardiyovasküler risk skor bilgileri bulunmaktadır.

Aylık çalışma ekranı: Bu ekranda Aile Hekimliği izleme değerlendirme şubesi aylık çalışma formları, anne-çocuk sağlığı ve aile planlaması ile ilgili aylık çalışma formları bulunmaktadır.

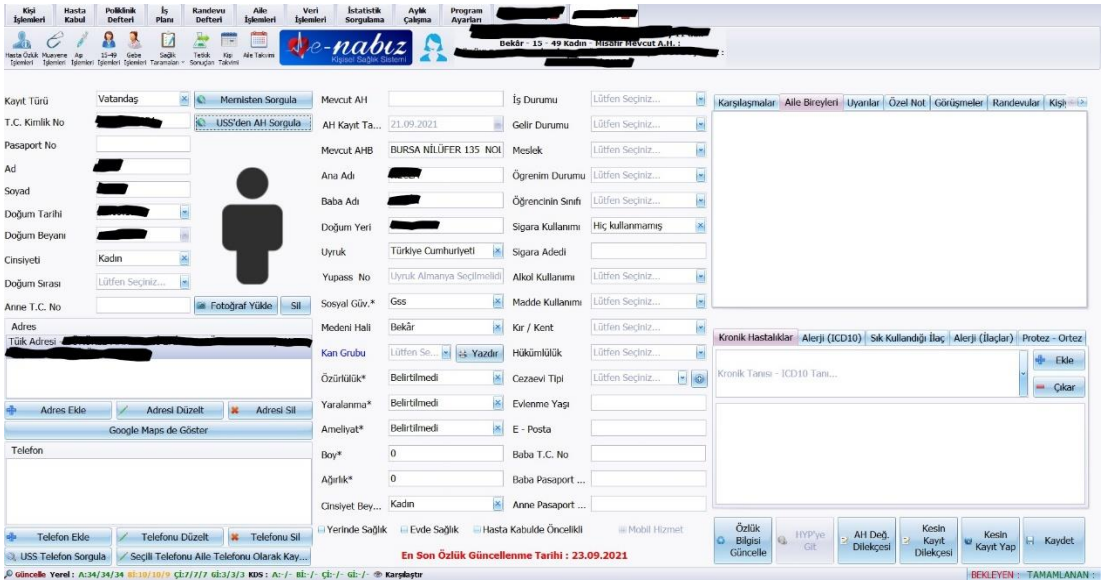
Program ayarları ekranı: Bu ekranda kullanıcı bilgileri, program tercihleri, güncelleme detayları, veri tabanı yedek alma işlemleri, veri tabanı geri yükleme işlemleri ve veri tabanı bakımı işlemleri yapılmaktadır.

Kullanıcı bilgileri ekranında aile hekimleri ile ilgili bilgiler bulunmaktadır. Aile hekiminin rolü, T.C. kimlik numarası, unvanı, adı, soyadı ve aktif olup olmadığı bilgilerinin yanı sıra branşı, telefon, e-posta, diploma tescil numarası, sertifika numarası, il, ilçe, TSM adı, ASM adı, AH birim adı, program şifresi, şifre hatırlama,

USS şifresi, SGK medula şifresi ve kullanıcı aktif bilgileri bulunmaktadır. Ayrıca program ayarları ekranında hasta kabul ayarları, servis bekleme süreleri ve form tercihleri, takvim ve uyarı paneli ayarları, muayene ayarları, renkli reçete ayarları, kişi listesi ve görünüm ayarları yapılabilmektedir. Aile hekimi ile ilgili vekalet bilgileri de bu ekrandadır.

4.2.2.2.Hasta ekranları

Hasta özlük işlemleri ekranı: Bu ekranda hastanın kimlik numarası, pasaport numarası, ad, soyad, doğum tarihi, doğum beyanı, cinsiyeti, doğum sırası, anne ve baba adı, doğum yeri, uyruk ve medeni halinin kaydedilebildiği kimlik bilgileri ile kan grubu, adres bilgileri, iletişim bilgileri, öğrenim ve meslek bilgisi ve anne-babanın T.C. kimlik numarası ile pasaport numarası bilgileri bulunmaktadır (Görsel 41).

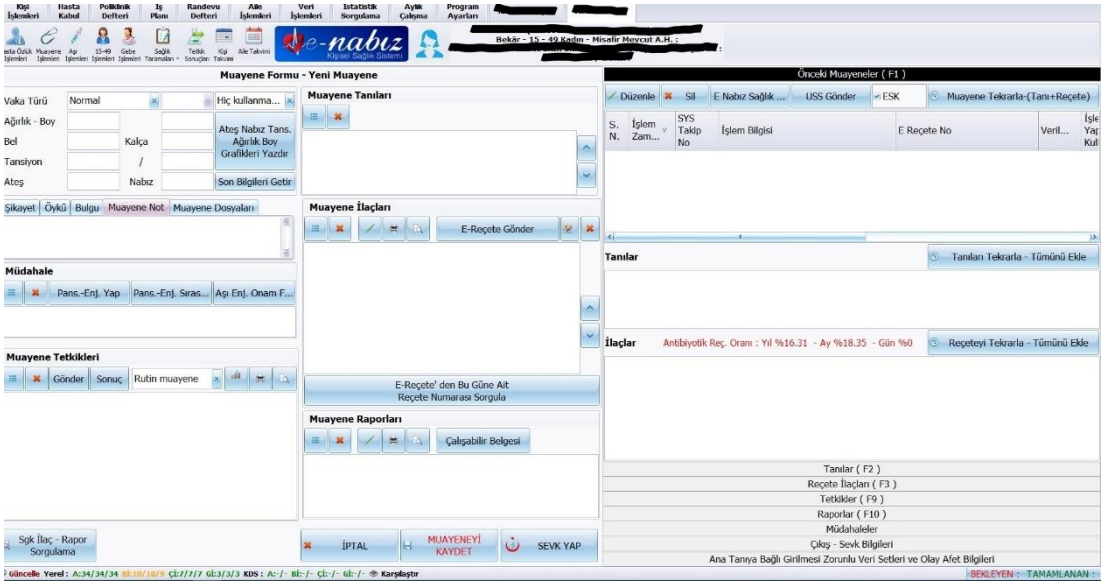


Görsel 41. Kayıtlı hastanın özlük bilgileri ekranı

Kayıtlı hastanın sigara, alkol ve madde kullanımı, hükümlülük durumu, hükümlüyse cezaevi tipi, evlenme yaşı, boy, ağırlık, özürlülük, yaralanma, GSS bilgileri ile kronik hastalık bilgisi, alerji, sık kullanılan ilaçları ve alerji ilaç bilgileri de bu ekranda bulunmaktadır. Hastayla ilgili Aile hekiminin özel muayene notları da bu ekrana kaydedilebilmektedir (Görsel 41).

Muayene işlemleri ekranı: Bu ekranda vaka türü, ağırlık, boy, kaçla, tansiyon, ateş, nabız, muayene tanıları, muayene ilaçları, müdahale, muayene tetkikleri, muayene raporları, şikayet, öykü, bulgu, muayene dosyaları ve notu kaydedilebilmektedir. Bu

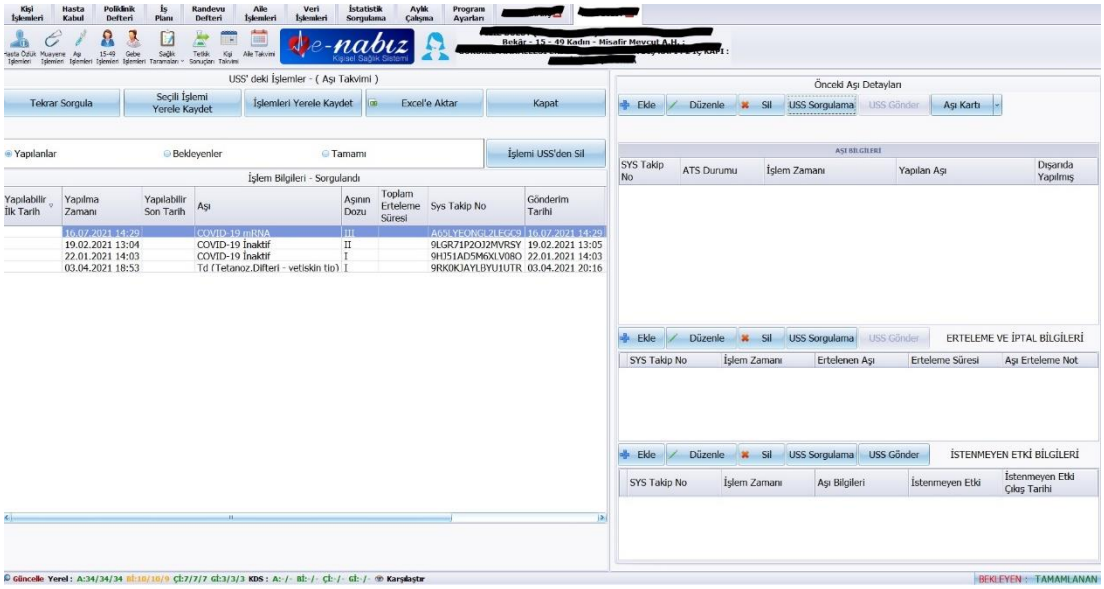
ekranda hastanın SGK ilaç ve rapor bilgileri sorgulanabilirken, hastanın geçmiş muayene bilgileri de görüntülenebilmektedir (Görsel 42).



Görsel 42. Muayene formu ekranı

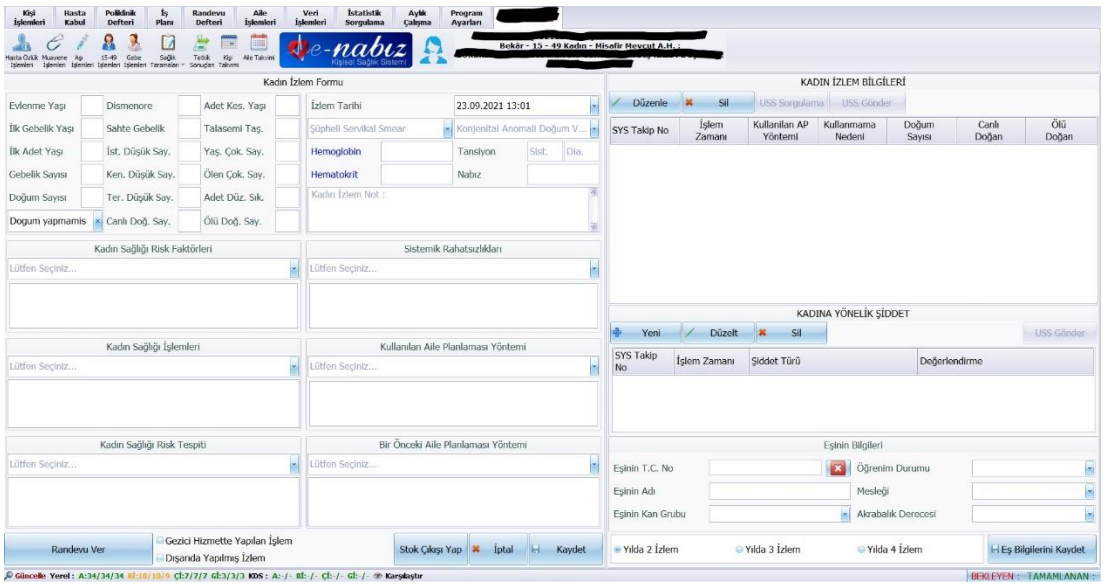
Muayene formu ekranında ayrıca e-Nabız kişisel sağlık kayıt sistemine erişim sağlanabilirken, 'USS gönder' butonu ile hastanın muayene bilgileri Sağlık Bakanlığı'na gönderebilmektedir (Görsel 42).

Aşı işlemleri ekranı: Bu ekranda, hastanın hangi aşıyı hangi tarihte yaptırdığı bilgilerine yer verilmektedir. Hastanın önceki aşı detayları USS'den sorgulanabilmektedir. Aşı ile ilgili erteleme ve iptal bilgileri ile aşının yan etkilerine dair bilgiler de bu ekrana kaydedilebilmektedir (Görsel 43).



Görsel 43. Aşı işlemleri ekranı

15-49 işlemleri ekranı: Bu ekranda 15-49 yaş kadınların izlemleri yapılmaktadır. Kadınların evlenme yaşı, ilk gebelik yaşı, ilk adet yaşı, gebelik sayısı, doğum sayısı, dismenore, sahte gebelik, düşük sayısı bilgileri, canlı doğum sayısı, adet kesilme yaşı, isteyerek düşük sayısı, kendiliğinden düşük, teratojenik düşük sayısı (hastalığa bağlı), canlı doğum sayısı, adet kesilme yaşı, talasemi taşıyıcılığı, yaşayan çocuk sayısı, ölen çocuk sayısı, adet düzeni sıklığı ve ölü doğum sayısı bilgileri bulunmaktadır (Görsel 44).



Görsel 44. Kadın (15-49 işlemleri) izlem işlemleri ekranı

Ayrıca izlem ile ilgili olarak, izlem tarihi, şüpheli servikal smear bilgisi, konjenital anomali doğum verileri, hemoglobin, hematokrit, tansiyon ve nabız bilgileri ile ilgili hekimin izlem notu yer almaktadır (Görsel 44).

Kadının sistemik rahatsızlıkları, kullandığı aile planlaması (hap, kondom, ria, deri altı implant vs.) yöntemi ve bir önceki aile planlaması yöntemi bu ekrana kaydedilebilmektedir (Görsel 44).

Kadın sağlığı işlemlerinde, üreme sağlığı danışmanlığı, beslenme danışmanlığı, emzirme danışmanlığı, diş sağlığı danışmanlığı, kendi kendine meme muayenesi eğitimi, klinik meme muayenesi, menopoz danışmanlığı ve servikal smear (pap smear) bilgileri de bu ekranda bulunmaktadır (Görsel 44).

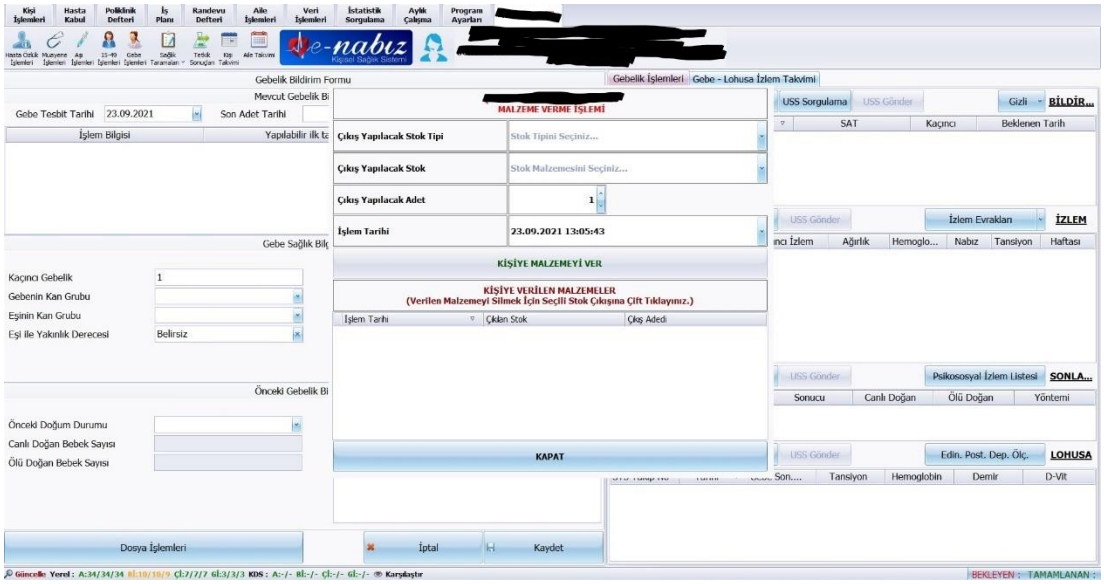
Kadın sağlığı risk faktörleri adet düzensizliği, kardiovasküler hastalıklar, psikiyatrik hastalıklar ve solunum sistemi hastalıkları seçenekleri ile hesaplanabilmektedir. Ayrıca 18 yaş altı gebelik, 35 yaş üstü gebelik, dört veya daha fazla doğum yapanlar, son doğum yapalı iki aydan az olanlar, sistemik hastalığı olanlar, adet düzensizliği olanlar, şüpheli PAP Smear, memede şüpheli kitle, kalıtsal hastalıklar, anemi ve sigara kullanıp kullanmadığı bilgilerine göre risk tespiti yapılabilmektedir (Görsel 44).

Son olarak bu ekran üzerinde kadına yönelik şiddet ile ilgili bir bölüm vardır. Burada kadına uygulanan şiddetin türü (sözlü veya fiziksel şiddet), kadının eşinin T.C. numarası, eşinin adı, kan grubu, öğrenim durumu, mesleği ve akrabalık derecesi bilgileri yer almaktadır (Görsel 44).

Gebe işlemleri ekranı: Bu ekranda gebe tespit tarihi, mevcut gebelik bilgisi, son adet tarihi, kaçıncı gebelik bilgisi, gebenin kan grubu, eşinin kan grubu, eşi ile yakınlık derecesi, önceki gebelik bildirimi, önceki doğum durumu, canlı doğan bebek sayısı ve ölü doğan bebek sayısı bilgileri bulunmaktadır.

Gebe hastaya verilen malzeme işlemleri bu ekran üzerinden yapılmaktadır. Kadın sağlığı ile ilgili preparatlar (Demir preparatı, D vitamini preparatı, Decavit) ve bebek çocuk sağlığı preparatları (Demir preparatı, D vitamini preparatı) bu ekrana kaydedilmektedir. Bu preparatlarının hastaya ücretsiz olarak, hangi tarihte kaç adet verildiği bilgileri aile hekimi tarafından kaydedilmektedir. Ayrıca yapılan aşı

(Kızamık Kabakulak Kızamıkçık, Difteri, Tetanoz, aBoğmaca, iPolio, Hib, Suçiçeği, Hepatit A, Konjuge Pnömokok Aşısı, Tetanoz, Difteri, Hepatit B, Opa, Bcg) bilgileri bu ekrandadır (Görsel 45).



Görsel 45. Gebelik bildirim ekranı

Gebelik bildirimi yapılan hastanın izlemi de bu ekranda yapılmaktadır. İzlem sürecinde gebe kadının kaçıncı izlemi olduğu, ağırlık, hemoglobin, nabız, tansiyon ve gebelik haftası bilgileri yer almaktadır (Görsel 45).

Gebe-Lohusa izlem takvimi ekranında hekimin zorunlu olarak yapması gereken toplam dört izlem görüntülenmektedir. Gebelik izlemlerinde fetal kalp atımı, boy, kilo, tansiyon ve ilaç kullanım bilgileri yer almaktadır. Ayrıca gebenin psikososyal izlem listesi de kayıt altına alınabilmektedir. Bu izlem ekranında canlı doğan, ölü doğan ve doğum yöntemi bilgileri bulunmaktadır (Görsel 45).

Sağlık taramaları ekranları: Sağlık taramaları ekranlarında özellikli izlem, kişinin e-raporları, kişiye malzeme verme, hemoglobinopati taraması, MHRS randevu işlemleri, toplum tabanlı kanser tarama, gebe izlem bildirim tutanağı, HPV taraması, rutin takipler, obezite takibi, RS20 bildirim ve takipler, yetişkin aşı takvimi, aile planlaması defteri işlemleri, evde sağlık, pansuman enjeksiyon, halk eğitim, diyabet takipleri ve okul çağı çocuk/gençlik sağlığı izlemlerinin yapıldığı ekranlar bulunmaktadır.

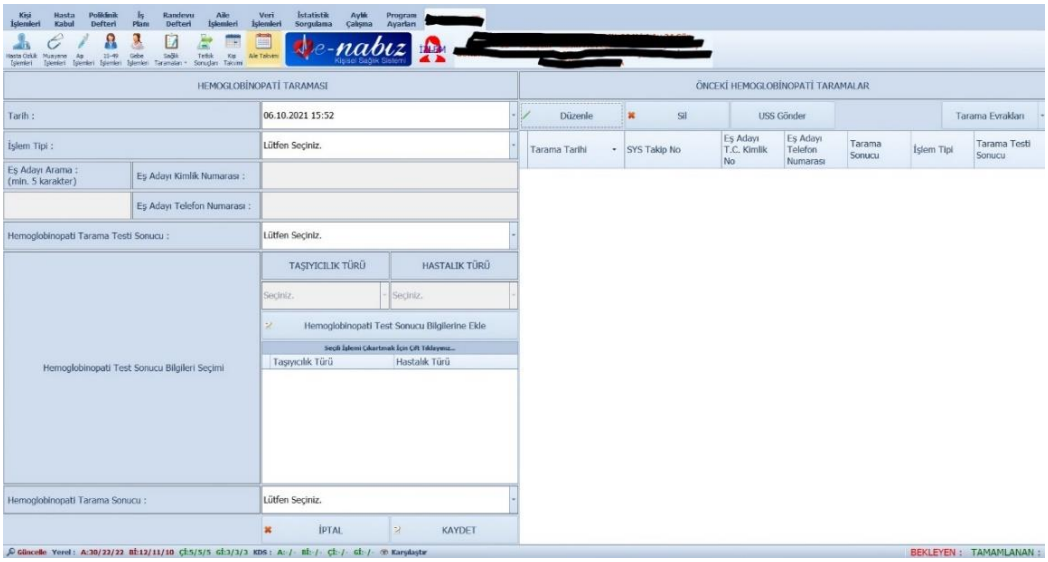
Özellikli izlem ekranı: Özellikli veya öncelikli izlem ekranında hastaya ait izlem bilgileri vardır. İzlem yapılıp yapılmadığı, yapılamadıysa gerekçesi (iletişim numarasına ulaşılamaması, kişinin bilgi vermemesi vb.), beyana dayalı işlem olup olmadığı bilgisi ve muayene bilgileri bulunmaktadır.

Muayeneye dair ateş, öksürük, nefes darlığı, baş ağrısı, kas ağrısı, tat koku kaybı ve ishal bilgileri ile numune alınıp alınmadığı, alınamadıysa gerekçesine dair bilgiler bulunmaktadır. Ekranda ayrıca önceki izlem bilgileri de listelenmektedir. Önceki izlemler, tarama tarihi, telefon, izlem yapılıp yapılmadığı, yapılmama nedeni, yapılmama açıklaması, beyana dayalı, izlem notu, semptom, ateş, öksürük, nefes darlığı olup olmadığı bilgileri, numune alınıp alınmadığı bilgisi, numune alınmadıysa alınmama nedeni, semptom açıklama, baş ağrısı, kas ağrısı, tat koku kaybı ve ishal bilgilerine göre listelenmektedir. Bu ekran pandemi döneminde Covid-19 hastaları için kullanılmaktadır.

Kişinin e-raporları ekranı: Bu ekranda, e-rapor oluşturma tarihi, rapor tipi (sürücü raporu, durum bildirir tek hekim sağlık raporu, askerlik raporu, sporcu raporu, yatağa bağlı seçmenler için durum bildirir tek hekim sağlık raporu, bütün raporlar), verilme sebebi ve raporu veren doktorun kimlik numarası bilgileri yer almaktadır.

"Kişiye malzeme ver" ekranı: Birinci basamak sağlık hizmetleri kapsamında hastalara aile planlaması malzemeleri, kadın sağlığı preparatları ve çocuk sağlığı preparatları ücretsiz olarak verilmektedir. Verilen malzemelerin hangi tarihte verildiği ve stok bilgileri bu ekrana kaydedilmektedir.

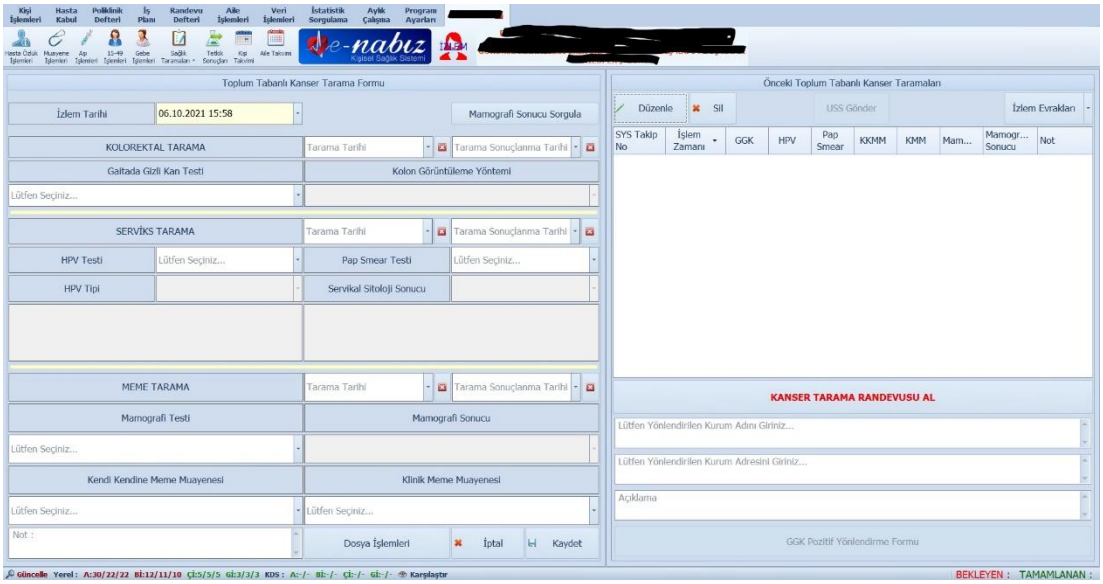
Hemoglobinopati tarama ekranı: Bu ekranda yapılacak işlemler tarih, işlem tipi (evlilik öncesi taraması, evlilik öncesi tarama dışı işlem), eş adayı kimlik numarası ve telefon numarası, tarama testinin sonucu, taşıyıcılık türü ve hastalık türü bilgilerine göre gerçekleştirilmektedir. Ayrıca önceki hemoglobinopati tarama sonuçları da bu ekranda listelenmektedir. Bu ekrana kaydedilen bilgiler Ulusal Sağlık Sistemine gönderilmektedir (Görsel 46).



Görsel 46. Hemoglobinopati tarama ekranı

MHRS randevu işlemleri ekranı: Hızır AHBS, hasta için randevu oluşturmak veya oluşturulan randevuları görüntüleyebilmek için MHRS ile senkronize bir şekilde çalışmaktadır. Aile hekimi hastayı sevk edebilmek ve başka bir poliklinikten randevu oluşturabilmek için bu ekranı kullanmaktadır. Bu ekranda diğer hekimlerin randevu doluluk oranları da görüntülenebilmektedir.

Toplum tabanlı kanser tarama ekranı: Bu ekranda mamografi sonucu sorgulanmakta, kolorektal ve serviks tarama yapılmaktadır. Ekranda daha önceki toplum tabanlı kanser tarama bilgileri listelenmektedir (Görsel 47).



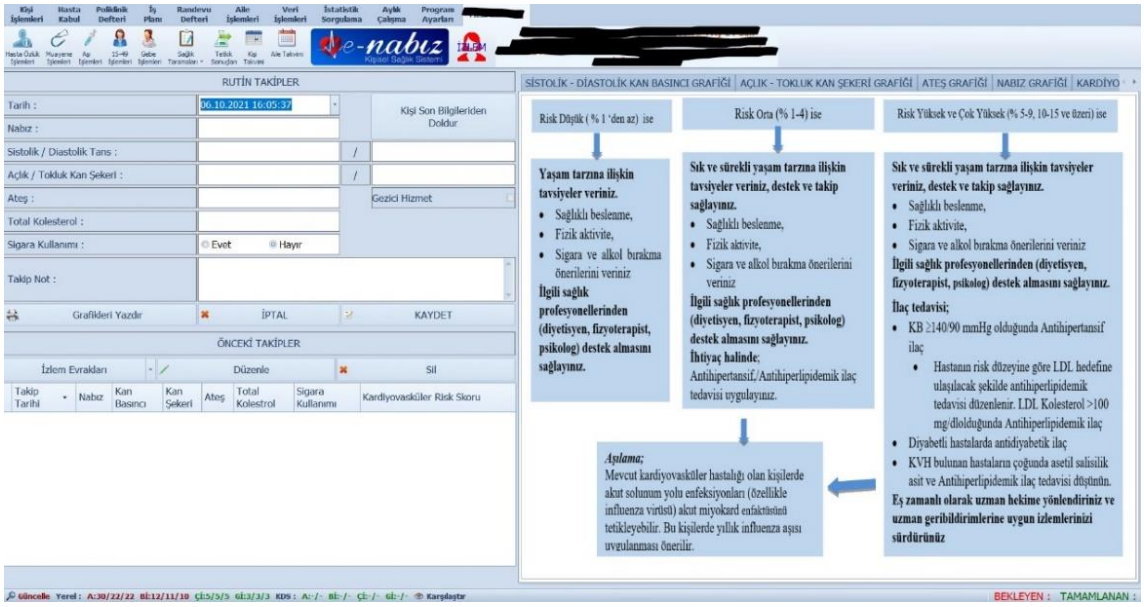
Görsel 47. Toplum tabanlı kanser tarama ekranı

Gebe izlem bildirim tutanağı ekranı[8]**:** Bu ekranda bildirimi yapılan gebe kadının izlem bilgileri bulunmaktadır.

HPV tarama ekranı: Bu ekranda HPV istemi yapılabilmekte ve HPV testi için işlem zamanı, barkod ve sonuç bilgileri bulunmaktadır.

Ekranda ayrıca HPV istem formu, HPV pozitif yönlendirme formu, yönlendiren kurum, kurum adresi ve başvuru usulü bilgileri yer almaktadır. Sağlık Net'e gönderilmiş HPV test bilgileri sorgulanabilmekte, yapılan sorgulama işlem tarihi, istem yapan kurum ve sonuç bilgisine göre listelenmektedir.

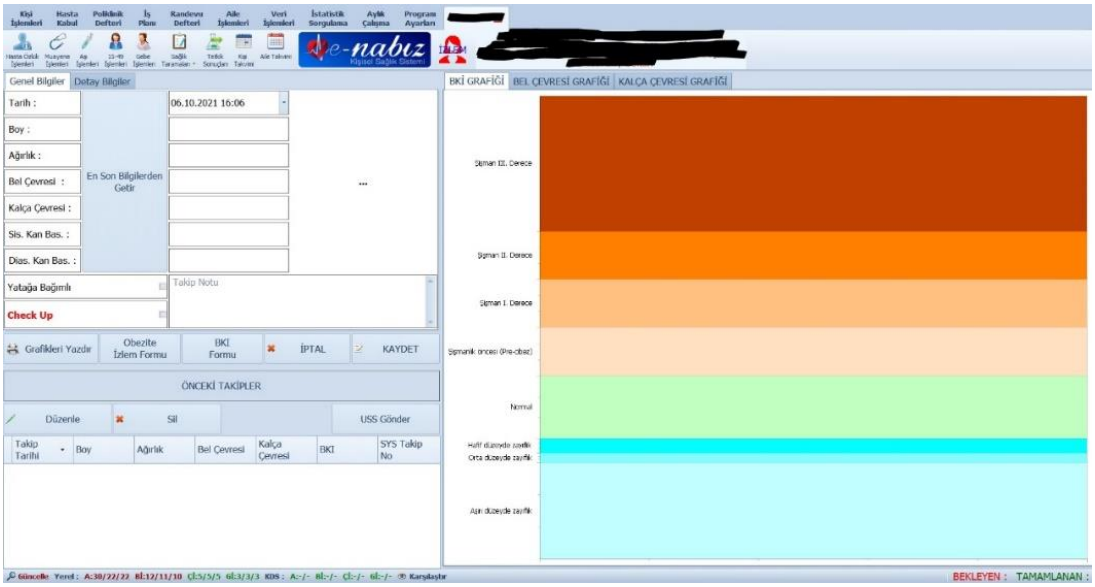
Rutin takipler ekranı: Hastanın rutin takiplerinin yapıldığı bu ekranda tarih, nabız, sistolik/diastolik tansiyon, açlık/tokluk kan şekeri, ateş, total kolesterol, sigara kullanımı ve takip notu bilgileri bulunmaktadır. Bu bilgiler grafik şeklinde de görüntülenebilmektedir (Görsel 48).



Görsel 48. Rutin takip ekranı

Obezite takip ekranı: Obezite takip ekranında obeziteli hastanın boy ağırlık, bel çevresi, kalça çevresi, BKI, sistolik ve diastolik kan basıncı, yatağa bağımlı olup olmadığı, Check Up bilgisi ve daha önceki izlem bilgileri bulunmaktadır (Görsel 49).

[8] Bu ekran "kişinin devam eden bir gebeliği yoktur" uyarısı nedeniyle incelenememiştir.



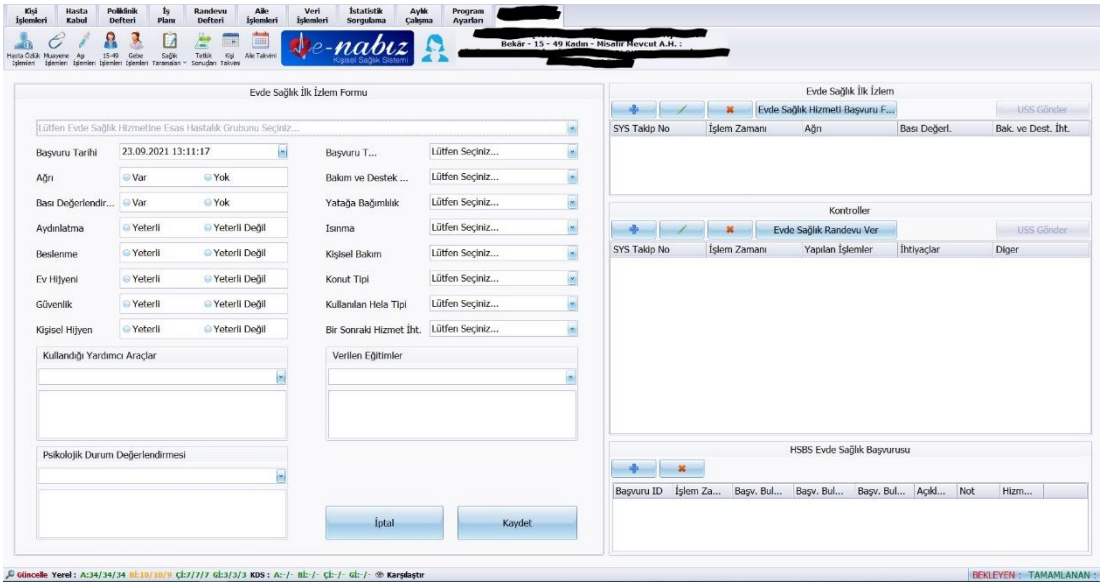
Görsel 49. Obezite takip ekranı

RS 20 bildirim ve takipler ekranı: RS 20 bildirim ve takip ekranı, ruh ve sinir hastalıkları hastanelerinden taburcu olan hastaların ayaktan takibinin yapılmasını sağlamak için kullanılmaktadır.

Yetişkin aşı takvimi ekranı: Yetişkin aşı takvimi ekranında aşı doz ve tarihine göre yetişkin aşı takvimi oluşturulmaktadır. Kişiye uygulanan aşılar, aşının yapıldığı tarih, aşı adı ve aşı dozu bilgileri bu ekranda listelenmektedir.

Aile planlaması defteri işlemleri ekranı: Bu ekranda aile planlaması ile ilgili bilgiler bulunmaktadır. Son üç ayda uygulanan korunma yöntemi, son gebelik sonlanma tarihi, son gebelik sonucu ve son adet tarihi bilgileri bu ekranda yer almaktadır.

Evde sağlık ekranı: Evde sağlık hizmetleri ile ilgili izlem bilgileri bu ekran üzerinden takip edilmektedir. Hastanın başvuru tarihi, ağrı bilgisi, bası değerlendirmesi, evin ısınma durumu, evin aydınlatması, konut tipi, kullanılan tuvalet tipi, ev hijyeni, güvenlik durumu, kişisel hijyen, hastanın beslenmesi, bakım ve destek ihtiyacı, yatağa bağımlılık durumu, kişisel bakım durumu, hastanın kullandığı yardımcı ilaçlar, hastanın psikolojik durumu, bir sonraki hizmet ihtiyacı ve verilen eğitimlerle ilgili bilgiler bu ekranda bulunmaktadır (Görsel 50).

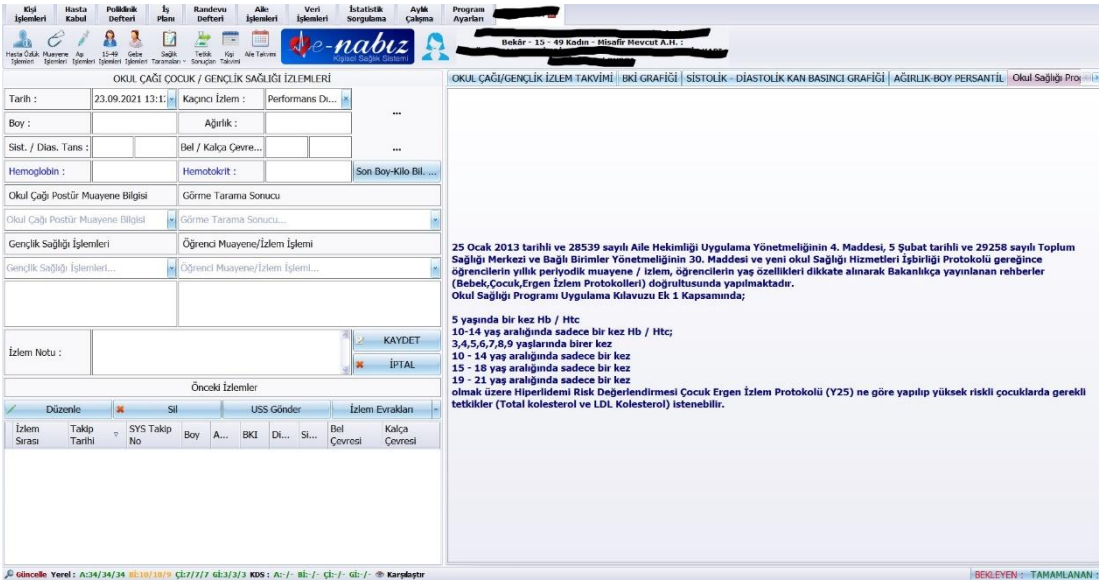


Görsel 50. Evde sağlık ilk izlem formu ekranı

Pansuman enjeksiyon ekranı: Bu ekranda reçeteyi düzenleyen hekim bilgisi, enjeksiyon ve pansuman bilgileri ile verilen ilaçlar ve aşı enjeksiyon onam formu bilgileri bulunmaktadır.

Halk eğitim ekranı: Bu ekranda eğitim türü, eğitim tarihi, eğitim süresi, verilen eğitimler ve mobil hizmette yapılan işlem bilgileri listelenmektedir.

Okul çağı çocuk/gençlik sağlığı izlemleri ekranı: Okul çağı çocuk veya gençlerin sağlığı ile ilgili izlemler bu ekran üzerinden yapılmaktadır. Çocukların sağlıkları ile ilgili boy, ağırlık, sistolik-diastolik kan basıncı, bel/kalça çevresi, hemoglobin, hemotokrit, son boy kilo bilgisi, okul çağı postür muayene ve görme tarama sonucu bilgileri bulunmaktadır. Gençlik sağlığı ve öğrenci muayene işlemleri ile ilgili bilgiler izlem notlarıyla birlikte bu ekrana kaydedilmektedir. Bu ekranda ayrıca okul çağındaki çocuklar için zorunlu aşı bilgileri bulunmaktadır (Görsel 51).

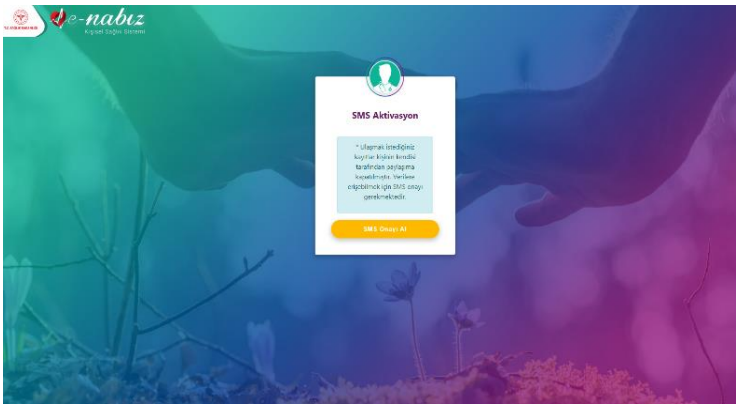


Görsel 51. Okul çağı/Gençlik sağlığı izlem formu ekranı

4.2.2.3.Hızır AHBS veri tabanından e-Nabız kaydına erişim

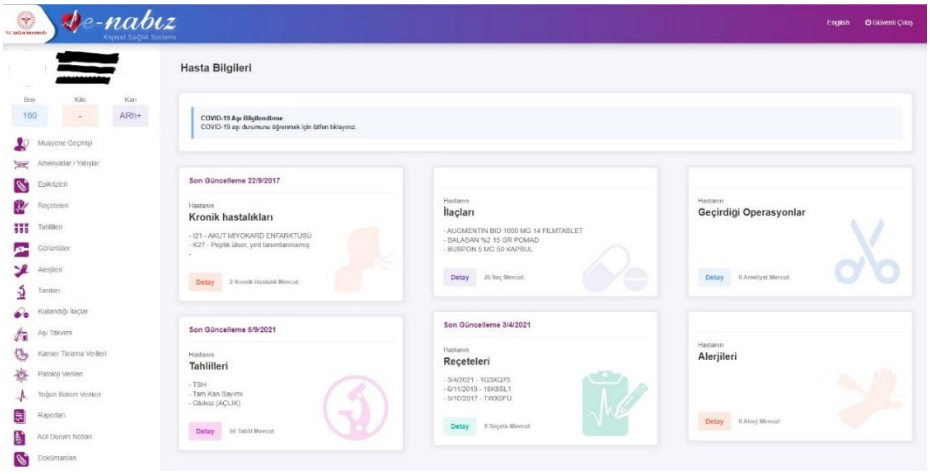
Bazı durumlarda aile hekimleri hastanın muayene veya tetkik bilgilerini görmek isteyebilmektedir. Bu durumda Hızır AHBS üzerinden e-Nabız kişisel kayıt sistemine erişim sağlanması mümkündür.

Aile hekiminin e-Nabız sistemine erişim sağlayabilmesi için ilk olarak hastanın onayı gerekmektedir. Hastanın cep telefonuna gönderilen aktivasyon kodu hasta tarafından hekimle paylaşılırsa, hekim hastanın e-Nabız kaydını görüntüleyebilmektedir (Görsel 52).

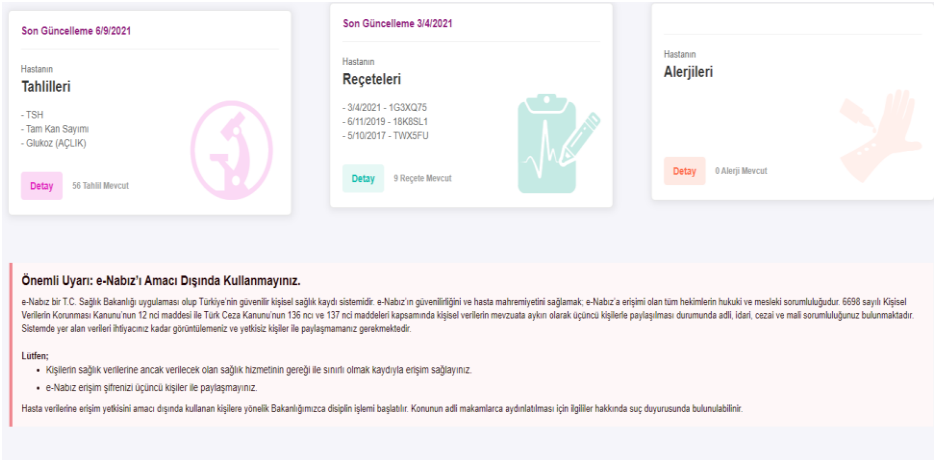


Görsel 52. E-Nabız aktivasyon kod ekranı

Hekim hastanın telefonuna gelen kodu hastanın onayı ile sisteme girdikten sonra hastanın e-Nabız kaydında yer alan bütün sağlık bilgilerini Görsel 53 ve Görsel 54'deki gibi görmektedir.



Görsel 53. E-Nabız aktivasyon kodu girildikten sonra hekimin gördüğü e-Nabız ekranı



Görsel 54. E-Nabız aktivasyon kodu girildikten sonra hekimin gördüğü e-Nabız ekranı

Hekimin erişim sağladığı e-Nabız kaydında hekim için bir uyarı mevcuttur. Bu uyarıya göre hekim, 6698 sayılı Kanun gereği vereceği sağlık hizmetinin gerekliliği kadar hastanın sağlık bilgilerine erişim sağlamalıdır (Görsel 54).

4.2.3. MİA MED veri tabanının incelenmesi

Hastanenin bütün kayıt ve dosya işlemleri MİA MED veri tabanı ile gerçekleştirilmektedir. Bu nedenle veri tabanının birçok farklı modül ekranı bulunmaktadır. Ana ekranda bulunan Müracaat sekmesi ile hasta kaydı yapılmakta ve yatış taburcu işlemleri gerçekleştirilmektedir. Sekme içerisinde kullanıcı işlemleri, mesajlar, hasta kart şema, e-rapor (ilaç/malzeme) hekim onay, duyuru tanımlama, yemek listesi görüntüle ve ilaç rapor e-imza onay gibi diğer işlemler bulunmaktadır. Tedavi hizmetleri sekmesi içinde poliklinikler, poliklinikler/ücretsiz muayene, anabilim dalları/klinikleri ve yataklı servislerle ilgili işlemlerin yapılabildiği ekranlar bulunmaktadır. Rapor istatistikler sekmesinden rapor işlemleri yapılmakta ve istatistikler-raporlarla ilgili veriler görüntülenmektedir. Ayrıca bu ekranda poliklinik işlemleri, hasta geçmiş bilgileri, hasta kimlik bilgileri, poliklinik istatistik işlemleri, kapı üstü monitör işlemleri ve sekreterya işlemleri bulunmaktadır.

MİA MED üzerinde yer alan işlemlerle ilgili kullanıcı bilgilerinden özetlenen işlevler aşağıdaki şekildedir.

Fiziksel tedavi ve rehabilitasyon (FTR) modülü ekranında FTR hastalarının fizik tedavi süreçleri ve medula raporlarının yazılarak takibi yapılmaktadır (Bülbül, 2019a). Bu ekran üzerinde ayrıca fizyoterapi programlama, tetkik, müdahale, e-reçete ve poliklinik istatistik işlemleri yapılmaktadır.

Hemodiyaliz modülü ekranında hastaneye başvuran diyaliz hastalarının tedavi süreçlerinin ve medula raporlarının yazılarak takibi yapılmaktadır (Bülbül, 2019b). Bu ekran üzerinde de tektik, müdahale, ilaç-sarf işlemleri, order, e-reçete ve poliklinik istatistik işlemleri yapılmaktadır.

Kan Bankası sistemi ile hastanenin kendi içerisindeki bağışçılardan alacağı kan ürünün ve Kızılay'dan tedarik edilen kan ürünlerinin sisteme girilerek stokları tutulmakta ve takibi yapılmaktadır. Bu modül ihtiyaca göre hastalara kan çıkarıldığı Kızılay sistemi ile entegre biçimde çalışan bir modüldür (Bülbül, 2019d). Bu sistem üzerinde ayrıca donör hasta listesi, klinik talep durumu, depo raf durumu, manuel ürün girişi, kritik stok ayarlama işlemi, Kızılay stok sorgulama ve kan bankası muayene işlemleri yapılmaktadır. Kan Bankası Laboratuvar ekranında kan merkezinin laboratuvar

sürecinin yürütülmesi işlemleri yapılmaktadır (Bülbül, 2019c). Burada laboratuvar arama, hasta listesi, laboratuvar işlemleri ekranları bulunmaktadır. Kan alma birimi modül işlemleri ekranında ise hasta istemleri görüntülenmekte ve barkod numaraları basılma işlemleri yapılmaktadır (Çimen & Bayraktar, 2019a). Kan alma işlemleri, tüp bilgileri ve barkod basma işlemleri, kapı üstü monitör işlemleri ve kan alma saati işlemleri bu ekran üzerinde gerçekleştirilmektedir.

Laboratuvar modülü ekranında hasta istemleri numune alımları sonrasında tüm laboratuvar işlemleri (kabul-takip-sonuç) bu ekran üzerinde gerçekleştirilmektedir (Çimen & Bayraktar, 2019b).

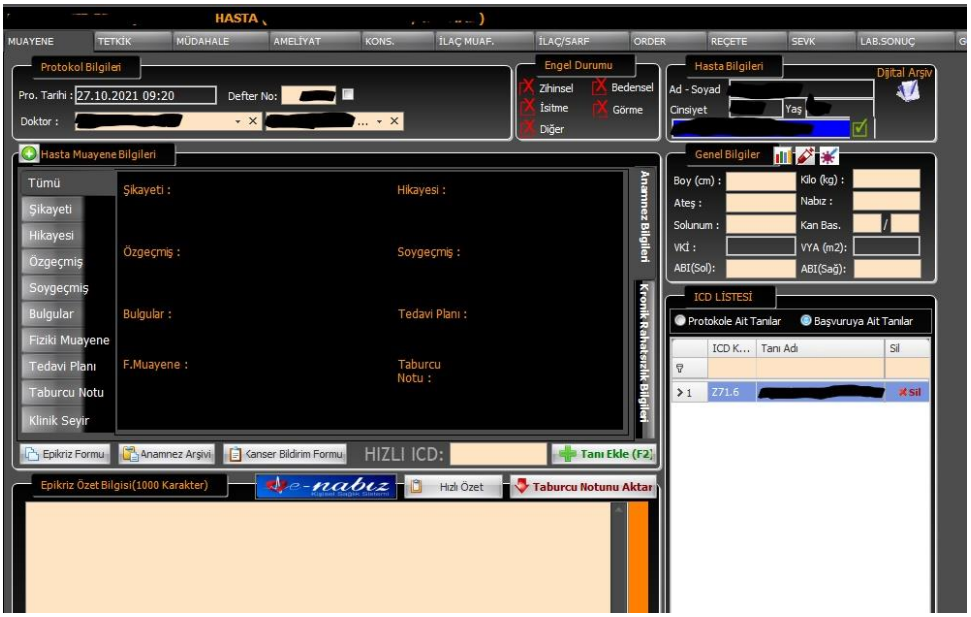
Hasta Kayıt Kabul modülü ekranında hastanın kayıt ve kabul işlemleri yapılmakta, hastane içerisindeki yönlendirme işlemleri yapılmakta ve hasta bilgileri sisteme kayıt edilmektedir (Başer, 2019a). Bu sistem ile yeni kayıt açılmakta, yeni doğan kaydı oluşturulmakta, poliklinik kaydı açılmakta ve eski kayıtlar sorgulanabilmektedir.

Patoloji Laboratuvarı modülü ekranında numune kabul ve talep formu, hatalı ve eksik istemler için hizmet ekleme ve değiştirme, hastanın muayene bilgilerini görüntüleme, rapor içerisinde kelime arama gibi birçok işlem yapılmaktadır (Bülbül, 2019e).

Poliklinik-klinik-yoğun bakım modülü ekranında hastanın poliklinik içerisindeki muayene işlemleri yapılmakta ve hastanın gerekli tetkikleri ile müdahale, reçete, rapor gibi bilgileri girilerek kaydı tutulmaktadır (Başer, 2019b).

Gebelik bildirim-gebe izlem-lohusa izlem modülü ekranında hastanın gebelik süreci ile ilgili bildirim, izlem ve takip işlemleri yapılmaktadır. Bu ekran üzerinde gebelik bildirimi, izlemi ve takibi ile ilgili bilgiler e-Nabızdan bildirimi varsa sorgulanabilmekte ve hastaya dair gebelik veri giriş işlemleri yapılabilmektedir (Başer, 2020).

İlk olarak MİA MED'in hasta ekranı açıldığında muayene, tetkik, müdahale, ameliyat, konsültasyon, ilaç muafiyet, ilaç sarf, order, reçete sevk, laboratuvar sonuç, görüntüleme gibi işlemlerle ilgili ekranlar görüntülenmektedir.



Görsel 55. Hasta geçmiş bilgileri ekranı

Hasta geçmiş bilgileri ekranında hastanın daha önceki muayene bilgileri ve engel durumu olup olmadığı bilgisine yer verilmektedir. Ayrıca bu ekran üzerinden dijital arşiv sistemi hasta dosyası görüntülenebilmekte ve e-Nabız sistemine erişim sağlanabilmektedir (Görsel 55).

4.2.3.1.Hasta kimlik bilgileri ekranları

Hasta kimlik bilgileri ekranında hasta kimlik bilgileri, muayene bilgileri, konsültasyon, reçete, sevk, laboratuvar sonuçları, görüntüleme sonuçları ve epikriz bilgileri bulunmaktadır.

Muayene ekranı: Hastanın muayene ekranında hekimin adı ile hastanın engel durumu bilgisi, adı soyadı, cinsiyeti, boy, kilo, ateş, nabız, solunum, kan basıncı, vücut kitle indeksi ve vücut yüzey alanı bilgileri ile hastanın muayene bilgileri bulunmaktadır.

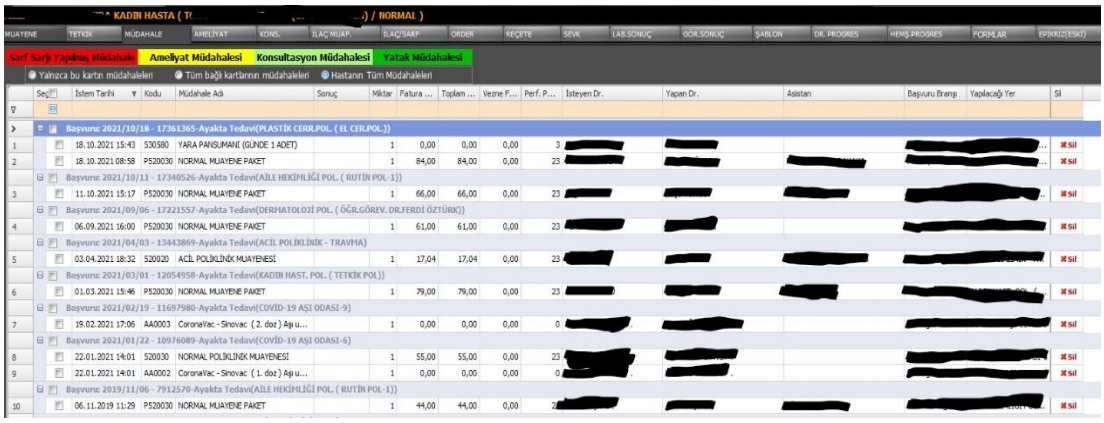
Muayene bilgilerinde ayrıca hastanın şikayeti, hikayesi, özgeçmiş, soy geçmiş, bulgular, tedavi planı, fiziksel muayene ve taburcu notu bilgileri bulunmaktadır. Yanı sıra hastalar ICD kodu ve tanı bilgisine göre listelenmektedir.

Tetkik ekranı: Hastanın tetkik ekranında istem tarihi, kodu, tetkik adı, sonuç, açıklama, numune alınıp alınmadığı bilgisi, laboratuvar kabul tarihi, sonuç tarihi,

fatura, vezne, performans puanı, tetkik isteyen doktor ve tetkiki yapan doktor bilgileri bulunmaktadır. Hastanın tüm tetkikleri de bu ekranda görüntülenmektedir (Görsel 56).

Görsel 56. Tetkik ekranı

Ekranın müdahale sayfasında hastanın tüm tetkik bilgileri Görsel 57'deki gibidir. Tetkik adı ve yapılan tetkik ile ilgili tüm sonuçlar tarih, saat, poliklinik bilgisi ve muayene ücreti bilgileri ile birlikte listelenmektedir.



Görsel 57. Tüm tetkikler ekranı

İlaç muafiyet ekranı: Bu ekranda hastanın rapor bilgileri bulunmaktadır. Buna göre, rapor doktoru, protokol tarihi, rapor no, düzenleme türü, başlangıç tarihi, geçerlilik süresi ve rapor açıklama bilgileri vardır (Görsel 58).

Şekil 58. İlaç muafiyet ekranı

Ekranda bulunan 'Medula gönder' butonu ile ilaç rapor bilgileri Medula sistemine gönderilebilmektedir (Görsel 58).

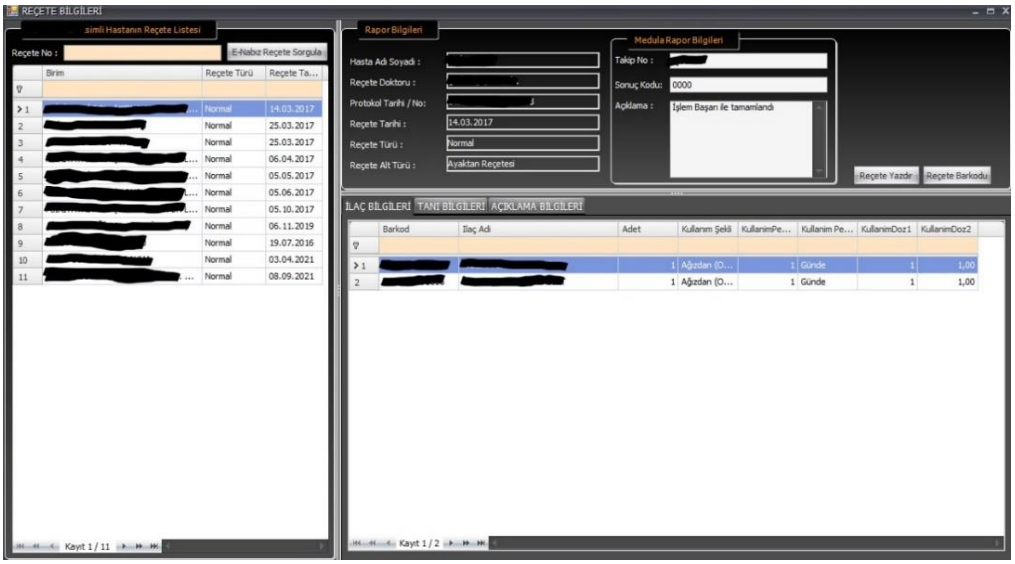
İlaç sarf ekranı: Bu ekranda ürün numarası, tarih, ürün adı, ilaç sarf tipi, reçete türü, miktar, toplam fatura fiyatı, isteyen birim, jenerik adı, verildiği birim, çıkış yapılan

depo, açıklama, doz birimi ve allogreft donör ID bilgilerine göre hastanın ilaç sarf bilgileri listelenmektedir.

Reçete ekranı: Bu ekranda reçete yazan doktor bilgisi, protokol numarası, reçete tarihi, reçete türü ve reçete alt türü (ayaktan vs.) bilgileri bulunmaktadır (Görsel 59).

Görsel 59. Reçete ekranı

Ekranda ayrıca Medula gönder, reçete yazdır, reçete sil, SMS gönder, yeni reçete ekle işlemi ve Medula e-reçete işlemleri yapılabilmektedir (Görsel 59).

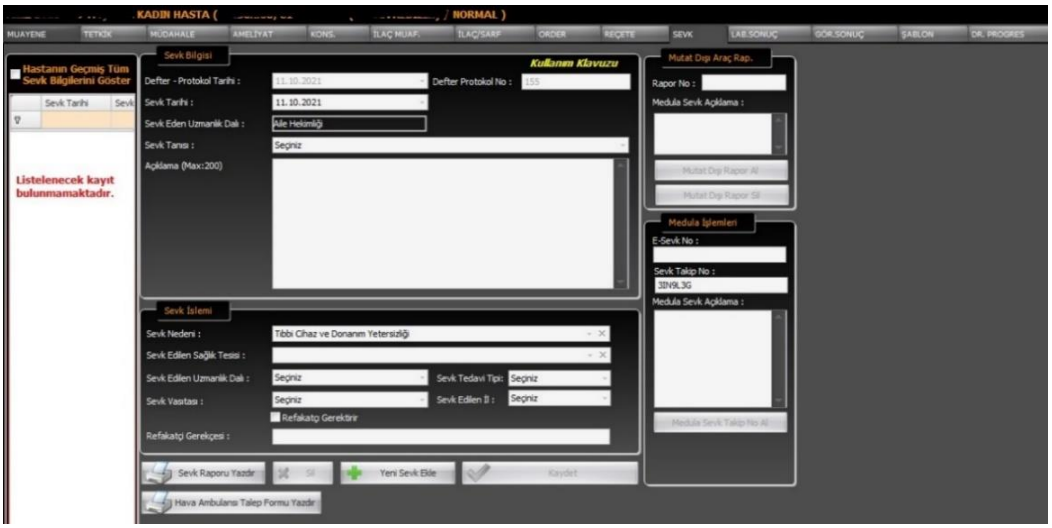


Görsel 60. Reçete bilgileri ekranı

Hastanın rapor bilgileri ve reçete edilen ilaç listesi de bu ekranda bulunmaktadır. Hastanın ilaç bilgilerinin yer aldığı bölümde ise ilaç ve kullanım şekli bilgileri ile hastanın aldığı tanı ve açıklama bilgilerine yer verilmektedir. Reçete bilgileri ekranında ayrıca "e-Nabız reçete sorgula" dan reçete sorgulaması yapılabilmektedir (Görsel 60).

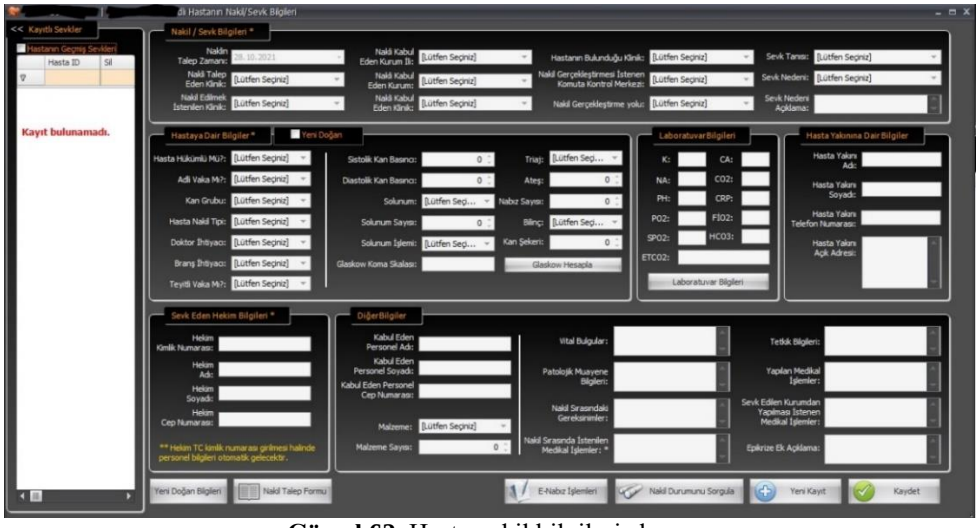
Sevk ekranı: Bu ekranda hastanın geçmiş tüm sevk bilgileri sevk tarihi ve sevk eden kurum bilgilerine göre listelenmektedir. Sevk bilgilerinde sevk edildiği tarih, sevk

tanısı ve açıklama bilgileri bulunmaktadır. Hastanın sevk isteminin de bu ekrandan yapılabilmesi için sevk nedeni, sevk edilen sağlık tesis, sevk edilen uzmanlık dalı, sevk tedavi tipi, sevk eden il, sevk vasıtası ve refakatçi gerekçesi bilgileri bulunmaktadır. Ayrıca hasta için hava ambulansı talebi de bu ekrandan yapılabilmektedir (Görsel 61).



Görsel 61. Sevk ekranı

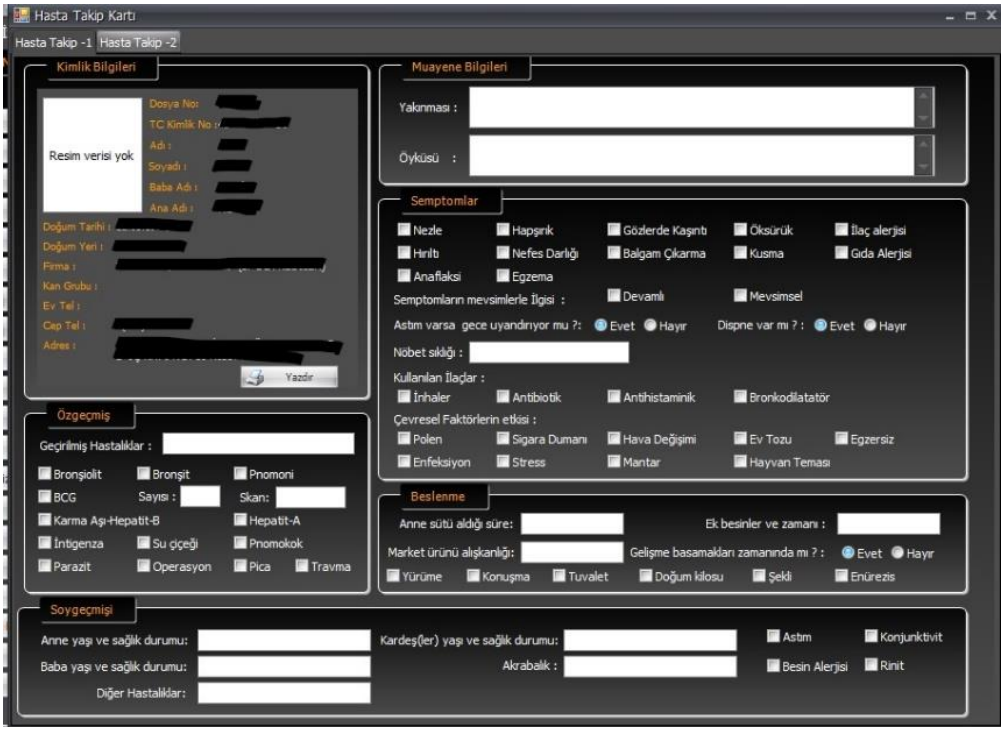
Hasta nakil bilgileri ekranında hastanın geçmiş sevk bilgileri listelenmekte ve sevk ile ilgili daha ayrıntılı bilgiler bulunmaktadır. Hastanın sevk bilgileri ile ilgili, naklin talep zamanı, nakli talep eden klinik, nakil edilmek istenen klinik, nakli kabul eden kurum il, nakli kabul eden klinik, hastanın bulunduğu klinik, nakil gerçekleştirmesi istenen komuta kontrol merkezi, nakil gerçekleştirme yolu, sevk tanısı ve sevk nedeni bilgileri bulunmaktadır (Görsel 62).



Görsel 62. Hasta nakil bilgileri ekranı

Nakli gerçekleşecek olan hastaya dair “hasta hükümlü mü?”, “adli vaka mı?”, kan grubu, hasta nakil tipi, doktor ihtiyacı, branş ihtiyacı, “teyitli vaka mı?”, sistolik kan basıncı, diastolik kan basıncı, solunum, solunum sayısı, solunum işlemi, glaskow koma skalası, triaj, ateş, nabız sayısı, bilinç ve kan şekeri olmak üzere daha detaylı bilgiler vardır. Ayrıca laboratuvar bilgileri, hasta yakını bilgileri ve sevk eden hekim bilgileri bulunmaktadır (Görsel 62).

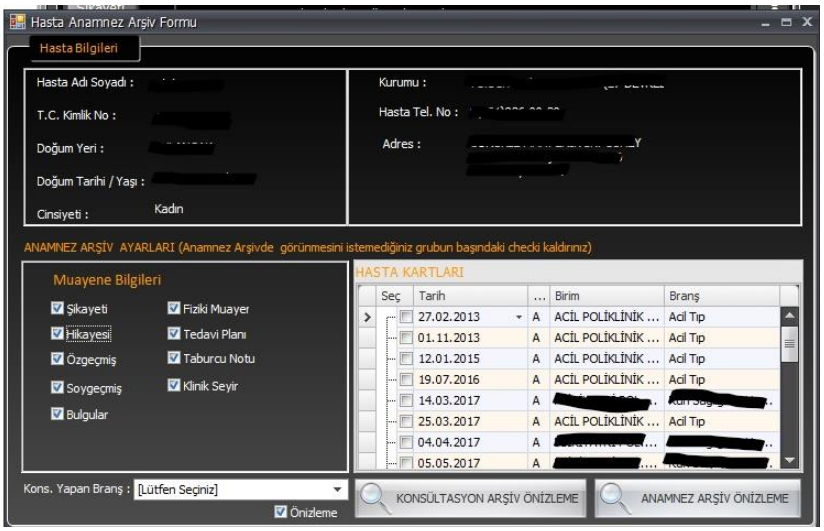
Hasta takip kartı ekranı: Bu ekranda hastanın kimlik numarası, adı, soyadı, baba adı, anne adı, doğum tarihi, doğum yeri, kan grubu, ev telefonu, cep telefonu ve açık adres bilgileri bulunmaktadır (Görsel 63).



Görsel 63. Hasta takip kartı ekranı

Hastanın sağlık bilgilerinin özetlendiği bu ekranda hastalık özgeçmişi (bronşiolit, bronşit, BCG, pnomoni, karma aşı-hepatit B, Hepatit A, intigenza, parazit, suçiçeği, operasyon, pnomokok, pica ve travma bilgileri), muayene bilgileri, semptomlar (nezle, hırıltı, anaflaksi, hapşırık, nefes darlığı, egzema, gözlerde kaşıntı, balgam çıkarma, öksürük, kusma, ilaç alerjisi, gıda alerjisi, astım, dispne, nöbet sıklığı, kullanılan ilaçlar, çevresel faktörlerin etkisi), beslenme ve soy geçmiş (anne yaşı ve sağlık durumu, baba yaşı ve sağlık durumu, kardeşlerin yaşı ve sağlık durumu ve akrabalık) bilgileri bulunmaktadır (Görsel 63).

Hasta anamnez arşiv formu ekranı: Bu ekranda hastanın adı soyadı, kimlik numarası, doğum yeri, doğum tarihi/yaşı, cinsiyeti, kurumu, telefon numarası ve adres bilgileri bulunmaktadır. Ayrıca hastanın hangi tarihte hangi polikliniğe gittiği bilgisi de yer almaktadır (Görsel 64).



Görsel 64. Hasta anamnez arşiv formu ekranı

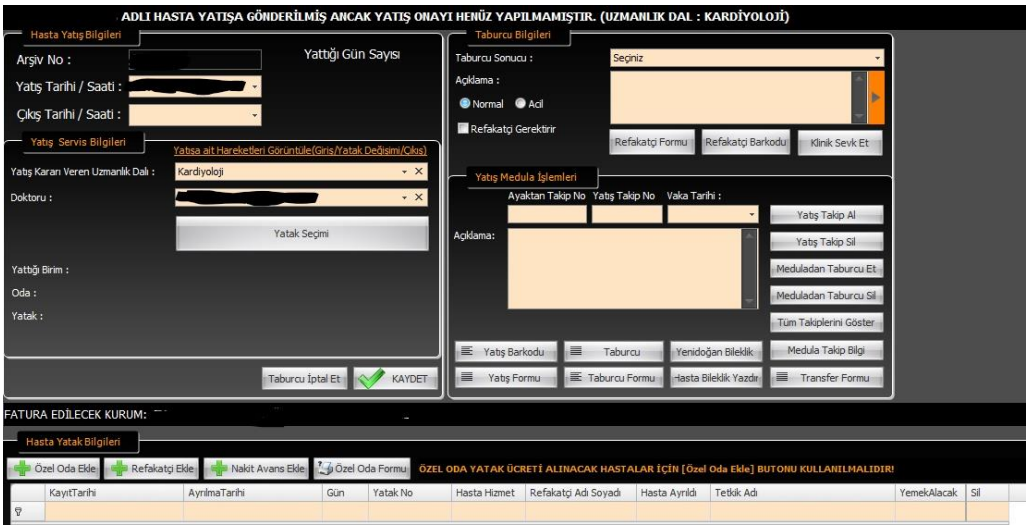
4.2.3.2.Sekreterya işlemlerinde bulunan hasta kayıt ekranları

Görsel 65. Sekreter işlemleri

Sekreterya işlemleri ekranı açıldığında hasta işlemleri ve raporları ekranları ile poliklinik/klinik istatistikleri görüntülenmektedir. Bu ekran üzerinde yer alan bilgiler, hasta kayıt ile ilgili en kapsamlı alandır (Görsel 65).

Yönlendirme işlemleri ekranları: Hasta yatış taburcu işlemleri ekranında "ameliyathaneye gönder", konsültasyon istemi, hasta çağrı kağıdı, hasta sevk işlemleri, hasta ex notu, ölüm bildirim, adli tıp muayene, "doğumhaneye gönder", "diyalize gönder", "sağlık kuruluna gönder", "fizyoterapiye gönder" ve "psikoloji ünitesine gönder" gibi yönlendirme işlemleri yapılmaktadır. Ekranda ayrıca enfeksiyon hastalıkları uzman onay, hastayı ameliyat listesine ekle, hasta eğitim bilgisi ekle, hemşirelik süreçleri, psikolojik değerlendirme raporu, randevu defteri, yoğun bakım değerlendirme formu işlemleri bulunmaktadır. Bu işlemlerden kişisel bilgi içeren ekranlar aşağıdaki şekilde incelenmiştir.

Hasta yatış taburcu işlemleri ekranı: Hasta yatış ve taburcu işlemlerinin yapıldığı bu ekranda hastanın yatış tarihi, çıkış tarihi, yattığı gün sayısı, yatış kararı veren uzmanlık dalı, doktoru, yattığı birim, oda, yatak bilgileri, tetkik, taburcu bilgileri ile refakatçi adı soyadı bilgileri bulunmaktadır (Görsel 66).

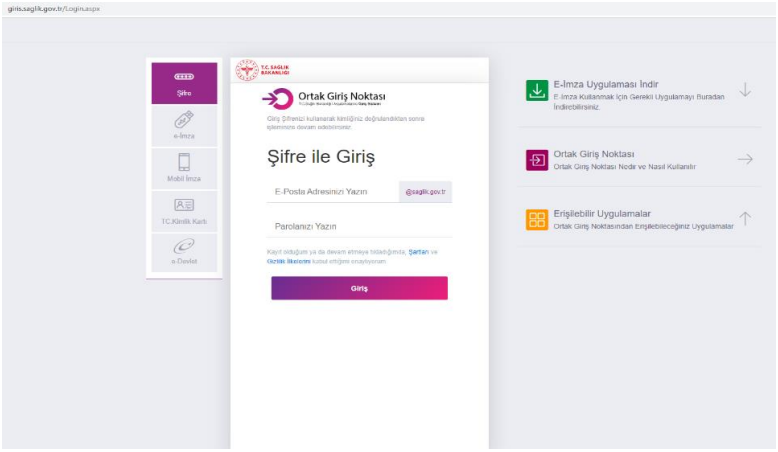


Görsel 66. Hasta yatış taburcu işlemleri ekranı

Aynı ekranda bulunan Medula işlemleri bölümünde ayaktan veya yataktan takip işlemleri ile taburcu işlemleri yapılmaktadır (Görsel 66).

Ölüm bildirim ekranı: Ölüm bildirim ekranı, ölüm bildirimi yapabilmek için hekimi Sağlık Bakanlığı'na yönlendirmektedir. Hekim e-imza, mobil imza, T.C. kimlik

numarası veya e-Devlet uygulamalarından biri ile giriş yaparak bildirimde bulunmaktadır (Görsel 67).



Görsel 67. Hasta ölüm bildirim girişi ekranı

Hasta tedavi raporları ve formları ekranları: Bu ekranda, rapor işlemleri yapılmakta ve Medula GSS tedavi raporu bulunmaktadır. Ekranda bulunan hasta tedavi formları şunlardır; Medula GSS diyabet formu, kanser kayıt bilgi formu, kadına şiddet tarama ve kayıt formları, intihar girişim formu, yenidoğan sevk ve nakil formu, bebek takip formu, gebe takip formu, gebelik bildirimi, aşı takip formu, alerji ve göğüs hastalıkları testleri, algoloji-anestezi formları, kardiyoloji formları, nöroloji muayene testleri, trafik kazası hastane bilgi formu, güvenli cerrahi kontrol listesi formu, hasta nakil formu, hasta vizit formu, bulaşıcı hastalık bildirimi, yatış formu, tıbbi malzeme rapor, tıbbi malzeme reçete ve anestezi öncesi muayene formu.

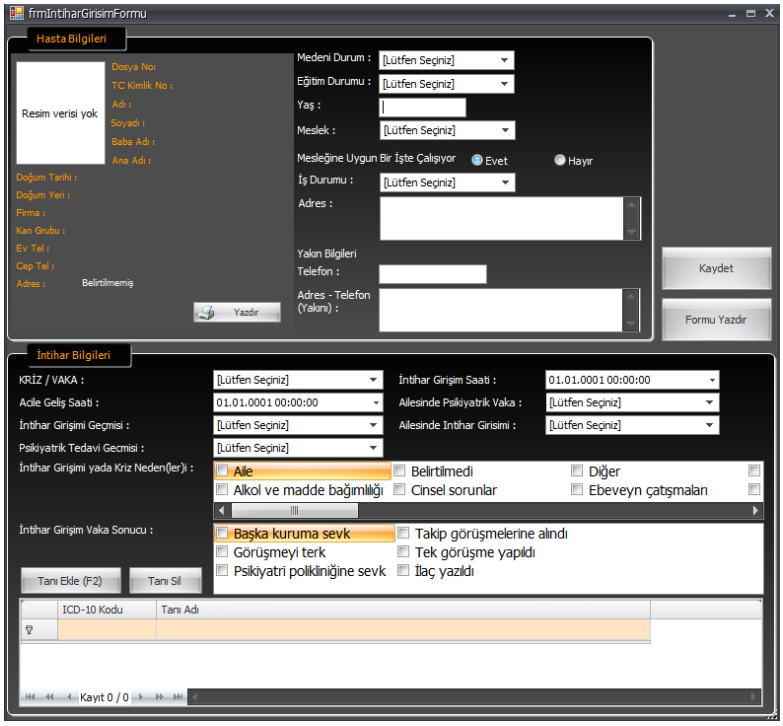
Rapor işlemleri ekranı incelendiğinde istirahat raporu, konsey kararı raporu, anabilim dalı raporu, iş göremezlik belgesi, engelli raporu, medikal malzeme raporu, sağlık kurulu raporu, çalışabilir kağıdı, askerlik formu, tüp bebek raporu bulunmakta ve diğer rapor seçeneği ile rapor verme işlemleri yapılmaktadır. Çalışabilir kağıdına, sigortalı kişinin T.C. kimlik numarası, adı soyadı, tahlil, tedavi, sevk, tedavisinin bittiği tarih ve saat ve çalışabileceği tarih bilgileri girişi yapılmaktadır. Bu ekranda ayrıca hastanın kimlik bilgileri de bulunmaktadır. T.C. kimlik numarası, adı soyadı, baba adı, anne adı, doğum tarihi, doğum yeri, kan grubu, ev telefonu, cep telefonu ve açık adres bilgileri bulunmaktadır.

Kanser kayıt formu ekranında hastanın kimlik bilgilerine ek olarak kanser teşhis tarihi, tümörün yerleştiği organ, histolojik tanı, çoğul primer durum türü, evre, hasta sağlık durumu, letarelite, tedavi, seer ozet evre (lenf nodları tutulumu/evrelemesi) tanıya esas olan yöntem bilgisi ve kanserin son kontrol tarihi bilgisi bulunmaktadır.

Kadın hastalar için kadına şiddet tarama ve kayıt formları ekranında hastanın adı ve soyadı, hekim adı ve şiddetle ilgili bazı sorular bulunmaktadır. Ayrıca kadına şiddet konusunda bir geri bildirim formu ekranı bulunmaktadır (Görsel 68).

Görsel 68. Kadına şiddet geri bildirim formu ekranı

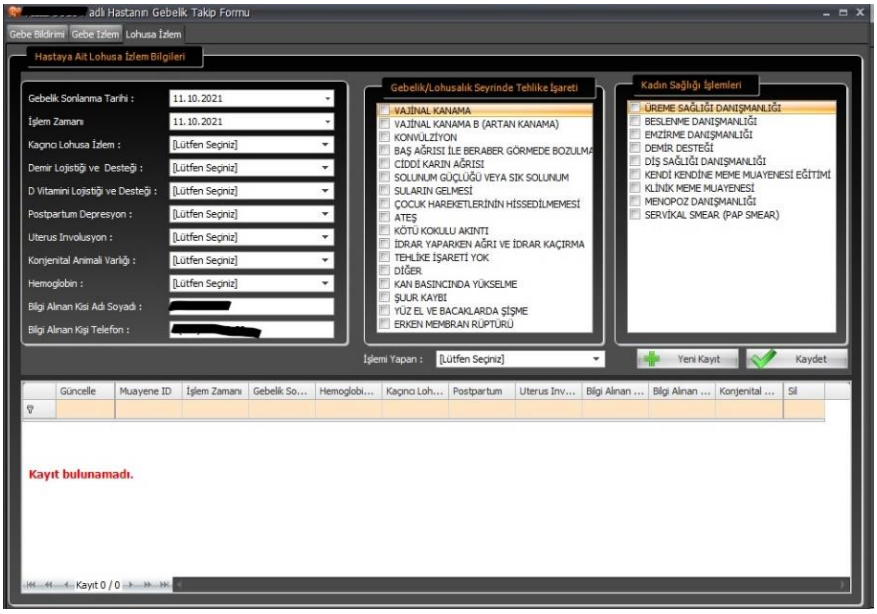
İntihar girişim formu ekranı: Bu ekranda hastanın kimlik bilgileri, medeni durumu, eğitim durumu, yaş, meslek, "mesleğine uygun bir işte çalışıyor mu?", iş durumu, adres, yakın bilgileri (telefon, adres) bilgileri bulunmaktadır. İntihar girişimi ile ilgili olarak kriz/vaka bilgisi, acile geliş saati, intihar girişimi geçmişi, psikiyatrik tedavi geçmişi, intihar girişimi ya da kriz nedenleri, intihar girişim saati, ailesindeki psikiyatrik vaka bilgisi ve ailesinin intihar girişimine ilişkin bilgi bulunmaktadır (Görsel 69).



Görsel 69. İntihar girişim formu ekranı

Gebe takip ekranı: Bu ekranda kişinin gebelik durumu / son adet tarihi, riskli gebelik durumu, riskli gebelik detayı ve önceki doğum durumu ile ilgili bilgiler yer almaktadır. Aynı ekranda bulunan gebe izlem bilgilerine dair, işlem zamanı, idrarda protein, hemoglobin, izlem işlem türü, kaçıncı gebe izlem olduğu bilgisi, demir lojistiği ve desteği, D vitamini ve lojistiği bilgisi, konjenital anomalili doğum varlığı, fetüs kalp sesi, tansiyon, gestasyonel diyabet taraması ve gebelikte risk faktörleri bilgileri bulunmaktadır (Görsel 70).

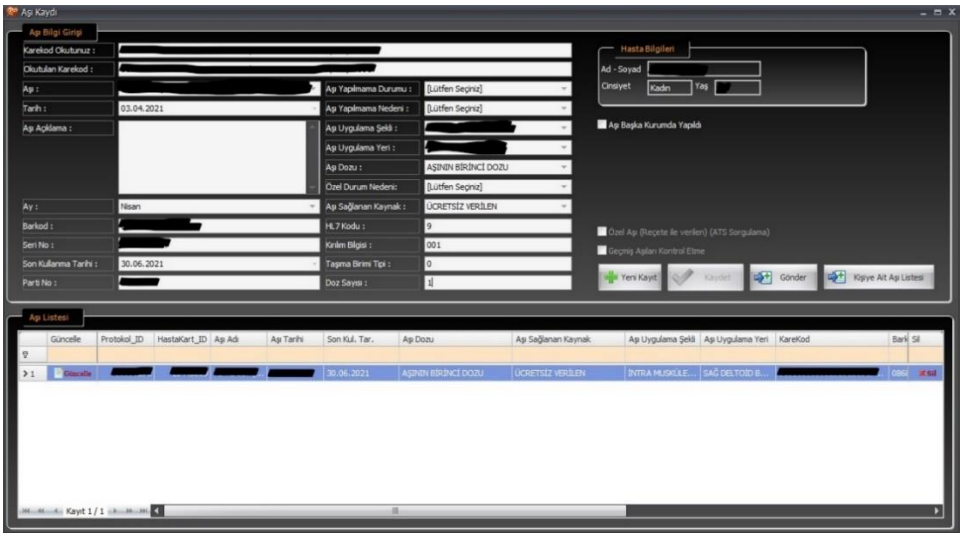
Lohusa izlem ekranında gebelik sonlanma tarihi, işlem zamanı, kaçıncı lohusa izlemi olduğu, demir lojistiği ve desteği, D vitamini lojistiği ve desteği, pospartum depresyon, uterus involusyon, konjenital anomali varlığı, hemoglobin, bilgi alınan kişi adı soyadı, bilgi alınan kişi telefon, gebelik/lohusalık seyrinde tehlike işareti ve kadın sağlığı işlemlerine ait bilgiler bulunmaktadır (Görsel 70).



Görsel 70. Gebe-lohusa izlem bilgileri ekranı

Aşı takip ekranı: Bu ekranda aşı bilgi girişi yapılmakta, hasta bilgileri özetlenmekte ve hastanın aşı kayıtları listelenmektedir.

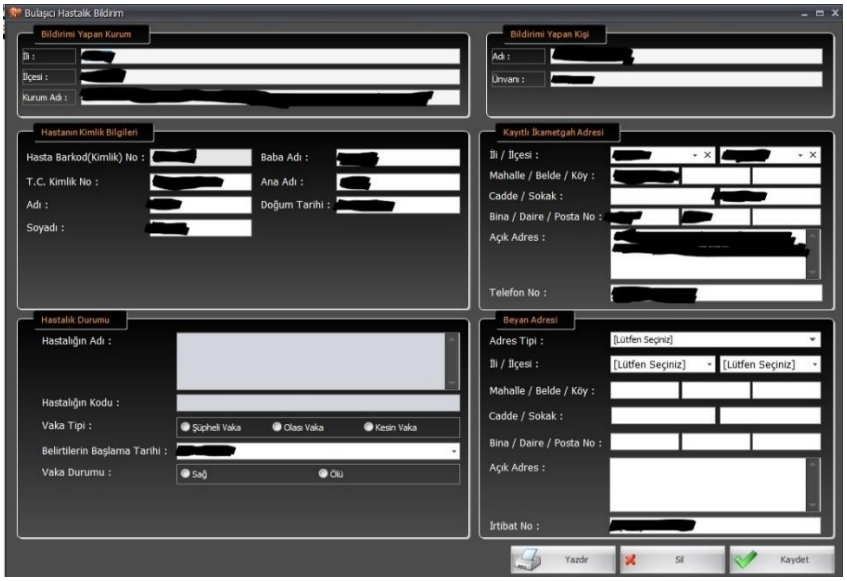
Aşı bilgi girişi için aşı, tarih, aşı açıklama, aşı yapılmama durumu, aşı yapılmama nedeni, aşı uygulama şekli, aşı uygulama yeri, aşı dozu, özel durum nedeni, aşı sağlanan kaynak, HL7 kodu[9], kırılım bilgisi, taşıma birimi tipi ve doz sayısı bilgileri bulunmaktadır (Görsel 71).



Görsel 71. Aşı kaydı ekranı

[9] HL7 (Health Level 7), sağlık bilişiminde dünya çapında yaygın olarak kullanılan standart bir dil'dir. Bu dil sayesinde insan ya da makine varlığının sağlıkla ilgili bir konuda birbiriyle haberleşebilmesi sağlanmıştır (Sağlık Bakanlığı, 2014b).

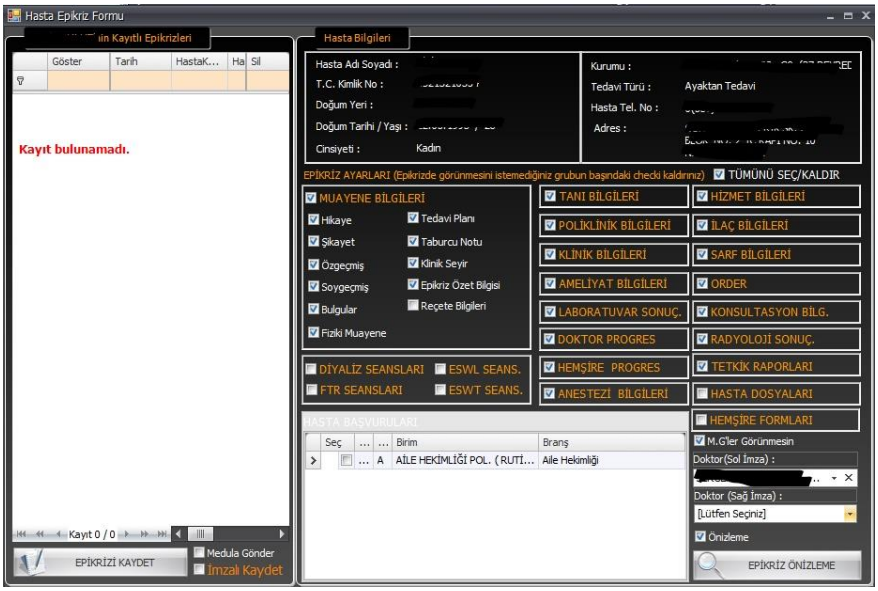
Bulaşıcı hastalık bildirim ekranı: Bu ekranda bildirimi yapan kurum bilgisi, bildirimi yapan kişi ve unvanı, hastanın kimlik bilgileri, hastanın kayıtlı ikametgah adresi, hastalık durumu ve beyan adresi bilgileri bulunmaktadır (Görsel 72).



Görsel 72. Bulaşıcı hastalık bildirim ekranı

Hasta istatistikleri – raporları ekranları: Hasta hizmet dökümü, epikriz raporu, hasta nakil bilgileri, anamnez arşivi, laboratuvar sonuçları göster, görüntüleme sonuçlarını göster, panik değer bildirimlerini görüntüle, hasta geçmiş dosyalarını göster, hasta refakatçi formu, hasta kartına dosya ekle, uzmanlık şablonları, toplu vizit ekle, eksik evrak hasta bilgilendirme formu, estetik amaçlı cerrahi işlem hasta bilgilendirme formu, meme formu, hasta formları ve hasta onam formları işlemlerinin yapıldığı ekranlar bulunmaktadır. Hasta hizmet dökümü ekranında hasta adı soyadı, hasta kart listesi ve birimler bilgileri bulunmaktadır.

Epikriz formu ekranı: Epikriz formunda hastanın daha önceki epikriz kayıtları listelenmekte ve hastanın adı soyadı, kimlik numarası, doğum yeri, doğum tarihi/yaşı, cinsiyeti, kurumu, telefon numarası ve açık adres bilgileri bulunmaktadır. Bu formun içinde diyaliz seans bilgileri, FTR seansları, tanı bilgileri, poliklinik bilgileri, klinik bilgileri, ameliyat bilgileri, laboratuvar sonuç bilgileri, doktor ve hemşire progres bilgileri, anestezi bilgileri, hizmet bilgileri, ilaç bilgileri, sarf bilgileri, order, konsültasyon bilgileri, radyoloji sonuç, tetkik raporları, hasta dosyaları ve hemşire formları ile ilgili bilgiler bulunmaktadır (Görsel 73).



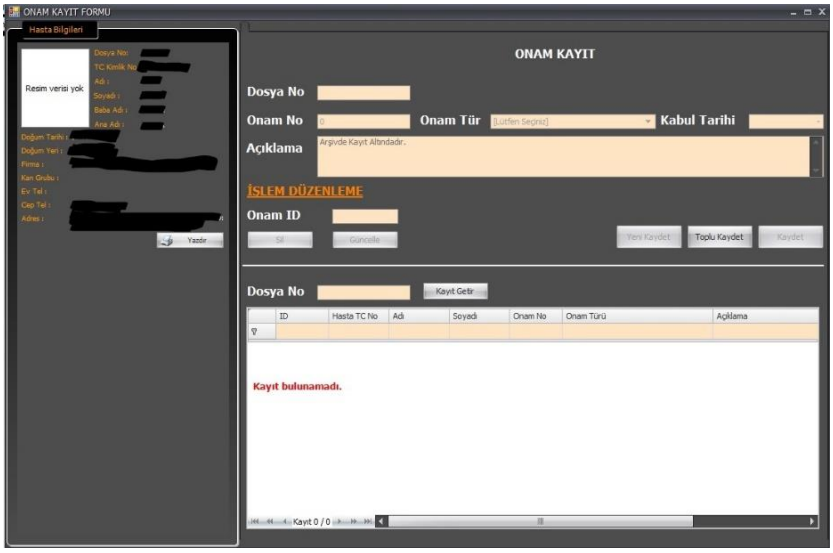
Görsel 73. Hasta epikriz formu ekranı

Laboratuvar sonuçları ekranı: Bu ekranda hastanın hangi polikliniğe gittiği, polikliniğe gidiş tarihi ve bütün tetkik bilgileri listelenmektedir.

Meme formu ekranı: Bu ekranda hastanın adı, soyadı, kimlik numarası, doğum tarihi, yaşı, başvuru tarihi ve telefon numarası bilgileri ile şikayet bilgileri bulunmaktadır. Hastanın şikayet bilgileri, kitle, ağrı, akıntı, deri, aksiller kitle ve meme başı bilgilerinden oluşmaktadır. Ayrıca kadın hastanın gebelik sayısı, menarş bilgisi, vücut kitle indeksi, mastit/abse öyküsü, doğum sayısı, menapoz, alkol kullanımı, ilk gebelik yaşı, emzirme süresi, infertilite tedavi bilgisi, radyasyon bilgisi ve ailedeki meme kanseri bilgileri bulunmaktadır. Hastanın ilgili tüm formları bu ekran üzerinde listelenebilmektedir.

Onam formu ekranı: Bu ekranda hastanın kimlik numarası, adı, soyadı, baba adı, anne adı, doğum tarihi, doğum yeri, kan grubu, ev telefonu, cep telefonu ve açık adres bilgileri bulunmaktadır.

Onam kaydı oluşturulması için hastanın T.C. kimlik numarası, adı, soyadı, onam türü, kabul tarihi bilgileri ve açıklama eklenmektedir (Görsel 74).



Görsel 74. Onam formu ekranı

Poliklinik/Klinik istatistikleri ekranları: Bu ekran üzerinde doktor hizmet kayıtları, puanı sıfırlanan defter dökümü, hizmet istatistikleri, ameliyat randevu listesi, evrak teslim formu, tanı istatistik formu, yatan hastalara ait günlük kayıt formu, aylık bilgi formu, intihar girişim formu, kadına şiddet geri bildirimi formu, hasta ve yatak izle formu ekranları bulunmaktadır. Ayrıca günlük muayene sayıları, randevu rapor, yatırılan hasta listesi, taburcu edilen hasta listesi, hemşire vardiya devir işlemleri, ameliyat listesi, toplu order dökümü, protokol defteri, sevk edilen hasta listesi, hizmet istatistikleri, hasta hizmetler listesi ve hastalara verilen narkotik ilaçlar ve diyet yemek detay bilgi ekranları bulunmaktadır. Bununla birlikte arşiv hasta raporu, hasta diyet raporu, hasta ilaç muafiyet raporu ve muafiyet raporu istatistiği ekranları vardır. Bu ekranda bulunan formlar daha önce işlendiği için burada tekrar yer verilmemiştir.

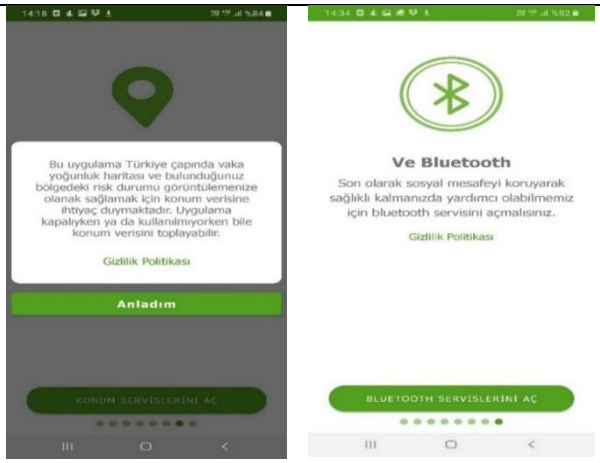
4.2.4. Mobil Sağlık Uygulamalarının İncelenmesi

4.2.4.1.Hayat Eve Sığar (HES) mobil uygulamasının incelenmesi

Türkiye'de bulaşıcı bir hastalıkla mücadele kapsamında kullanılan ilk mobil uygulama HES uygulaması olmuştur. Uygulama Covid-19 testi pozitif çıkan ve tanı konulan kişiler ile tanı konulanlarla yakın teması olan tüm kişileri kapsamaktadır.

Uygulama ile amaçlanan, evde izolasyon altında bulunması gereken kişilerin, evi terk etmeleri durumunda uyarılabilmesi ve bu kişilerle anında iletişime geçilebilmesidir.

Uygulamanın kurulum aşamasında, telefona gelen kısa mesaj ile hesap doğrulaması yapıldıktan sonra ilk olarak koronavirüs olma ihtimaline karşı mini bir test karşımıza çıkmaktadır. Kurulum aşamasında kullanıcının konum verisi ve Bluetooth servisine erişim bilgileri işlenmektedir. Konum bilgisine erişim gerekçesi, "Bu uygulama Türkiye çapında vaka yoğunluk haritası ve bulunduğunuz bölgedeki risk durumu görüntülemenize olanak sağlamak için konum verisine ihtiyaç duymaktadır. Uygulama kapalıyken ya da kullanılmıyorken bile konum verisini toplayabilir." biçiminde açıklanmaktadır (Görsel 75).



Görsel 75. Konum bilgisi ve Bluetooth servisi erişim zorunluluğu hakkında bilgilendirme ekranları

Konum bilgisi ve Bluetooth servisi erişim zorunluluğu bilgilendirme ekranları kabul ettikten sonra karşımıza uygulamanın Gizlilik Politikası çıkmaktadır.

Gizlilik Politikası[10]

Bu gizlilik politikası, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("KVK Kanunu") 10 uncu maddesi uyarınca hazırlanmıştır.

Veri Sorumlusunun Kimliği
Bu uygulamada işlenen kişisel verileriniz bakımından veri sorumlusu T.C. Sağlık Bakanlığı'dır.

[10]Pandemi sürecinde uygulamanın aydınlatma metni bu şekildedir. Bu metinin güncel versiyonu için bakınız EK-3.

Kişisel Verilerin İşlenme Amaçları

Bu uygulamada aşağıda yer alan kişisel verileriniz, **pandemi ile mücadele süresiyle sınırlı olmak üzere,** şu amaçlarla işlenmektedir:

- **Kimlik verisi:** TC Kimlik Numarası, baba adı ve doğum tarihi bilgileriniz, kimliğinizin doğrulanması amacıyla işlenmektedir. Bu verilerinizi girmeksizin de uygulamayı bazı kısıtlamalarla kullanabilmektesiniz. Eğer TC Kimlik Numarasını girmek istemezseniz, COVID-19 riskinizin hesaplanabilmesi için yaşınızı girmeniz gerekmektedir.
- **İletişim verisi:** Uygulamayı ilk yüklediğinizde, SMS ile gönderilecek olan kodu girmek ve telefonunuzu doğrulamak amacıyla GSM numaranız işlenmektedir. Her bir GSM numarası ile uygulamaya yalnızca bir kez kayıt olunabilmekte; aynı GSM numarası ile birden fazla kişinin uygulamayı kullanma imkânı bulunmamaktadır. Ayrıca, uygulamanın "Aile" sekmesinde takip etmek istediğiniz sevdiklerinize davetiye göndermek için, onların GSM numaralarını girmeniz veya kişi listesinden seçmeniz gerekmektedir.
- **Konum verisi:** Konum bilginiz, harita üzerinde konumuzun gösterilmesi, bulunduğunuz bölgede COVID-19 pozitif ve risk yoğunluğunun harita üzerinden gösterilmesi, izolasyon altında bulunduğunuz lokasyonun belirlenmesi, bu lokasyonu terketmeniz durumunda tarafınıza bildirim gönderilmesi ve ilgili makamlara bilgi verilmesi amaçlarıyla işlenmektedir.
- **Sağlık verisi:** Sağlık bilgileriniz, COVID-19 riskinizin belirlenmesi amacıyla işlenmektedir. Yöneltilen sorulara vereceğiniz yanıtlara göre en yakın sağlık tesisini ziyaretiniz istenebilecek veya periyodik aralıklarla hastalık belirtileriniz hakkında tarafınıza devam sorular yöneltilecektir.
- **Meslek verisi:** Sağlık çalışanı olup olmadığınız ve eğer sağlık çalışanıysanız hastalarla temasınızın olup olmadığı bilgisi, hastalık riski seviyesini belirlemek amacıyla işlenmektedir.

Kişisel Verilerin Aktarımı

İzolasyon altında bulunmanız gereken bölgeyi terk etmeniz halinde bu uygulama ile elde edilen kimlik, iletişim ve konum verileriniz, kamu sağlığının korunması ve salgının yayılmasını önleme amaçlarıyla İçişleri Bakanlığı ve kolluk kuvvetleri ile paylaşılmaktadır.

Kişisel Veri Toplamanın Yöntemi ve Hukuki Sebebi

Kişisel verileriniz bu uygulama aracılığı ile tamamen otomatik yollarla elde edilmekte olup, KVK Kanununun 6 ncı maddesinin üçüncü fıkrası uyarınca 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 işlenmesi hukuki sebebine dayanarak işlenmektedir.

İlgili Kişilerin Hakları

KVK Kanunu'nun 11 inci maddesinde yer alan haklarınızı, KVK Kanunu'nun 13 üncü maddesi ile Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ'in ("Veri Sorumlusuna Başvuru Tebliği") ilgili hükümleri uyarınca Bakanlığımıza başvuru yapmak suretiyle kullanabilirsiniz.

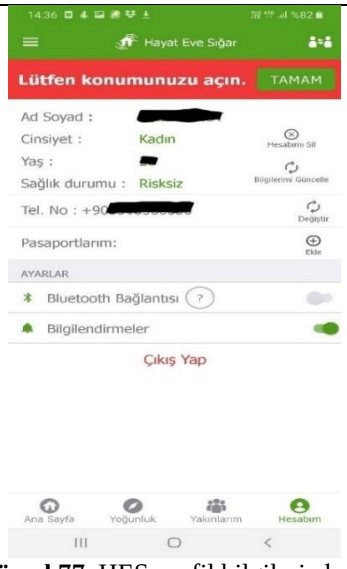
Veri Sorumlusuna Başvuru

KVK Kanunu'nun 13 üncü maddesi uyarınca yapacağınız yazılı başvuruları "T.C. Sağlık Bakanlığı, Üniversiteler Mahallesi, 6001. Cadde, No:9, Çankaya, Ankara" adresine; Kayıtlı Elektronik Posta (KEP) ile yapacağınız başvuruları ise "sb@hs01.kep.tr" adresine iletebilirsiniz.

Gizlilik politikası "okudum, anladım" ibaresi işaretlendikten sonra uygulama kullanılmaya hazırdır.

Uygulamanın ana ekranı: Uygulamanın içeriğinde HES kodu sorgulaması, HES kodlarım kutucuğu, ihbarda bulun özelliği, kullanıcının Covid-19 aşı bilgileri, AB uyumlu sağlık pasaportu, alan barkod okutma özelliği, korona riskini hesaplama özelliği ve uygulamayı değerlendiren bir anket yer almaktadır (Görsel 76).

Görsel 76. HES ana ekranı



Görsel 77. HES profil bilgileri ekranı

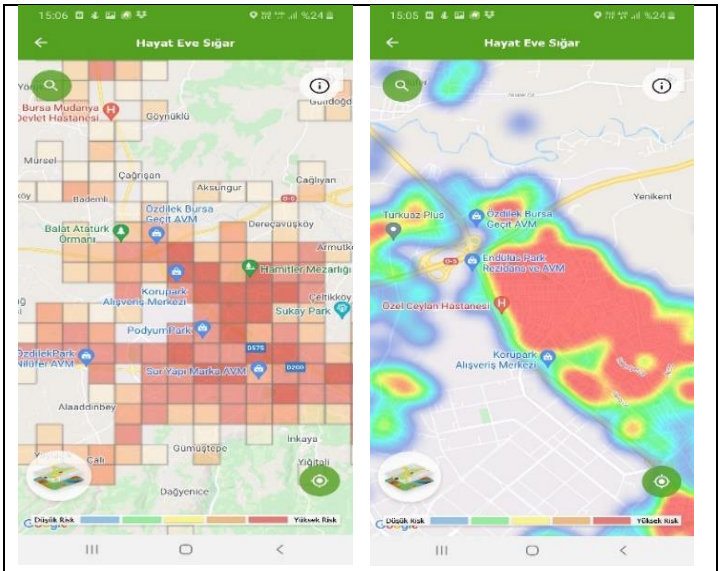
AB uyumlu sağlık pasaportu, uygulamada şu şekilde açıklanmaktadır (Görsel 76);

Dünya Sağlık Örgütü (DSÖ) tarafından pandemi (küresel salgın) olarak nitelendirilen yeni tip korona virüs salgını (Covid-19) ile ülkemiz ve dünya genelinde etkin bir şekilde mücadele edebilmek, virüsün yayılmasına engel

olmak ve bulaşma riskini en aza indirmek amacıyla ülke içinde ve ülkeler arası seyahatlerde aşı, bağışıklık ve diğer sağlık bilgilerinin ülke otoriteleri ve hava yolları firmaları ile paylaşılabilmesine olanak sağlayan bir sağlık pasaport uygulamasıdır.

Uygulama konum bilgisinin açılması gerektiğini sürekli olarak kırmızı uyarı ile belirtmektedir (Görsel 77).

Kullanıcının "Hesabım" ekranında ad, soyad, cinsiyet, yaş, sağlık durumu, telefon numarası bilgileri bulunmakta ve istenirse pasaport bilgileri eklenebilmektedir.

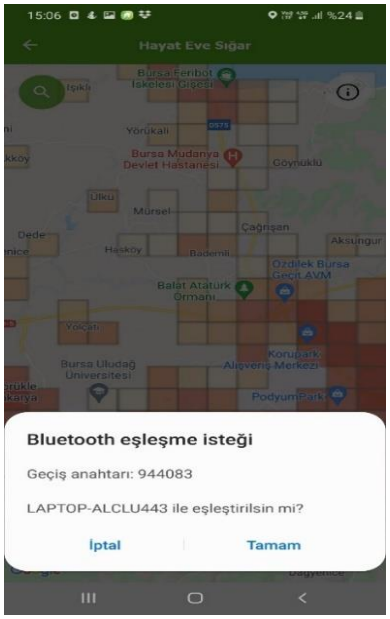


Görsel 78. Korona yoğunluğunu gösteren haritalar

Yoğunluk ekranında telefonun konum verisi açıksa, korona yoğunluğunu gösteren haritalar görüntülenebilmektedir (Görsel 78). Böylece kişi yaşadığı bölgedeki korona yoğunluğunu takip edebilmektedir.

Yakınlarım ekranında, kişi eklemesi yapılarak kullanıcının eklediği kişinin durumu hakkında kullanıcı tarafından takip yapılabilmektedir.

Bilgilendirme özelliği de bulunan uygulama, günlük güncel koronavirüs tablosunu göstermektedir.



Görsel 79. Bluetooth erişim isteği

Uygulama analiz sırasında, Bluetooth-Laptop eşleşmesi istemiştir (Görsel 79).

Uygulama konum verisi açık olarak çalışırken aynı zamanda telefonda Bluetooth servisinin de açık olması gerekmektedir. Bu özellik ile kullanıcıdan yakın cihazlara erişim istenebilmektedir.

Görsel 80. İhbarda bulunma ekranı

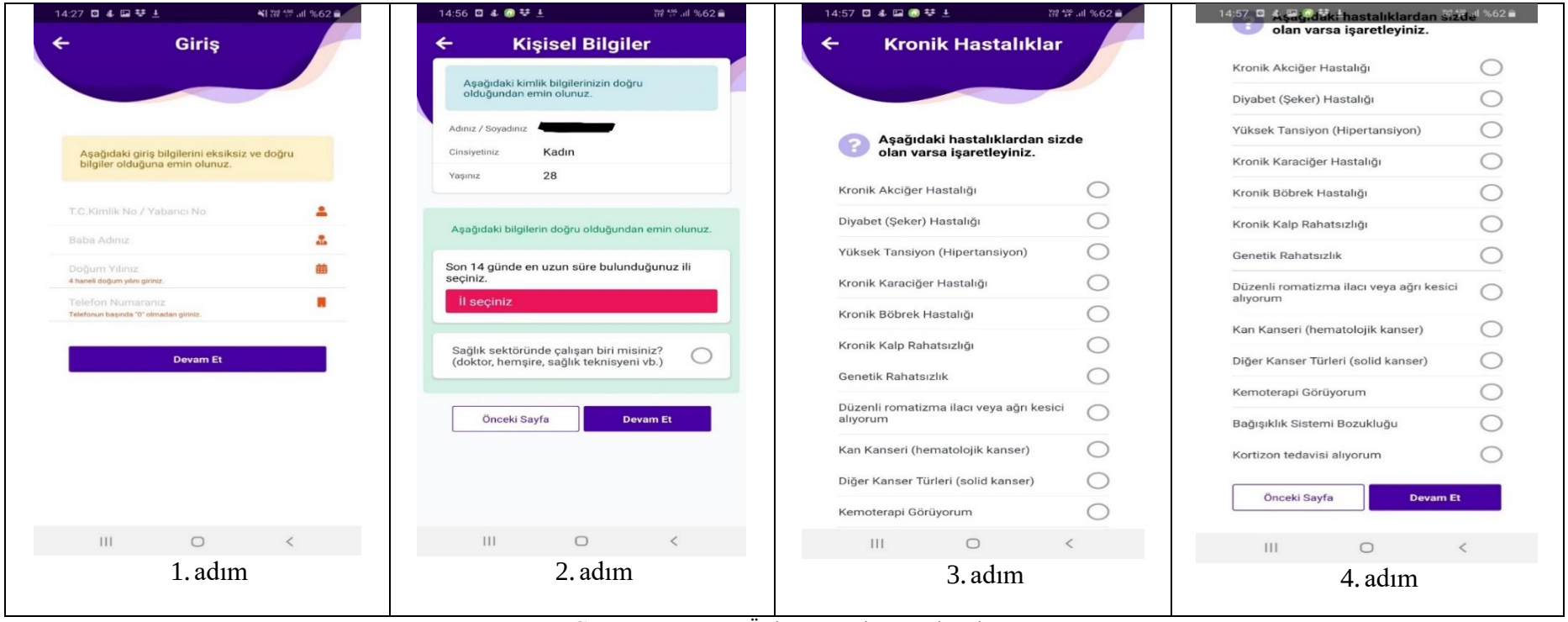
Uygulamanın bir diğer işlevi, "ihbarda bulun!" biçiminde belirtilen özelliktir. İhbar konusu; "havalimanı", "iş yeri", "izolasyona tabi kişi", "kişi", "toplumsal etkinlikler" ve "toplu taşıma" biçimindedir (Görsel 80).

İhlal türü; "maske kullanmıyor", "sosyal mesafeye uyulmuyor" ve "temizlik kurallarına uyulmuyor" şeklindedir (Görsel 80).

İhbar anının fotoğrafı çekilebilmekte ve uygulama üzerinden bildirim yapılabilmektedir. İl, ilçe, köy, mahalle ve adres bilgileri eklenerek, ihbara ilişkin detaylı bilgiler verilebilmektedir (Görsel 80).

4.2.4.2.Korona Önlem uygulamasının incelenmesi

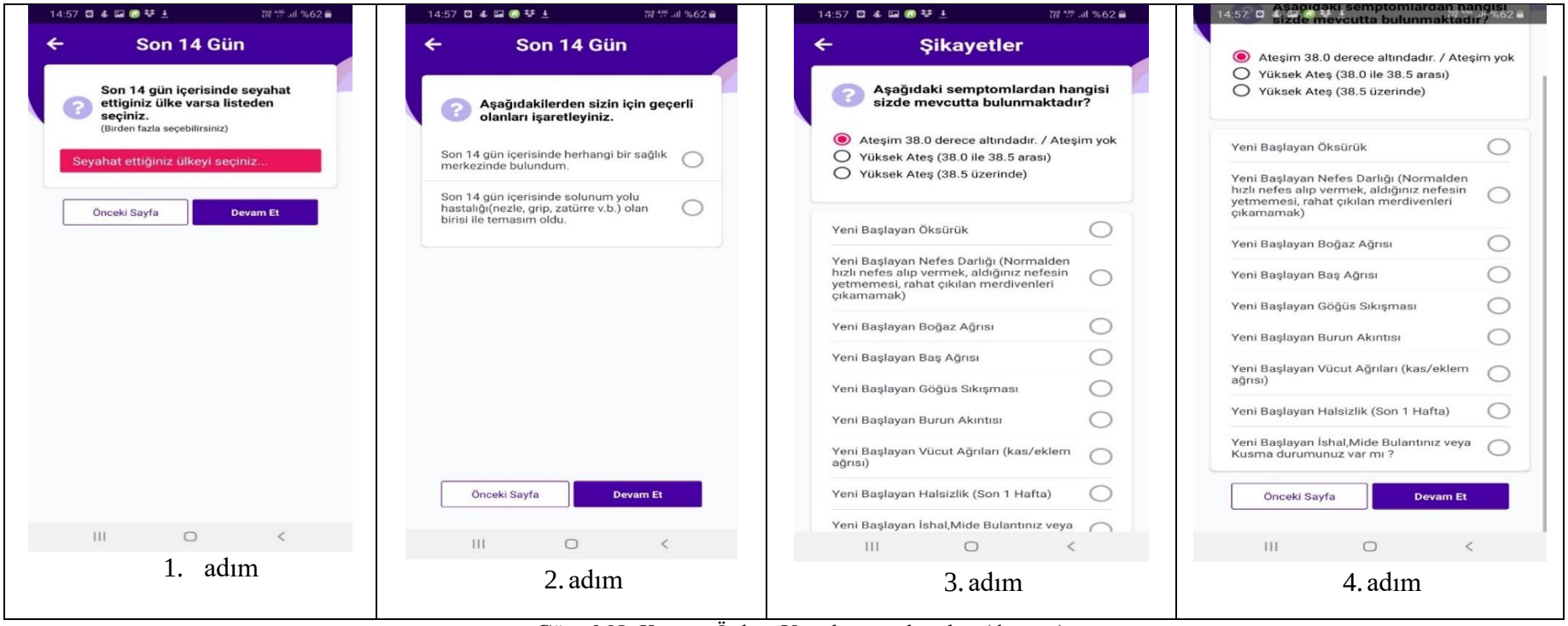
Tablo 5. Korona Önlem uygulamasının ekranları



Görsel 81. Korona Önlem Uygulaması ekranları

Uygulamaya işlenen kişisel bilgiler: T.C. kimlik numarası, baba adı, doğum yılı, telefon numarası, adı, soyadı, cinsiyeti ve yaşı biçimindedir (Görsel 81).

Tablo 5. Korona önlem uygulamasının ekranları (devamı)



Görsel 82. Korona Önlem Uygulaması ekranları (devamı)

Uygulama ayrıca kullanıcının sağlık çalışanı olup olmadığını sorgulamaktadır. Uygulamanın 3. ve 4. adımlarında kronik hastalık bilgisi sorgulanmaktadır (Görsel 82).

Korona Önlem uygulamasına istenen bilgiler kullanıcı tarafından işaretlendikten sonra kullanıcının kronik bir hastalığı olup olmadığı sorgulanmaktadır (Görsel 81, 3.adım). Kullanıcı tarafından kronik hastalık bilgisi kaydedildikten sonra kişinin son 14 gün içerisinde başka bir ülkeye seyahat edip etmediği sorgulanmaktadır (Görsel 82, 1.adım). Bu bilgilerin ardından kullanıcının semptom bilgileri sorgulanmaktadır (Görsel 82, 4.adım). Herhangi bir semptom göstermediği yönünde işaretleme yapılırsa kullanıcıya koronavirüs hastalığı ile karşılaşma ihtimalinin düşük olduğu bilgisi verilmektedir.

Bütün bilgiler girildikten sonra uygulamanın Sonuç ekranında koronaya yakalanma olasılığı açıklanmaktadır (Görsel 83). Uygulama bu yönleriyle e-Nabız uygulamasında bulunan "Neyim Var?" uygulamasına benzer biçimde çalışmaktadır.

Görsel 83. Korona Önlem sonuç ekranı

Korona Önlem uygulamasının aydınlatma metni aşağıdaki şekildedir:

Aydınlatma Metni

Bu Aydınlatma Metni, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("KVK Kanunu") 10 uncu maddesi uyarınca hazırlanmıştır.

Veri Sorumlusunun Kimliği: e-Nabız'da işlenen kişisel verileriniz bakımından veri sorumlusu T.C. Sağlık Bakanlığı'dır.

Kişisel Verilerin İşlenme Amaçları: Bu uygulamada yalnızca; yeni koronavirüs (COVID-19) semptomlarına göre ön değerlendirme yapmak ve yapılan ön değerlendirmenin olumlu çıkması durumunda bir sağlık tesisini ziyaret etmeniz tavsiyesinde bulunmak, ayrıca girilen bilgilerle istatistiki çalışma yapmak amaçlarıyla kimlik bilgileriniz, iletişim bilgileriniz, IP adresiniz ve sağlık verileriniz işlenmektedir.

Kişisel Verilerin Aktarımı: Bu uygulamada işlenen kişisel verileriniz, hiçbir amaçla üçüncü taraflara (kişi, kurum ve kuruluşlara) aktarılmamaktadır.

Kişisel Veri Toplamanın Yöntemi ve Hukuki Sebebi: Kişisel verileriniz tamamen otomatik yollarla (bu uygulama aracılığı ile) elde edilmekte olup kişisel verilerinizin işlenmesinin hukuki dayanağı, KVK Kanunu'nun 6 ncı maddesinin üçüncü fıkrası uyarınca kamu sağlığının korunmasıdır.

İlgili Kişilerin Hakları: KVK Kanunu'nun 11 inci maddesinde yer alan haklarınızı, KVK Kanunu'nun 13 üncü maddesi ile Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ hükümleri çerçevesinde Bakanlığa başvurmak suretiyle kullanabilir.

Veri Sorumlusuna Başvuru: KVK Kanunu'nun 13 üncü maddesi uyarınca yapılacak yazılı başvurular "T.C. Sağlık Bakanlığı, Üniversiteler Mahallesi, 6001. Cadde, No:9, Çankaya, Ankara" adresine; Kayıtlı Elektronik Posta (KEP) ile yapılacak başvurular ise "sb@hs01.kep.tr" adresine iletilmelidir.

4.2.5. Veri Tabanlarının İlkelere Göre Uyumluluklarının İncelenmesi

Toplum yararı ilkesi: Toplum yararı ilkesi ile uyumlu bir veri tabanı için aşağıdaki üç soruya yanıt aranması gerekmektedir. Bu sorulardan ilki veri tabanlarına işlenen bilgiler halk sağlığı hedeflerine[11] katkıda bulunuyor mu? İkinci soru veriler toplanırken insan haklarına saygı gösteriliyor mu? Üçüncü soru ise verilerin nasıl kullanıldığı konusunda bireyler söz sahibi mi?

Veri tabanlarına işlenen bilgiler halk sağlığı hedeflerine katkıda bulunuyor mu?

Kişisel sağlık kayıt sistemi olarak kullanılan e-Nabız uygulamasında işlenen bilgiler incelendiğinde, doğrudan halk sağlığı hedeflerine katkıda bulunmayacak türde kişisel bilgi kaydedildiği saptanmıştır. Buna göre kullanıcının kimlik bilgileri, adres, iletişim bilgileri, hamilelik testleri, alkol-madde-sigara kullanımı, eğitime devam etme

[11]Dünya Sağlık Örgütü "21. Yüzyıl İçin Herkes İçin Sağlık 21 Hedef" belirlemiştir. Tez kapsamında halk sağlığı hedefleri olarak, DSÖ'nün belirlemiş olduğu bu hedefler dayanak alınmıştır.

durumu, gelir durumu, ailesinde intihar bilgisi, cinsel partner bilgileri, kişisel bakım, kişisel hijyen, mahkumiyet/tutukluluk durumu, 15-46 yaş arası kadınların doğum, düşük durumu ve sayıları, babanın kan grubu, doğum ya da düşükle sonuçlanan tüm gebelikler gibi çok özel nitelikteki bilgiler sisteme işlenmektedir. Bu bilgilerin bazıları halk sağlığı hedefleri için gerekli olsa da cinsel partner bilgileri gibi bazı bilgilerin işlenmesi bu ilke açısından tartışmalıdır.

Birinci basamak sağlık hizmetleri kapsamında incelenen Hızır AHBS veri tabanına işlenen bilgiler incelendiğinde çoğunlukla halk sağlığı hedeflerine katkıda bulunabilecek türdeki sağlık verileri işlenmektedir. Bununla birlikte intihar girişim bilgisi, mahkumiyet/tutukluluk durumu, gebelikle ilgili çok ayrıntılı bilgiler ve kadına şiddetle ilgili bilgiler gibi çok özel bilgiler işlenmektedir. Bu bilgiler halk sağlığı hedeflerine katkıda bulunabilir. Ancak halk sağlığı hedefleri için bu bilgilerin kimlik bilgileri ile birlikte işlenmesinin gerekli olup olmadığı tartışmalıdır.

Yataklı tedavi hizmetleri kapsamında kullanılan MİA MED veri tabanı, intihar girişimi bilgisi, gebelikle ilgili ayrıntılı bilgiler ve kadına şiddetle ilgili bilgiler gibi çok özel kişisel bilgi işlediği saptanmıştır.

Veri tabanlarına işlenen sağlık verilerinin işlenme gerekçeleri, Sağlık Bakanlığı'nın yayımlamış olduğu Ulusal Sağlık Veri Sözlüğünde açıklanmaktadır. Sözlükte belirtilen bazı sağlık verilerinin gerekçeleri toplum yararı açısından sorgulanmış ve Türkiye'deki mevcut durum ile birlikte değerlendirilmiştir. Buna göre işlenen birçok veri, toplum yararı açısından gerekli olabilecek verilerden oluşmaktadır. Ancak bu verilerin kimlik bilgileri içermesi ve beraberinde yaratabileceği riskler birlikte değerlendirildiğinde toplum yararı ilkesi açısından bazı verilerin işlenmemesi gerektiği sonucuna ulaşılmıştır.

Veriler toplanırken insan haklarına saygı gösteriliyor mu?

Söz konusu sağlık verilerinin işlenmesi olduğu için en temel insan hakları ile yakından ilişkilidir. Buna göre özel yaşamın gizliliği hakkı, kişisel verilerin korunması hakkı, sağlık hakkı ve kişilik haklarıdır. Sağlık verisi işlenirken kişilik haklarının korunabilmesi için kişinin özgür ve aydınlatılmış onamını vermiş olması ve bu onamı istediği zaman geri çekebilmesi gerekir. Sağlık verisi işlenen veri tabanlarının kişilik

haklarını koruyacak niteliklerde özelliklere sahip olup olmadığına göre değerlendirme yapılabilir. Buna göre;

E-Nabız uygulamasına işlenecek veriler için uygulama gönüllülüğe dayalıdır. İşlenecek veriler için aydınlatılmış onam metni bulunmakta ve bu metinde hangi bilgilerin işlendiği açıklanmaktadır.

Hızır AHBS ve MİA MED uygulamalarına işlenen veriler için sistem üzerinde aydınlatılmış onam alınmasına dair herhangi bir özellik saptanmamıştır. Sağlık çalışanlarının doğru bir şekilde onam alamaması, yalnızca hukuki bir güvence olarak onam alınması, olumsuz çalışma koşulları nedeniyle onam alınamaması gibi nedenler olmakla birlikte veri tabanı üzerinde işlenecek hemen her bilgi için aydınlatılmış onam alındığının işaretlenebilmesi gerekir. Dolayısıyla Hızır AHBS ve MİA MED sistemleri için verinin işlenmesi aşamasında aydınlatılmış onam açısından insan haklarına saygı gösterildiğine işaret eden bir özellik saptanmamıştır.

Verilerin nasıl kullanıldığı konusunda bireyler söz sahibi mi?

Hızır AHBS ve MİA MED veri tabanlarına işlenen veriler için bireylerin hem işlenme aşamasında hem de daha sonra verilerin nasıl kullanılacağına ilişkin mevcut durumda herhangi bir söz sahibi değildir.

Minimum veri ilkesi: Toplum yararı ilkesi ile uyumlu olmadığı saptanan veri tabanlarının, bu ilkeye de aykırı olduğu belirlenmiştir. E-Nabız uygulamasında, kimlik bilgileri, adres, iletişim bilgileri, hamilelik testleri, sağlık geçmişi, özürlülük durumu, medeni hal, alkol-madde-sigara kullanımı, iş, meslek, öğrenim durumu, eğitim kurumuna devam etme durumu, gelir durumu, ailesinde intihar geçmişi, cinsel partner bilgileri, kişisel bakım, kişisel hijyen, mahkumiyet durumu, hastalık şikayetleri, hastanın anamnezi, bütün tetkik sonuçları, tetkik istenen kurumlar, 15-46 yaş arası kadınların, doğum, düşük türü ve sayıları, kadın sağlığı işlemleri, kullanılan aile planlaması yöntemi, son adet tarihi, babanın kan durumu, doğum ya da gebelikle sonuçlanan tüm gebelikler, ağız ve diş sağlığı ile ilgili tüm koruyucu hekimlik, teşhis ve tedavi işlemleri gibi birçok bilgi çok ayrıntılı olacak şekilde bulunmaktadır. Bu bilgilerden hamilelik testleri, ailesinde intihar geçmişi, mahkumiyet durumu, 15-46 yaş arası kadınların, doğum, düşük türü ve sayıları ve babanın kan durumu gibi özel

nitelikteki bilgilerin e-Nabız kaydında bulunması, verinin minimum veri ilkesine göre toplanmadığına işaret etmektedir. Çünkü bu veriler toplum yararı ilkesi açısından doğrudan gerekli değildir.

Ulusal Sağlık Veri Sözlüğünde belirtilen veri toplama gerekçeleri sorgulanmış, örneğin Gebelik Sonucu Veri Setinin "gebe olduğu tespit edilmiş olsun ya da olmasın, doğum ya da düşükle sonuçlanan tüm gebelikler ile tespiti yapılıp izlemi yapılmakta iken sahte gebelik olduğu tespit edilen gebelikleri kapsadığı" belirtilmektedir. Bu veri setinin hem gebe hem de bebek sağlığı açısından önemli veriler sunduğu, toplanan verilerin, gebe ve bebek sağlığının takip edilmesinde, verilen hizmetin analizinde ve sağlık hizmetlerinin planlanmasında kullanılması nedeniyle verinin toplandığı açıklanmaktadır. Bu veri setinin toplum yararı açısından değeri sorgulandığında verinin işlenmesi haklı çıkarılabilir görünmektedir. Ancak verinin kapsamı dikkate alındığında, gebelik ile ilgili bilgi alanı oldukça geniş tutulmaktadır. Bununla birlikte toplum yararına kullanılacak verinin kimlik bilgileri gerektirmemesi nedeniyle, belirtilen veri setinde kimlik bilgilerinin bulunması ve incelenen veri tabanlarında sonsuz sayıda verinin kimlik bilgileri ile işlenebildiği saptamasından hareketle minimum veri ilkesi ile uyumlu bir yaklaşımdan söz edilememektedir.

Veri tabanlarında işlenen bazı verilerin amaçla bağlantılı, sınırlı ve ölçülü bir şekilde işlenmediği ve kişisel verilerin işlenmesi gerekliliğinin toplum yararına uygunluğunun değerlendirilmesinin takip edilen amaç(lar) ışığında yapılmadığı saptanmıştır.

Eşitlik ve adalet ilkesi: Minimum veri ilkesi ile uyumlu bir şekilde işlenecek sağlık verisi eşitlik ve adalet ilkesine uygun olarak da işlenmelidir. Eşitlik ve adalet ilkesine göre sağlık hakkı kapsamında sağlık veri tabanlarına herkesin erişebilir olması gerekir. Buna göre e-Nabız uygulamasını isteyen herkesin kullanabilmesi, Hızır AHBS ve MİA MED veri tabanlarına ise işlenen kişisel sağlık verilerine dilediği zaman erişim sağlanabilmelidir. Genel olarak bilgi ve iletişim teknolojilerine kültür, dil, gelir düzeyi ve yaş gibi değişkenler açısından e-Nabız uygulamasına erişim sorunları yaşanabilmektedir. Günümüzde her dört kişiden birinin e-Nabız sistemini kullandığı belirtilmektedir (Sağlık Bakanlığı, 2021). E-Nabız uygulamasına herkesin erişebilir olması çok önemlidir ancak eşitlik ve adalet ilkesi açısından bu sayının yeterli olmadığı ileri sürülebilir. Yanı sıra uygulamanın okur-yazar olmayanlar, düşük gelirli gruplar,

yaşlılar gibi dezavantajlı gruplar açısından ve coğrafi koşulların uygun olmaması gibi nedenlerden dolayı eşitlik ve adalet ilkesi ile uyumluluktan söz edilememektedir.

Özerklik ilkesi:

E-Nabız uygulaması*:* E-Nabız sistemi üzerinde profil oluşturma (kayıt olmak), yeni kişisel bilgiler ekleyebilmek, hangi bilgilerin bulunduğu bilgisine erişim ve bilgilerin düzeltilmesini isteyebilmek gibi konularda özerklik ilkesi geçerliliğini korurken, bilgilendirme açısından profil oluşturma veya karar verme için hangi algoritmaların kullanıldığı bilgisi ile kayıtlı sağlık verilerini silebilme özelliğinin bulunmadığı saptanmıştır. Özerklik açısından bir diğer özellik, uygulama üzerinde bazı bilgilerin akışta gizlenebilmesi kullanıcıya tanımlanmıştır.

Uygulamanın Aydınlatma metni aşağıdaki şekildedir:

> **Aydınlatma Metni**[12]
>
> Bu Aydınlatma Metni, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("KVK Kanunu") "Veri Sorumlusunun Aydınlatma Yükümlülüğü" kenar başlıklı 10 uncu maddesi uyarınca ve KVK Kanunu kapsamında veri sorumlusu olan T.C. Sağlık Bakanlığı (Bakanlık) tarafından, e-Nabız kullanıcılarına, kullanıcılara ait kişisel veriler hususunda bilgilendirme yapmak amacıyla hazırlanmıştır. KVK Kanunu uyarınca veri sorumlusu sıfatını haiz Bakanlığın merkez adresi "Bilkent Yerleşkesi, Üniversiteler Mah. Dumlupınar Bulvarı 6001. Cad. No:9 Çankaya/Ankara 06800"dir.
>
> **Veri Sorumlusunun Kimliği:** e-Nabız'da işlenen kişisel verileriniz bakımından veri sorumlusu T.C. Sağlık Bakanlığı'dır.
>
> **Kişisel Verilerin İşlenme Amaçları:** Bu uygulamada aşağıda yer alan kişisel verileriniz şu amaçlarla işlenmektedir:
>
> - **Kimlik verisi:** Kimlik bilgileriniz kimliğinizin doğrulanması, sağlık hizmeti süreçlerinin yürütülmesi/denetimi/analizi/izlemi amacıyla işlenmektedir.
>
> - **İletişim verisi:** İletişim bilgileriniz acil durum yönetimi süreçlerinin yürütülmesi, sağlık hizmetlerine yönelik iletişim faaliyetlerinin yürütülmesi, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmeti süreçlerinin yürütülmesi/denetimi/analizi/izlemi amacıyla işlenmektedir.

[12] Güncelleme 22 Ağustos 2022.

- Ceza mahkumiyeti ve güvenlik tedbirleri verisi: Cezaevi öyküsü bilginiz var ise bu bilgiler tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetlerinin planlanması/yönetilmesi, sağlık hizmeti süreçlerinin yürütülmesi/denetimi/analizi/raporlanması/izlemi amacıyla işlenmektedir.

- İşlem güvenliği verisi: İşlem güvenliği bilgileriniz bilgi güvenliği süreçlerinin yürütülmesi, erişim yetkilerinin yürütülmesi amacıyla işlenmektedir.

- Özlük verisi: Özlük bilgileriniz acil durum yönetimi süreçlerinin yürütülmesi, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmeti süreçlerinin yürütülmesi/denetimi/analizi/raporlanması/izlemi amacıyla işlenmektedir.

- Finans verisi: Finans bilgileriniz faaliyetlerin mevzuata uygun yürütülmesi, kamu finansman verimliliğinin artırılması, iş faaliyetlerinin yürütülmesi/denetimi, sağlık hizmeti süreçlerinin yürütülmesi, finans ve muhasebe işlerinin yürütülmesi amacıyla işlenmektedir.

- Lokasyon verisi: Konum bilgileriniz acil durum yönetimi süreçlerinin yürütülmesi, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, iletişim faaliyetlerinin yürütülmesi, sağlık hizmeti süreçlerinin yürütülmesi amacıyla işlenmektedir.

- Sağlık verisi: Sağlık bilgileriniz iş sürekliliğinin sağlanması faaliyetlerinin yürütülmesi/ denetimi/analizi/raporlanması/izlemi, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, kamu finansman verimliliğinin artırılması, sağlık hizmetlerinin yürütülmesi/planlanması/yönetilmesi, sağlık hizmetine yönelik bildirim süreçlerinin (SMS, Push Notification, e-Posta vb.) yürütülmesi amacıyla işlenmektedir.

- Mesleki deneyim verisi: Meslek bilgileriniz iş sürekliliğinin sağlanması faaliyetlerinin yürütülmesi, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmeti süreçlerinin yürütülmesi amacıyla işlenmektedir.

- Görsel ve işitsel veri: Sağlık probleminiz ile ilgili fotoğrafınız ve profil içerisinde eklenen fotoğrafınız iş sürekliliğinin sağlanması faaliyetlerinin yürütülmesi, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmeti süreçlerinin yürütülmesi amacıyla işlenmektedir.

Kişisel Verilerin Aktarımı: Sağlık hizmeti sunan özel sağlık kuruluşlarından hizmet almanız halinde, e-Nabız'daki kişisel verileriniz KVK Kanunu'nun 6 ncı maddesinin üçüncü fıkrası kapsamında mevcut güvenlik tercihleriniz doğrultusunda ilgili hekim(ler)in erişimine sunulabilmektedir. Yoğun bakım veya acil sağlık hizmeti almanız halinde, durumunuzun hayati tehlike arz edebilecek olması sebebiyle e-Nabız hesabınızdaki veriler, ilgili hekimin erişimine sunulabilmektedir[13]. Ayrıca, almış olduğunuz sağlık hizmeti bedelinin Sosyal Güvenlik Kurumu tarafından karşılanacak

[13] Bu ifade daha sonra eklenmiştir. Karşılaştırmak için bkz Görsel 13.

olması halinde, sağlık hizmeti süreçlerinizin yürütülmesi amacıyla kişisel verileriniz T.C. Sosyal Güvenlik Kurumunun erişimine sunulabilmektedir. KVK Kanununun 28 inci maddesinin ilk fıkrasında yer alan muafiyet halleri saklıdır.

Hasta Takip Ekranları: Sağlık tesislerinde muayene sırasının takip edildiği hasta takip ve poliklinik çağrı ekranlarında adınız ve soyadınızın maskelenerek (Ör: Ay*** Ün***) gösterilmesini talep etmeniz durumunda, e-Nabız profili üzerinde yer alan Profil Düzenleme alanında "Sağlık kuruluşlarındaki hasta takip ve poliklinik çağrı ekranlarında adımın ve soyadımın yıldızlanarak gösterilmesini istiyorum. Adımın ve soyadımın açıkça belirtilmesini istemiyorum." seçeneğini işaretleme imkanınız bulunmaktadır.[14]

İki Aşamalı Güvenli Giriş: e-Nabız profiline girişiniz esnasında TC kimlik numaranız ve e-Nabız şifrenizi girdikten sonra profilinizde yer alan birincil olarak kayıtlı telefon numarasına kısa mesaj (SMS) ile şifre gönderilebilmekte olup bu özelliği e-Nabız profilinizdeki Profil Düzenleme alanında aktifleştirebilme imkanınız bulunmaktadır.[15]

Kişisel Veri Toplamanın Yöntemi ve Hukuki Sebebi: Kişisel verileriniz e-Nabız Sistemi aracılığı ile otomatik yollarla veya boy, kilo gibi bilgilerin manuel olarak sizin tarafınızdan profilinize eklenmesi suretiyle elde edilmektedir. Kişisel verileriniz, KVK Kanunu'nun 5 inci maddesinin ikinci fıkrasının (a) bendindeki "Kanunlarda açıkça öngörülmesi", (ç) bendindeki "Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması" hukuki sebepleri ile 6 ncı maddesinin üçüncü fıkrası uyarınca; 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 veya yetkili kişiler veya yetkili kurum/kuruluşlar tarafından işlenmektedir.

İlgili Kişilerin Hakları ve Veri Sorumlusuna Başvuru: e-Nabız kullanıcıları KVK Kanunu'nun 11 inci maddesinde düzenlenen haklarını, KVK Kanunu'nun 13 üncü maddesi ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ hükümleri çerçevesinde Bakanlığa başvurmak suretiyle kullanabilir. KVK Kanunu'nun 13 üncü maddesi uyarınca yapılacak yazılı başvurular "T.C. Sağlık Bakanlığı, Üniversiteler Mahallesi, 6001. Cadde, No:9, Çankaya, Ankara" adresine; Kayıtlı Elektronik Posta (KEP) ile yapılacak başvurular ise "sb@hs01.kep.tr" adresine iletilmelidir.

Bu metin "aydınlatılmış onam" açısından incelendiğinde, metin içerisinde verilen onamın geri çekilebileceğine ilişkin bir bilgi bulunmadığı saptanmıştır. Metin açık ve anlaşılır olmakla birlikte bilgilendirme açısından yetersiz bulunmuştur. Buna göre, metinde veri sorumlusu açıklanmakta, hangi tür kişisel verilerin işleneceği ve üçüncü

[14] Bu ifade daha sonra eklenmiştir. Karşılaştırmak için bkz Görsel 13.
[15] Bu ifade daha sonra eklenmiştir. Karşılaştırmak için bkz Görsel 13.

taraflarla paylaşım bilgileri verilmekte, kişisel veri toplamanın yöntemi ve hukuki sebebi ve ilgili kişinin hakları konusunda KVK Kanunu'nun ilgili maddesi belirtilmiş, ancak verinin toplanması, depolanması ve kullanımındaki risklere ilişkin herhangi bir bilgilendirme yapılmamıştır. Bununla birlikte bireylerin istedikleri zaman onamlarını değiştirebileceği, sağlık veri tabanından bilgilerinin çekilmesini isteyebileceği ve bilgilerin ticari amaçlarla söz konusu kullanımı konularında bilgilendirme yapılmadığı saptanmıştır. Yanı sıra aydınlatılmış onam kapsamında "ret" hakkının kullanılabileceğine ilişkin bir ifade metinde yer almamaktadır.

Hızır AHBS ve MİA MED veri tabanları*:* Hızır AHBS veri tabanı, aile hekimliklerinde çalışan hekimler ve hemşireler tarafından kullanılmaktadır. Bu nedenle hastanın veri tabanına doğrudan bir erişimi bulunmamaktadır. Hastaların, aile hekiminden kendileri hakkında sahip oldukları bilgilere erişimini isteyebilmesi, verilerin kullanımı konusunda hekimden bilgi talep edebilmesi ve bilgilerinin eksik veya hatalarının düzeltilmesini isteyebilmesi aile hekimine bağlıdır. MİA MED veri tabanı da hastaların doğrudan erişim yetkisi yoktur. Hastalar, kendileri hakkında sahip oldukları bilgileri ilgili sağlık çalışanından talep edebilirler. Hastanın özerkliği açısından bir diğer önemli bulgu, hasta yaptırmış olduğu tetkiklerin sonuçlarını hastanenin sonuç ekranından takip edebilmektedir. Her iki veri tabanında hekimlerin hasta bilgilerini veri tabanına kaydetmeleri ve bazı sağlık verilerini Sağlık Net veya USS'ye göndermek gibi bildirim yükümlülükleri bulunmaktadır. Bu durum hekimin özerkliği açısından tartışmalı bulunmuştur.

Mahremiyet ve Gizlilik ilkesi: Tez kapsamında tanımlanan mahremiyet ve gizlilik ilkesine göre veri tabanlarının tasarım açısından minimum veri ilkesine uygun olması gerekmektedir. Bununla birlikte bu ilke, mevcut durumda veri tabanları aracılığı ile toplanmış olan sağlık verisinin mahremiyet ve gizliliğinin korunup korunmadığı ile ilgilidir. Buna karşın incelenen üç veri tabanının uygulama özellikleri açısından mahremiyet ve gizlilik ilkesi ile uyumlulukları değerlendirilebilir.

Üç veri tabanının da minimum veri ilkesi ile uyumlu olmadığı saptamasından hareketle mahremiyet ve gizlilik ilkesi ile de uyumlu olmadığı belirtilebilir. Bununla birlikte mahremiyet ve gizlilik ilkesini, minimum veri ilkesi ile birlikte değerlendirmek gerekir. Buna göre hangi verinin gerekli olduğu, hangi veri gerekli olsa dahi

mahremiyet ve gizlilik ilkesi açısından risk oluşturabileceği ve bu riskin göze alınıp alınamayacağının ayrıntılı değerlendirilmesi, tartışma bölümünde ele alındığı için burada yer verilmemiştir.

Bununla birlikte mahremiyet ve gizlilik ilkesi ile ilgili olarak veri tabanlarında saptanan sorunlara aşağıda yer verilmiştir.

E-Nabız uygulaması: E-Nabız uygulamasının *Gizlilik, Kullanım ve Telif Hakları* metninde; "Kişilerin E-Nabız'daki sağlık bilgilerini sadece kişilerin onayını alan hekimler ve/veya kişiler görebilir. Kişilerin, E-Nabız'da paylaşmış olduğu bilgiler, kişilerin onayı dışında ya da yargı kararı ve/veya yasal bir yükümlülük altında bulunmadığı sürece herhangi bir üçüncü şahıs, kurum ve kuruluş ile hiçbir nedenden ötürü paylaşılmayacak ya da verilmeyecektir. Yasal düzenlemelerle bu bilgilerin açıklanmasını gerektiren bir durum gerçekleşmediği sürece hiçbir istisna ile bu bilgiler açıklanmayacaktır." bilgisi yer almaktadır[16]. Bu ifade açısından mahremiyet ve gizlilik korunmaktadır.

Mahremiyet ve gizlilik ilkesine uyumluluğu belirlemek için anonimleştirmeye özen gösterilmesi gerekmektedir. Uygulamanın ara yüzünde anonimleştirmeye yönelik herhangi bir teknik donanım saptanmamış, yalnızca bazı bilgilerin akışta gizlenebileceği saptanmıştır.

E-Nabız uygulamasına üçüncü tarafların erişimi için kullanıcının cep telefonuna gelen kodun aile hekimi ile paylaşılması gerekmektedir. Bu özellik kullanıcının mahremiyet ve gizliliğini korumaya yönelik bir özellik olarak belirtilebilir. Bununla birlikte uygulamanın bildirimler ekranı incelendiğinde, kullanıcının e-Nabız kaydına erişim sağlayan kişilerin (hekimlerin) erişim bilgileri bulunmaktadır (Görsel 16). Bu özellik, kullanıcıyı bilgilendirmesi açısından olumlu; ancak erişim sağlayan kişinin kullanıcının izni olmadan erişim sağlayabilmesi nedeniyle mahremiyet ve gizlilik ilkesi ile uyumlu olmadığını göstermektedir.

Hızır AHBS uygulaması: Uygulamanın mahremiyet ve gizlilik ilkesi ile uyumlu olabilecek bir özelliği olarak gizli hasta bildirimi yapılabilmesi özelliği bulunmaktadır.

[16] Güncelleme 22 Ağu. 2022

Buna göre örneğin HIV hastası ile ilgili bilgiler, oluşturulan hasta kodu ile sistem üzerinden Sağlık Net'e gönderilmektedir.

Mahremiyet ve gizlilik ilkesi ile uyumlu bir özellik olarak, hekim sistem üzerinden hastanın e-Nabız kaydına girmek istediğinde hastanın telefonuna gelen kodu, hastadan alması gerekmektedir.

Bununla birlikte, Hızır AHBS uygulamasına bilgileri girilen hastanın ekranını kurumda çalışan diğer aile hekimleri hasta kendisine kayıtlı olmasa dahi kendi ekranlarından görüntüleyebilmektedir. Kurumda çalışan hemşireler de kendi ekranları üzerinden diledikleri hastanın bilgilerine erişim sağlayabilmektedir. Hasta ve hekim arasındaki mahremiyet olgusu, hasta ve sağlık çalışanları biçiminde algılanmaktadır. Bu durum başta olmak üzere yukarıda belirtilen nedenlerle Hızır AHBS uygulaması, mahremiyet ve gizlilik ilkesi ile uyumlu bulunmamıştır.

MİA MED veri tabanı: MİA MED hastanenin bütün işleri için kullanılan bir veri tabanıdır. Bu nedenle bazı yetkili olmayan kişilerin hasta verilerine erişim sağlayabilmesi mümkündür. Bununla birlikte bir poliklinik ekranından hastanın diğer poliklinik ziyaretlerine erişim sağlanabilmektedir. Örneğin Aile Hekimliği Polikliniği ekranından hastanın Ruh Sağlığı Polikliniğine yaptığı ziyaretleri görüntülemek mümkündür. Bu iki nedenden dolayı MİA MED veri tabanı, mahremiyet ve gizlilik ilkesi ile uyumlu bulunmamıştır.

4.3.Mobil Uygulamaların İlgili Kılavuza Göre İncelenmesi

Mobil uygulamaların etik açısından analizi için Avrupa Konseyi'nin "Guidance on Apps supporting the fight against COVID-19 pandemic in relation to data protection" kılavuzunda belirtilen ilkeler temel alınmıştır (European Commission, 2019). Bu kılavuz, Covid-19 ile mücadele kapsamında çıkarılan mobil uygulamaların güvenilir ve hesap verilebilir kullanımı için rehberlik etmektedir. Bu kılavuza göre incelenen HES ve Korona Önlem uygulamasına dair sonuçlar şu şekildedir:

Uygulamanın cihaza yüklenmesi gönüllü olmalı ve uygulamayı indirmemeye /kullanmamaya karar veren kişi için herhangi bir olumsuz sonuç doğurmamalıdır (Md.3.2)

Her iki uygulamanın cihaza yüklenmesi, gönüllülüğe dayalıdır. HES kodu uygulaması zorunlu tutulduğu için uygulamayı kullanan kişiler bu kodu nispeten daha kolay edinebilmektedir. Buna karşın Korona Önlem Uygulamasını kullanmak istemeyen kişiler için herhangi bir olumsuz sonuç saptanmamıştır.

Farklı uygulama işlevleri (örn. bilgi, semptom kontrol, temas izleme ve uyarı işlevleri), bireyin her bir işlev için özel olarak kendi onayını verebilmesi için bir araya getirilmemelidir. Bu, sağlayıcı tarafından bir seçenek olarak sunuluyorsa, kullanıcının farklı uygulama işlevlerini birleştirmesini engellememelidir (Md.3.2).

Uygulamanın kurulum aşamasında, telefona gelen kısa mesaj ile hesap doğrulaması yapılmakta ve koronavirüs olma ihtimaline karşı mini bir test uygulanmaktadır. Test soruları yanıtlandıktan sonra konum verisi ve Bluetooth servisine erişim isteği kullanıcıdan ayrı ayrı istenmektedir. Bu bilgiler sağlayıcı tarafından bir seçenek olarak sunulmamakta, zorunlu olarak işlenmekte, bu konuda kullanıcı ekranında bilgilendirme yazısı yer almaktadır (Görsel 75). Bu işlevler onam alınabilmesi için kullanıcıya ayrı ayrı sunulmakta ve kullanıcı bu işlevlere onam vermeden uygulamanın diğer işlevlerini kullanamamaktadır. Uygulamanın kurulumu tamamlandıktan sonra tercihe bağlı olarak konum verisi ve Bluetooth servisine erişim kapatılabilmektedir.

HES uygulaması, İlacımı Kontrol Et, Maskemi Kontrol Et ve Korona Önlem Uygulaması gibi uygulamalarla birleştirilmiştir. Bu uygulamalara erişim HES üzerinden sağlanabilmektedir. Korona Önlem Uygulaması ön tanıya yönelik bir uygulama olduğu için farklı özellikteki uygulamalar sisteme tanımlanmamıştır.

Yakınlık verileri kullanılıyorsa (Bluetooth servisi) bunlar kişinin cihazında saklanmalıdır. Bu veriler sağlık yetkilileriyle paylaşılacaksa, ancak ilgili kişinin COVID-19 ile enfekte olduğu teyit edildikten sonra ve bunu yapmayı seçmesi şartıyla paylaşılmalıdır. Sağlık yetkilileri, enfeksiyon riski taşıyan kişilerle iletişim kurabilmeleri için yalnızca virüs bulaşmış bir kişinin cihazından gelen yakınlık verilerine erişebilmelidir (Md.3.2).

HES uygulamasında yakınlık verisi olarak konum verisi ve Bluetooth servisi kullanılmaktadır. Covid-19 ile enfekte olduğu tespit edilen kişinin verileri, hem sağlık yetkilileri hem de İçişleri Bakanlığı ve kolluk kuvvetleri ile paylaşılmaktadır (Bkz s.166). HES kodu aracılığı ile yoğunluk takibi yapılmakta, virüs taşıyan kişilerin

bilgileri bu koda tanımlanmaktadır. Kod aracılığı ile virüs taşıdığı belirlenen kişilerin seyahatleri engellenmektedir. Verinin aktarımı için ayrıca onam istenmemekte, veri aktarımı yapılabileceği uygulamanın aydınlatma metninde açıklanmaktadır.

Korona Önlem Uygulamasında herhangi bir yakınlık verisi kullanılmamaktadır.

Sağlık yetkilileri, bireylere kişisel verilerinin işlenmesiyle ilgili tüm gerekli bilgileri sağlamalıdır (Md.3.2).

HES uygulamasının Gizlilik Politikası başlıklı metninde veri sorumlusunun kimliği, verinin işlenme amaçları, hangi kişisel bilgilerin işlendiği ve işlenen bilgilerin hangi taraflara aktarılacağı açıklanmaktadır.

Korona Önlem uygulamasının aydınlatma metninde, veri sorumlusunun kimliği, verinin işlenme amaçları, hangi kişisel bilgilerin işlendiği ve işlenen bilgilerin hiçbir amaçla üçüncü taraflarla paylaşılmayacağı açıklanmaktadır.

Kişiler GDPR kapsamındaki haklarını (özellikle erişim, düzeltme, silme) kullanabilmelidir (Md.3.2).

HES uygulamasına kaydedilen kişisel bilgilere erişim sağlanabilmekte, kaydedilen bilgileri düzeltme işlemleri yapılabilmektedir. Buna karşın kayıtlı olan kişisel bilgiler silinememektedir. Uygulamayı kullanmaktan vazgeçilmesi durumunda "hesabımı sil" seçeneği mevcuttur.

Korona Önlem uygulamasında profil oluşturulamadığı için bilgilere erişim, düzeltme ve silme gibi işlemler yapılamamaktadır.

Uygulamalar en geç pandeminin kontrol altına alındığı ilan edildiğinde devre dışı bırakılmalıdır; devre dışı bırakma, kullanıcı tarafından kurulumun kaldırılmasına bağlı olmamalıdır (Md.3.2).

Her iki uygulamanın devre dışı bırakılması, kullanıcı tarafından kurulumun cihazdan kaldırılmasına ("hesabımı sil" dahil) bağlıdır.

Uygulamaların yüklenmesi ve kullanıcının cihazında bilgilerin saklanması: kullanıcının cihazında bilgilerin depolanmasına veya halihazırda saklanan bilgilere erişim sağlanmasına yalnızca (i) kullanıcının onay vermesi veya (ii) depolama ve/veya erişim izni vermesi durumunda izin verilir (Md.3.3).

Her iki uygulamanın da cihaza yüklenmesi kullanıcının gönüllülüğüne bağlıdır. HES uygulamasına işlenen bilgilere erişim onayı, kurulum aşamasında alınmış onaya bağlıdır. Her iki uygulama için de kullanıcıdan ayrıca depolama ve her bilgi için ayrıca onam alınmamaktadır.

Onam, "özgürce verilmiş", "spesifik", "açık" ve "aydınlatılmış" olmalıdır. Bireyin net bir olumlu eylemiyle ifade edilmelidir.

Her iki uygulamayı kullanmak gönüllülüğe bağlıdır. İki uygulamanın da Aydınlatma metni, bireyin net bir olumlu eylemiyle ifade edebileceği *"anladım"* ibaresi ile son bulmaktadır. Buna karşın onamın aydınlatılmış olabilmesi için kişinin "anlaması" sağlanmalıdır. Kişinin anlamasının sağlanması, sağlık çalışanı tarafından yapılan aydınlatma ile mümkün olabilir. Bu nedenle uygulamalar için "aydınlatılmış olma" özelliğinin tam olarak sağlanmadığı söylenebilir.

Pandemi sürecinde HES uygulamasına tanımlanan HES kodu uygulaması zorunlu tutulmuştur. HES kodu uygulamasının hayata geçirilmesi ile birlikte temas takibi zorunlu bir şekilde gerçekleştirilmiştir. Kişiler HES kodunu paylaşmadan şehirlerarası uçak, tren ve otobüs yolculuğu için bilet satın alamamış, kamu kurumları, alışveriş merkezleri gibi birçok mekanın girişinde özel güvenlik görevlileri tarafından kişilerin HES kodu sorgulanmış, HES kodunu paylaşmak istemeyen kişilerin, bu yerlere girişi engellenmiştir. Dolayısıyla "özgürce verilmiş" bir onamdan bahsetmek mümkün değildir.

Enfekte kişi, potansiyel olarak temasta bulunduğu ve uyarılacak kişilerin kimliği hakkında bilgilendirilmemelidir. Enfekte kişinin kimliği, temasta bulunduğu kişilere açıklanmamalıdır. Son 16 gün içinde enfekte bir kişiyle temas halinde olduklarını kendilerine iletmeleri yeterlidir. Bu tür temasların zamanı ve yeri ile ilgili veriler saklanmamalıdır. Enfekte olduğu tespit edilen bir uygulama kullanıcısının temaslarını izlemek için, ulusal sağlık yetkilileri yalnızca, semptomların başlamasından 48 saat öncesinden 14 güne kadar enfekte kişinin temas halinde olduğu kişinin kimliği hakkında bilgilendirilmelidir (Md.3.3; Md.3.5).

Pandemi sürecinde kişilerin temas verileri, HES uygulamasının yanı sıra bu uygulamaya tanımlı HES kodu aracılığı ile toplanmıştır. Enfekte olduğu tespit edilen kişinin karantina sürecinde evini terk edip etmediği HES uygulaması ile sağlık

çalışanları tarafından takip edilmiştir. Sağlık çalışanları, enfekte olduğunu tespit ettiği kişiye potansiyel olarak temasta bulunduğu ve uyarılacak kişilerin kimliği hakkında bilgi vermemiştir. Enfekte kişinin kimliği de temasta bulunduğu kişilere açıklanmamıştır. Ancak diğer yandan pandemi sürecinde zorunlu tutulan ve geçici süreli HES kodu uygulaması ile kişilerin sağlık verileri herkes tarafından sorgulanabilmiştir (Zorer, 2021). Sağlık Bakanlığınca verilen "riskli" ya da "riskli değil" bilgileri, yapılan sorgulama sonucunda görüntülenebilmiştir.

HES uygulamasında "ihbarda bulun" özelliği bulunmaktadır. Bu özellik ile pandemi kullarını ihlal eden kişileri, vatandaşlar ihbar edebilmektedirler. Enfekte kişi hakkında bilinen kişisel bilgiler ve kişiye ait görüntüler paylaşılabilmektedir.

Veri işlemenin yasal dayanağı: Herhangi bir ulusal yasa, veri öznelerinin hak ve özgürlüklerini korumak için özel ve uygun önlemler sağlamalıdır. Genel bir kural olarak, bireylerin özgürlükleri üzerindeki etki ne kadar güçlüyse, ilgili kanunda buna karşılık gelen güvenceler de o kadar güçlü olmalıdır. Veri işlemede Covid-19, toplum sağlığının korunması için yasal bir dayanak oluşturur. Yasal bir dayanak olarak temel işleme amacı sağlanmalıdır (Md.3.3).

Her iki uygulamaya da işlenen verilerin yasal dayanağı, KVK Kanunu'nun 5. maddesinin ikinci fıkrasının a bendine dayandırılabilmektedir. Bu maddeye göre veri işlemek için *"Kanunlarda açıkça öngörülmesi"* gerekmektedir. Veri işlemede Covid-19'un toplum sağlığının korunması için yasal bir dayanak oluşturduğu kanun maddesi 6. maddenin 3. fıkrasında belirtilmektedir. Buna göre ilgili ifade şu şekildedir; "… 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.". Bu yasal dayanak ayrıca iki mobil uygulamanın aydınlatma metinlerinde belirtilmektedir.

Pandemi sürecinde zorunlu tutulan HES kodu uygulamasının, bireylerin özgürlükleri üzerindeki etki çok güçlü olmuştur. Bireylerin takibi bu kod aracılığı ile gerçekleşmiş, bu kodu paylaşmak istemeyen kişilerin bazı hizmetleri almalarına izin verilmemiştir. Bu kod, kişiye ait, tekil nitelikte kodlar olarak bireylere tanımlandığı için özel nitelikte

bir kişisel veridir. Bu verinin açık rızaya dayalı olmadan işlenebileceği, KVK Kanunu'nun 6. maddesinin 3. fıkrasına dayandırılmaktadır.

Uygulama kaldırıldığında kullanıcılar için hiçbir olumsuz sonuç ortaya çıkmamalıdır (Md.3.3).

Çalışmanın yazıldığı 2022 yılı itibarıyla HES kodu uygulaması kaldırılmış, HES uygulaması ve Korona Önlem uygulamalarının kullanımına bir süre devam edilmiştir. HES uygulaması PlayStore'da bulunurken Korona Önlem uygulaması PlayStore'dan kaldırılmıştır. Her iki uygulamanın da kaldırılmasının kullanıcılar için herhangi bir olumsuz sonuç ortaya çıkarması yönünde bir durum saptanmamıştır.

Veri minimizasyonu: Kişisel verinin işlenmesi sınırlı, amaçla bağlantılı ve ölçülü olmalıdır. Bilgi işlevselliği (Yalnızca gerekli olan bilgi işlenmeli, bilgi işlevselliğine sahip olmak için bir gerekçe olmadıkça sağlık yetkilileri hiçbir bilgiye erişememelidir). Semptom denetleyici ve tele-tıp işlevleri için ilgili mevzuatta işlenen kişisel veriler listelenmelidir (Md.3.4).

HES uygulamasında işlenen kişisel verilerin sınırlı, amaçla bağlantılı ve ölçülü olup olmadığını incelemek için uygulamaya işlenen kişisel bilgileri sorgulamak gerekir. Buna göre işlenen bilgiler incelendiğinde şu şekilde bir sınıflama yapılabilir:

Amaçla bağlantılı olabilecek veriler: konum verisi, kimlik bilgileri, iletişim bilgileri, sağlık verisi ve meslek verisi.

Amaçla bağlantılı ancak sınırlılık ve ölçülülüğe aykırı olabilecek veriler: Bluetooth verisi, kamera verisi, kişi listesi ve dosya verisi (video, ses, görüntü). Bluetooth servisine erişim için uygulamanın aydınlatma metninde belirtilen açıklama;

> "HES Uygulaması üzerinden izin vermeniz dahilinde kullanıcıların sosyal mesafeyi koruyarak sağlıklı kalmasına yardımcı olunması adına Bluetooth bilginiz işlenebilmektedir. Bu izin uygulama içerisinde gelecek olan uyarı penceresi sayesinde verilebilecektir."

Korona Önlem uygulamasına işlenen bilgiler açısından kılavuzda belirtilen *"information functionality"* (bilgi işlevselliği) terimine aykırı bulunmuştur. Buna göre uygulama amacı gereği herhangi bir kişisel bilgiyi işlemesi gerekli değildir. Ancak uygulama, T.C. kimlik numarası/Yabancı numarası, baba adı, doğum yılı, telefon numarası, adı, soyadı, cinsiyet, yaş, son 14 günde en uzun süre bulunulan il bilgisi ve

sağlık sektöründe çalışan biri olup olmadığı bilgilerini işlemektedir. Bu bilgilerden kişinin hangi kronik hastalıklara sahip olduğu ve son 14 gün içerisinde seyahat edilen ülke, sağlık merkezi ziyareti ve solunum yolu hastalığı olan biri ile temas bilgileri, bilgi işlevselliği açısından gerekli görünmektedir. Daha sonra ateş, öksürük, nefes darlığı, boğaz ağrısı, baş ağrısı, göğüs sıkışması ve burun akıntısı bilgileri işlenmektedir. Bu bilgiler de uygulamanın ön tanı koyabilmesi için gerekli olan bilgilerden oluşmaktadır. Bu bilgiler DSÖ'nün açıklamış olduğu koronavirüs hastalığına ilişkin en yaygın görülen belirtiler ile daha seyrek görülen belirtileri bir arada işlediği için bilgi işlevselliğine uygun görünmektedir[17] (WHO, 2021a).

Korona Önlem uygulamasının aydınlatma metni incelendiğinde, Covid-19 ile ilgili sağlık bilgilerinin işlendiği belirtilmiş; ancak hangi bilgilerin işlendiği metinde açıklanmamıştır (Bkz. s.172).

Enfeksiyon zincirinin kırılması için Bluetooth gibi yakınlık verileri, yalnızca gerçek bir enfeksiyon riski varsa oluşturulmalı ve kullanılmalıdır (Md.3.4).

HES uygulamasında Bluetooth verileri yakınlık verisi olarak işlenirken Korona Önlem uygulamasında herhangi bir yakınlık verisinin işlenmediği saptanmıştır.

Temas izlemek için konum verileri kullanılmamalıdır (Md.3.4).

HES uygulamasında temas izlemek için konum verisi zorunlu olarak işlenmektedir.

Bir uygulamanın her işlevi için bir amaç olmalıdır. İşlenen veriler Covid-19 ile mücadele kapsamı dışında kullanılmamalıdır (Md.3.5).

Temas takip uygulaması olarak kullanılan HES uygulamasına, bu işleve hizmet edecek verilerin işlenmesi amaçlanmaktadır. Uygulamanın aydınlatma metninde, işlenen verilerin Covid-19 ile mücadele kapsamı dışında kullanılmayacağı belirtilmektedir.

Ön tanı koymak için kullanıma koyulan Korona Önlem Uygulamasına, bu işlevin gereği olan sağlık verileri işlenmektedir. Uygulamanın aydınlatma metninde, işlenen verilerin Covid-19 ile mücadele kapsamı dışında kullanılmayacağı belirtilmektedir.

[17]WHO 2021 bilgilerine göre Covid-19'un en yaygın belirtileri: ateş, kuru öksürük ve yorgunluk hissidir. Daha seyrek görülen belirtiler ise tat veya koku kaybı, burun tıkanıklığı, konjonktivit, boğaz ağrısı, baş ağrısı, kas veya eklem ağrısı, farklı cilt döküntüleri türleri, mide bulantısı/kusma, ishal, üşüme ve baş dönmesi biçiminde sınıflandırılmaktadır.

Kişisel veriler gereğinden uzun süre saklanmamalıdır. Semptom belirlemeye yönelik uygulamalarda toplanan veriler, sağlık yetkilileri tarafından en fazla bir ay veya kişi test edildikten ve sonuç negatif çıktıktan sonra silinmelidir. Sağlık yetkilileri, anonimleştirilmiş bir biçimde olması koşuluyla, verileri sürveyans raporlaması ve araştırma için daha uzun süre saklayabilir. Kişisel cihazdan ulusal sağlık yetkililerine yapılan tüm aktarımlar şifrelenmelidir (Md.3.5).

Her iki uygulamaya da işlenen kişisel verilerin gereğinden uzun süre saklanması konusunda Sağlık Bakanlığı'nın herhangi bir açıklaması bulunmamaktadır. Yanı sıra verilerin depolanması, aktarımı ve kopyalanması gibi konularda da bir açıklama yapılmamıştır. Semptom belirlemeye yönelik olarak kullanılan Korona Önlem uygulamasına işlenen verilerin silinip silinmediği konusunda bir açıklama bulunmamaktadır. Veriler anonim bir şekilde değil, kimlik bilgileri ile birlikte işlenmektedir.

Bununla birlikte HES uygulamasına işlenen T.C. kimlik numarası, baba adı, doğum tarihi bilgilerini kullanıcı uygulamaya kaydetmeden de uygulamanın kısıtlı olarak kullanılabileceği bilgisi verilmektedir.

HES uygulamasında kişinin hastalık durumu riskli ve risksiz diye ayrılmaktadır. Önce pozitif çıkan kişi daha sonra negatife döndüğünde uygulama üzerinde risksiz duruma dönmektedir. Kişinin pozitif bilgisi negatife döndüğünde eski bilginin silinip silinmediğine ilişkin bir bilgi bulunmamaktadır. Uygulamanın aydınlatma metni incelendiğinde uygulamaya işlenen verilerin sürveyans raporlaması ve araştırma için verilerin uzun süre saklanıp saklanmayacağı yönünde bir bilgilendirme saptanmamıştır.

Kişisel cihazlardan ulusal sağlık yetkililerine yapılan tüm aktarımlar için şifreleme bilgisi, her iki uygulamanın aydınlatma metinlerinde açıklanmamaktadır.

Veriler, kullanıcının cihazında saklanmalı ve yalnızca kullanıcılar tarafından iletilen ve amacı yerine getirmek için gerekli olan veriler, bu seçeneğin seçildiği durumlarda sağlık yetkililerinin erişimine açık olan sunucuya yüklenmelidir. Verilerin merkezi bir sunucuda saklanması durumunda, yönetici erişimi de dahil olmak üzere erişim kayıt altına alınmalıdır (Md.3.8).

Söz konusu her iki uygulama aracılığı ile işlenen veriler, kullanıcı cihazında değil, merkezi veri tabanında tutulmakta ve verilerin eşleştirilmesinde merkezi veri sistemi

benimsenmektedir (Çayır, 2020b, 2020d). Merkezi veri sisteminde saklanan veriler için yönetici erişimi gibi yapılacak erişimlerle ilgili olarak her iki uygulamanın da aydınlatma metinlerinde herhangi bir bilgi saptanmamıştır.

Yakınlık verileri yalnızca bireyin cihazında şifreli ve takma adlarla oluşturulmuş biçimde oluşturulmalı ve saklanmalıdır. Üçüncü tarafların takibinin hariç tutulduğundan emin olmak için, diğer konum servislerini etkinleştirmek zorunda kalmadan Bluetooth'un etkinleştirilmesi mümkün olmalıdır (Md.3.8).

HES uygulamasında kullanılan yakınlık verileri, yalnızca bireyin cihazında şifreli ve takma adlarla oluşturulmuş biçimde oluşturulmamıştır. Konum verisi ve Bluetooth servisini işlemek zorunlu tutulmaktadır. Uygulama üzerinde konum servisini etkinleştirdikten sonra Bluetooth servisi etkinleştirilmektedir.

Korona Önlem uygulamasında yakınlık ve konum verileri işlenmemektedir.

İşlenen kişisel verilerin doğruluğu sağlanmalıdır. Temasın daha kesin bir şekilde değerlendirilmesine izin veren teknolojiler kullanılmalıdır (Bluetooth gibi) (Md.3.9).

HES uygulamasına işlenen kişisel verilerin doğruluğu konusunda bir bilgilendirme bulunmamakla birlikte Covid-19 hastalığı riski taşıyan kişilerin durumları devamlı olarak güncellenerek HES koduna tanımlanmaktadır. Uygulamada temasın daha kesin bir şekilde değerlendirilmesi için Bluetooth servisi kullanılmaktadır.

Veri Koruma Yetkilileri, uygulamanın geliştirilmesi sürecinde tam olarak yer almalı ve uygulamayı inceleme altında tutmalıdır (Md.3.10).

HES uygulamasına gelen kullanıcı yorumları incelendiğinde, T.C. Sağlık Bakanlığı kullanıcıların sorunlarını çözebilmek için kullanıcıları yanıtlamış ve kullanıcıların karşılaştıkları sorunların ekran görüntülerini hesdestek@saglik.gov.tr eposta adresine yollamalarını istediği görülmüştür. Bakanlığın uygulamayı sürekli olarak inceleme altında tuttuğu ve kullanıcılara destek olduğu belirtilebilir.

Korona Önlem uygulaması, PlayStore'dan kaldırıldığı için gelen kullanıcı yorumları incelenememiştir.

5. TARTIŞMA

Tez çalışması kapsamında kişisel verileri doğrudan konu edinen ve maddeleri bakımından kişisel verilerle ilgili olan ulusal düzenlemeler ve sağlık hizmetlerinde kullanılan veri kayıt sistemleri incelenmiştir. Kişisel verileri konu edinen ulusal düzenlemelerin sahip olması gereken nitelikler, kişisel verinin önemi, değeri ve korunması için yapılması gerekenler açısından önem taşımaktadır. Veri kayıt sistemlerinin incelenmesi ise, daha çok düzenlemelerin çizdiği sınırların uygulama alanındaki karşılığını ifade etmeleri açısından önem taşımaktadır.

Bu çalışma kapsamında günümüzde Büyük Veri bağlamında kişisel sağlık verilerine yaklaşımı konu alan uluslararası etik kılavuzlardan derlenen ilkeler altı başlıkta gruplandırılmıştır. Bu başlıklar sağlık verisinin toplanmasından önce, toplanırken ve toplandıktan sonra veriye yaklaşım süreçlerini ele almaktadır. Buna göre toplanan sağlık verisinin niçin gerekli olduğu sorusu toplum yararı ilkesi, günümüzde neredeyse sonsuz sayıda toplanan verinin ne kadarının gerekli olduğu minimum veri ilkesi ile tartışılmıştır. Sağlık verisine ilgili düzenlemeler bağlamında yaklaşımın nasıl olması gerektiği hassas veri ilkesi ile değerlendirilmiş, veri toplanırken dikkat edilmesi gereken kurallar eşitlik ve adalet ile özerklik ilkesi kapsamında ele alınmıştır. Son olarak bu ilkelerle uyumlu bir şekilde toplanan sağlık verisinin korunması, mahremiyet ve gizlilik ilkesi başlığında değerlendirilmiştir. Böylece sağlık verisinin toplanması sürecine karşılık gelen bir ilke tanımlanmış ve ilgili yasal düzenleme ve veri kayıt sistemlerinin bu ilkelerle uyumluluk düzeyleri tartışılmıştır.

Son olarak Covid-19 pandemisi gibi olağandışı durumlarda kişisel sağlık verilerinin toplanması süreci ele alınmıştır. Buna göre salgın döneminde kullanılmaya başlayan Hayat Eve Sığar (HES) ve Korona Önlem mobil uygulamalarının özellikleri ve topladığı veriler, Avrupa Konseyi'nin mobil uygulamalarla ilgili yayımladığı "Guidance on Apps supporting the fight against COVID-19 pandemic in relation to data protection" başlıklı kılavuz dayanak alınarak incelenmiştir (European Commission, 2019). Bu kılavuza göre saptanan sorunlar ışığında uygulamaların hangi özelliklerinin güvenli olduğu, aydınlatma metinlerinin bilgilendirme açısından yeterli olup olmadığı, gerçekten toplanması gerekli olan verinin toplanıp toplanmadığı ve bu

verilerin nasıl kullanıldığı gibi sorunlar temelinde, Türkiye'nin salgın döneminde izlediği veri politikaları ile birlikte değerlendirilmiştir.

5.1. Etik İlkelere Göre Düzenleme ve Veri Tabanlarının Tartışılması

5.1.1. Toplum yararı ilkesi açısından

Elektronik sağlık kayıt sistemlerinin kullanılmasıyla birlikte, sağlık hizmetlerinin tüm aşamalarında çok fazla sağlık verisi kayıt altına alınmaya başlamıştır. Hasta tedavisinin yanı sıra bilimsel ve istatistik değerlendirmeler yapılabilmesi ve böylece sağlık hizmetlerinin toplumun gereksinimlerine uygun biçimde sunulabilmesi için sağlık verisine ihtiyaç bulunmaktadır. Bununla birlikte veri paylaşımı ve verinin yeniden kullanımı, mahremiyet ve gizlilik, özerklik, bilgilendirilmiş onam gibi temel etik sorun başlıklarını gündeme getirmektedir. Sağlık verilerinin bir meta olarak görülmesi ve amacı dışında kullanılabilmesi gibi verilerin kötüye kullanımı bir diğer etik sorun kümesidir. Bu ve benzeri etik sorunları karşısında sağlık verisine olan ihtiyacın toplum yararı açısından sorgulanması gerekmektedir. Toplanan verilerin toplum yararı açısından değeri, verinin gerçekten gerekli olup olmadığı ve toplum yararına kullanılıp kullanılmadığı gibi sorular temelinde mevcut durumun etik açısından değerlendirilmesi önemli görünmektedir.

5.1.1.1. Kişisel sağlık verisinin toplanması, toplum yararı açısından gerekçelendirilmeli

Bilgi toplama, depolama, kopyalama, transfer etme ve internet aracılığıyla yayma devletler tarafından toplum yararı temellendirmesiyle yapılırken, şirketler tarafından tüketici tercihleri temellendirmesiyle yapıldığı ifade edilmektedir (İzgi, 2014). Devletler ve şirketler insanları etkilemek, yönetmek, yönlendirmek veya korumak gibi amaçlarla bireyleri izlemek istemektedir. Bu bağlamda özellikle terör ve güvenlik, devletin bireyleri izlemek için ürettiği temel söylemler olarak karşımıza çıkmaktadır. Bu konunun en bilinen örneği 11 Eylül 2001 yılında ABD'de gerçekleşen terör saldırısıdır. Özellikle toplumun güvenlik kaygısı, temel özgürlüklerden vazgeçebilmek için sağlam bir gerekçe oluşturabilmektedir. Bu nedenle devlet söz gelimi bu kaygıyı gidermek için hassas bilgiler de dahil olmak üzere tüm kişisel verileri sürekli ve düzenli olarak kayıt altına almak istemektedir.

Günümüzde sağlık hizmetlerinin bir parçası haline gelen elektronik sağlık kayıt sistemleri, sağlık verisinin işlenmesindeki en önemli araçlardır. Bu araçlar sağlık verisinin oldukça ayrıntılı bir şekilde kaydedilebilmesine olanak tanımaktadır. TTB Kişisel Sağlık Verileri Çalışma Grubu, sağlık verisi ile "kalite ve verimin artması, iş akışının otomize olması, hasta tedavi ve bakımının iyileştirilmesi, acil durumlarda hasta bilgilerine hızlı ulaşım ve uygun çalışma alanlarının belirlenmesi, tetkiklerin tekrarından kaçınma (ekonomik) ve zamandan kazanma, daha iyi dokümantasyon ve gelişmiş denetim yeteneği, dokümanlara çok sayıda kişi ve kolay ulaşım, arşivleme ve belge dolaşımında fiziksel yararlar, yasal bilgi ve belge oluşturmada kolaylık ve sağlık hizmetinin daha iyi planlanabilmesini sağlamak" gibi faydalar elde edileceğini belirtmektedir. Burada belirtilen özellikler, veriye olan ihtiyacı, verinin kullanımına bağlı olarak sağlayabileceği yararları ifade etmektedir.

Türkiye'deki mevcut durum incelendiğinde, özellikle 2012 yılında Sağlık Bakanlığı'nın yayımlamış olduğu "Sağlık Net 2 Veri Gönderimi" başlıklı bir Genelge[18] ile kişisel sağlık verilerine yaklaşım oldukça tartışmalı olmaya başlamıştır. Bakanlık bu Genelge ile sağlık hizmeti veren tüm sağlık kuruluşlarından hasta bilgilerini kendisine göndermelerini istemiştir. KVK Kanunu çıkarıldıktan sonra ise "Sağlık.Net Online ve e-Nabız Hakkında 2016/6 Sayılı Genelge[19]" çıkarılmıştır. Genelgede veri toplama gerekçesi belirtilmiş ve e-Nabız kişisel sağlık sistemi uygulamasının geliştirildiği duyurulmuştur. Buna göre veri toplama gerekçesi olarak "kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi ile sağlık hizmetlerinin planlanması, yönetimi ve finansmanı konularında veri ve işlevselliği artırmak" ifadeleri kullanılmaktadır. E-Nabız sistemi ile ilgili veri toplama gerekçesi şu şekilde belirtilmiştir;

> "…kişiler kendi sağlık durumları ile ilgili doğrudan bilgi sahibi olacak, bu bilgiler ışığında sağlıkları ile ilgili kararlara katılmak suretiyle kendi sağlık durumlarını yönetecek, teşhis ve tedavi süreleri kısaltılarak gereksiz tetkik tekrarları önlenecek, bu suretle sağlıkları ve ekonomik çıkarları korunacak, tüm bunlara ilaveten ülke ekonomisine katkı sağlanacaktır."

[18] 17.11.2012 tarih ve B.10.0.SBS.0.77.00.00/700/3872 sayılı Genelge
[19] 24.04.2016 tarih ve 67189002 sayılı Genelge

Bununla birlikte Sağlık Bakanlığı sağlık hizmetlerinin tüm basamaklarında kullanılan veri tabanları için Ulusal Sağlık Veri Sözlüğünü yayımlamıştır (Sağlık Bakanlığı, 2014b). Bu sözlükte, toplamda 66 tane veri setinin amacı ve kapsamı ayrı ayrı açıklanmıştır. Sözlükte ayrıca hangi veri setinin zorunlu hangi veri setinin koşullu olarak hekim tarafından Sağlık Net 2 sistemine gönderileceği bildirilmektedir. Hekimin göndermekle yükümlü tutulduğu bu sağlık bilgilerinin bildirimi zorunlu hastalıklara ilişkin olmadığını belirtmek gerekir. Birçok verinin gönderimi zorunlu tutulmuş, gönderilecek veriler muayene paketlerine göre tanımlanmış ve sisteme ücretli bir biçimde gönderileceği tarif edilmiştir. "Sözlük" biçiminde isimlendirilen bu belge sıfır noktasında, verinin toplanma gerekçelerini açıklaması nedeniyle oldukça önemlidir. Sağlık verilerinin Sözlükte de belirtildiği üzere ekonomik bir değeri vardır. Bu değer karşısında devletlerin bu verilerden kar ya da kazanç elde etmek gibi bir amacı olmamalıdır.

Mevcut uygulamaya göre Sağlık Bakanlığı'nın sağlık verilerini tek bir merkezde toplamak istemesi, önemli etik sorunları ortaya çıkarmaktadır. Bunlardan en önemlisi hasta mahremiyetinin ihlal edilmesidir. Hasta mahremiyeti ihlal edildiğinde kişiler maddi, manevi ve sosyal yönden zarar görebilir, ayrımcılığa maruz kalabilir ve sağlık hizmetlerine erişimi olumsuz yönde etkilenebilir. Yanı sıra hekimlere olan güven azalabilir, hasta-hekim arasındaki güvene dayalı ilişkinin bozulması ile hastalar sağlık durumları ile ilgili bilgilerini paylaşmak istemeyebilirler. Bu durum bildirimi zorunlu olan hastalıklar açısından yaşandığında toplum sağlığı riske girebilir. Nitekim sağlık verilerinin mahremiyetinin birey ve toplum açısından önemi, AİHM'nin Z. ve Finlandiya kararlarında şu şekilde vurgulanmıştır;"…Sadece hastanın özel hayatına saygı göstermek değil, hastanın tıp mesleğine ve genel olarak sağlık hizmetlerine duyduğu güveni de korumak şarttır. Böyle bir koruma olmazsa, tıbbi yardıma ihtiyacı olanlar doğru tedavi görmek için, hatta tıbbi yardım almak için, gerekli olan kişisel bilgilerini açıklamaktan cayabilir. Bu durumda hem kendi sağlığını hem de bulaşıcı hastalıklar söz konusu olduğunda toplum sağlığını tehlikeye atar." (Güner, 2020).

Bakanlığın sağlık verilerini tek bir merkezde toplaması ile ilgili olarak ortaya çıkan bir diğer sorun verilerin amacı dışında veya kötüye kullanılması riskidir. Örneğin siyasi bir partinin e-Nabız kaydında toplanan bilgilerden kısıtlı seçmen bilgilerine ulaşarak

bu bilgileri parti seçiminde kullanması söz konusu olmuş ve bu durum dava konusu olmuştur (Öztürk, 2019). Aynı davada antidepresan kullanan kişilerin dahi kısıtlı olduğu belirtilerek seçimleri kendi lehine çevirmeye çalıştıkları ortaya çıkmıştır. Bir diğer önemli sorun sağlık verisinin ekonomik değeri nedeniyle bir meta olarak değerlendirilmesi ve alınıp satılabilir hale gelebilmesidir. Bu konuda örneğin SGK tarafından sağlık verilerinin satılması söz konusu olmuş ve bu bilgi kurum tarafından doğrulanmıştır (Erbaş, 2014). Dolayısıyla her bir sağlık verisinin işlenmesi özel yaşamın gizliliğine müdahale, verilere yetkisiz erişim ve kötüye kullanım gibi etik sorunlar barındırmaktadır.

Sağlık hizmetlerinin koruyucu, geliştirici, tedavi edici ve esenlendirici boyutlarıyla bir bütün olarak sunulması gerektiği hakim anlayışı açısından sağlık verisine ihtiyaç bulunmaktadır. Ancak mahremiyet ve özel yaşama müdahale, kötüye kullanım gibi ülkemizde yaşanılan örnekler nedeniyle sınırsız sayıda sağlık verisinin işlenmesi savunulabilir bir yaklaşım değildir. Bu nedenle sağlık verilerinin işlenme sürecinin etik ilkelerle uyumlu hale getirilmesi oldukça önemlidir. Bu bağlamda kişisel sağlık bilgisinin işlenmesi veya tek bir merkezde toplanmak istenmesi olgusunu toplum yararı ilkesi ile uyumluluğu sorgulandığında şu soruların yanıtlarının ilk olarak Sağlık Bakanlığı tarafından verilmesi gerekir: Toplanan sağlık verileri daha sonra yeniden kullanacak mı? Kullanılmayan veri ile ne yapılacak? Toplanan veriler bu amaçlara uygun olarak kullanılıp kullanılmadığı topluma nasıl gösterilecek? Verilerin toplanması sağlık hizmetlerine nasıl yansıyacak? Bu temel sorular hesap verilebilirlik ve şeffaflık açısından yanıtlandıktan sonra Sağlık Bakanlığı veri toplama hazırlığı içine girebilir. Bununla birlikte daha önce de belirtildiği üzere veri sızıntılarından en çok sağlık alanının etkilendiği bilinmektedir (Winally, 2018). Dolayısıyla veri gerekli olsa bile yaratacağı riskler açısından değerlendirmek de gerekmektedir. Buna göre Sağlık Bakanlığı, veri sızıntılarına karşı aldığı/alacağı güvenlik önlemlerini de paylaşmalıdır. Bu tezin yazılma sürecinde Sağlık Bakanlığı "Sağlık Bilgi Yönetim Sistemleri Hakkında Yönetmeliği"ni 25 Ağustos 2022 tarihinde yürürlüğe koymuştur. Yönetmelikte, sağlık bilgi yönetim sistemleri kapsamında kullanılan tanımlara yer verilmiş, birinci basamak sağlık hizmetleri kapsamında kullanılan AHBS ilk kez bu yönetmelikte tanımlanmış ve sağlık bilgi yönetim sistemleri ile ilgili standart kuralların oluşturulması adına taraflara bazı yükümlülükler verilmiştir. Veri tabanları açısından

böyle bir yönetmeliğin yürürlüğe girmesi çok önemlidir. Özellikle verilerin aktarımı, yedeklenmesi, gizlilik ve güvenliği, denetim ve yaptırım gibi konulara ilişkin daha ayrıntılı bilgiler söz konusudur. Buna karşın yönetmelik incelendiğinde kişisel sağlık verilerinin korunabilmesini düzenleyen diğer düzenlemelerin sahip olduğu boşlukları yeterince doldurmadığı, beraberinde yukarıda belirtilen soruların yanıtlarına ilişkin ne bu yönetmelikte ne de Sağlık Bakanlığının ilgili sayfalarında herhangi bir rapor/bilgi bulunmadığı ileri sürülebilmektedir.

Bakanlığın, sağlık hizmetleri sunumunu örgütlemek, denetlemek ve hizmetleri iyileştirmek gibi görevleri bulunmaktadır. Bu görevleri yerine getirebilmek için bu hizmetleri kapsayan verilerin toplanması önemli ve gerekli görünmektedir. Ancak ilgili Bakanlık aynı zamanda toplanan sağlık verilerinin kullanılması ile elde edilen sonuçların hizmetlere nasıl yansıdığını da göstermelidir. Verinin araştırma, planlama ve istatistik gibi amaçlarla işlenmesi, uygulama alanında karşılık bulmalıdır. Bununla birlikte kanun kapsamında milli savunma, güvenlik, kamu düzeni, ekonomik güvenlik gibi muğlak ifadeler, hassas verinin toplanabileceği yönünde sağlam bir gerekçe oluşturamamaktadır. Dolayısıyla ülkemizdeki yaklaşım verilerin ileriye dönük *"gelecekte bir gün kullanılır"* mantığıdır. Bu mantık çerçevesinde veri toplanması, sağlık verilerinin gereksiz yere riske atılması anlamına gelmektedir.

Türkiye'de sağlık verisinin işlenmesi ile ilgili olarak mevcut durumda, verinin işlenmesinin toplum yararı açısından mutlaka gerekli olduğunu belirten sağlam ve ikna edici bir gerekçe ileri sürülmemektedir. Nitekim TTB, Sağlık Bakanlığının çıkarmış olduğu Sağlık Net 2 Veri Gönderimi başlıklı Genelgeye karşı Danıştay'da iptal davası açmış ve Genelge, Danıştay kararı[20] ile iptal edilmiştir. Karar'da Anayasa'nın 20. maddesine atıfta bulunulmuş ve 663 sayılı KHK ile özel hayatın gizliliği ve kişisel verilerin korunması hakkına ilişkin olarak kanun hükmündeki bir kararname ile düzenleme yapılamayacağı belirtilmiştir. Bununla birlikte aynı kararda Anayasa Mahkemesi'nin daha önce almış olduğu 04.12.2014 tarih ve 20137114,2014/184 sayılı kararda belirtilen ölçülülük ilkesine vurgu yapılmıştır. Bu ilke, "özel hayatın ve kişisel

[20] Sağlık Net 2 Davası: 20.04.2016 tarih ve K:2016/2728 sayılı karar, 27.03.2019 tarih ve K:2019/1360 karar ile temyiz istemi reddedilmiştir.

verilerin korunması haklarına yapılabilecek her türlü sınırlama için sınırlama aracının sınırlama amacına uygun ve orantılı olması gerektiği" biçiminde ifade edilmiştir.

Dolayısıyla verinin tek bir merkezde toplanması veya genel olarak verinin işlenmesi uygulamaları için belirtilen gerekçeler toplum yararı ilkesi açısından yeterli değildir. Etik açısından bu ilke ile uyumlu olunabilmesi için Sağlık Bakanlığı, Anayasa Mahkemesi kararında belirtildiği üzere verinin işlenmesi ile işleme amacının nasıl birleştirdiğini göstermeli ve toplumu bu sürece dahil etmelidir. Bu konudaki AİHM kararlarında, Avrupa İnsan Hakları Sözleşmesinin 8. maddesinin asıl amacının "bireyi kamu otoritelerinin keyfi uygulamalarına karşı korumak" olduğu belirtilmekte, haklara meşru müdahalede bulunabilmek için yasallık şartının yeterli olmadığını savunmaktadır. Bu bağlamda düzenlenecek bir yasa kapsamında, toplumun söz konusu yararı için özellikle sağlık verisinin toplanmasının seçeneksiz bir biçimde gerekli olduğunun belirtilmesi gerekir. Literatür incelendiğinde KVK Kanunu başta olmak üzere KSV Yönetmeliği ve ilgili diğer yönetmeliklere ilişkin çeşitli açılardan eleştirel değerlendirmeler yapılmaktadır (Akgül, 2015; Akkurt, 2020; Erdinç, 2020; Güner, 2020; Korkmaz, 2016; Örnek Büken & Zeybek Ünsal, 2017). Bu düzenlemelerin toplum yararı ilkesi ile uyumluluk düzeyleri incelendiğinde, KVK Kanunu'nun 28. maddesinin birinci fıkrasının (b) bendinde, anonimleştirilen kişisel verinin araştırma, planlama ve istatistik gibi amaçlarla işlenebileceği belirtilmektedir. Aynı fıkranın (c) bendinde ise milli savunma, güvenlik, kamu düzeni, ekonomik güvenlik ve özel hayatın gizliliği hakları ihlal edilmemesi suretiyle sanat, tarih, edebiyat veya bilimsel amaçlarla ya da ifade özgürlüğü kapsamında verinin işlenebileceği ifade edilmektedir. Bu ifadeler oldukça genel söylemler olmakla birlikte kanun kapsamındaki bir düzenlemede, sağlık verileri hakkında istisnaya yer verilemeyeceğinin belirtilmesi gerekir. Örneğin sağlık verilerinin işlenebilmesi için toplum yararı açısından sağlık verisinin 'seçeneksiz bir biçimde işlenmesi gerektiği' ne ilişkin bir düzenleme maddesine kanunda yer verilebilir. Böylece tıp etiği açısından hekimin yaşayabileceği toplum yararı karşısında özerklik ve mahremiyet gibi değer çatışmaları karşısında hekim toplum yararını önceleyebilir veya özerkliğe aykırı olarak veri işleme söz konusu olduğunda özerklik değerini koruyabilir. Bununla birlikte merkezi sisteme veri gönderiminin hekimin zorunlu tutulması, hekimin bireysel özerkliğine de aykırılık oluşturmaktadır. Hekimler korunması gereken bir değer olarak bireysel özerkliklerini

korumalıdır. Söz konusu kişisel sağlık verileri olduğunda, veriye yaklaşım daha hassas bir nitelik kazanmaktadır. Bu nedenle ilgili düzenlemelerin açık, anlaşılır, kişilerin temel hak ve özgürlüklerini kullanabilmeleri açısından elverişli, mahremiyet ve gizlilik konusunda güvence sağlayan düzenleme maddeleri içermeleri beklenmektedir. Böylece sağlık verisinin gereksiz ve keyfi kullanımlara dayalı işlenmesi engellenmiş olacak, tıp etiği açısından hekimin yaşayabileceği değer çatışmalarında yol gösterici olacaktır.

5.1.1.2.Biyometrik verinin toplanma amacı kimlik doğrulamak değil; toplum yararı olmalı

Günümüzde biyometrik verilerin toplanması da söz konusudur. Biyometrik veriler genellikle "kamu düzeni", "güvenlik", "ekonomik güvenlik" ve "milli savunma" gibi gerekçelerle işlenmektedir.

Bu amaçlarla Türkiye'de, 10 Ocak 2022 tarihinde Biyometrik Veri Yönetim Sistemi kurulduğu duyurulmuş ve Türkiye'nin dünyada biyometrik veri işleyen yedinci ülke olduğu belirtilmiştir. Bununla birlikte bu proje ile biyometrik verilerin tek bir merkezde toplanacağı, sayısallaştırılacağı, saklanacağı ve diğer kurumların sistemleri ile entegre edileceği bildirilmektedir (Mehmet, 2022). Sistemin ilk aşamasında parmak izi tanıma modülünün tanımlandığı, daha sonra avuç izi tanıma, damar izi tanıma, yüz tanıma, iris ve retina tanıma, ses tanıma ve imza/el yazısı tanıma modüllerinin hayata geçirileceği de belirtilmektedir (Mehmet, 2022). Biyometrik verinin kanun düzeyinde toplanabileceği, Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun 67. maddesinde "…biyometrik yöntemlerle kimlik doğrulamasının yapılması…" biçiminde eklenen ifade ile işaret edilmiştir. Sosyal Güvenlik Kurumu (SGK), "Biyometrik Kimlik Doğrulama Sistemi" adıyla parmak ya da avuç içi izi ile işlem yapılmasını özel hastanelerde zorunlu hale getirmiştir. TTB, SGK'nın bu sistemi zorunlu kılmasını keyfi bir uygulama olarak nitelendirmiş, özel sağlık kuruluşlarında sağlık hizmeti alabilmek için biyometrik yöntemlerle kimlik doğrulaması zorunluluğu getiren tüm düzenlemeler ve buna bağlı işlemlerin, başta Anayasa olmak üzere konuya ilişkin uluslararası sözleşme hükümlerine aykırı olduğunu belirtmiştir (TTB, 2013).

TTB'nin konuyla ilgili açtığı dava Danıştay[21] tarafından reddedilmiştir. Temyiz istemi ve karar düzeltme istemleri de reddedilmiştir. Karar yazısı incelendiğine toplum yararı açısından iki sorun bulunmaktadır. Bunlardan ilki Danıştay Biyometrik veriyi, hassas veri kategorisinde değerlendirmemektedir. Hassas veri türünde olmadığı için sağlık kuruluşlarında kimlik doğrulama yöntemi olarak kullanılabileceği belirtilmiştir. Avrupa Birliği uyarınca biyometrik verilerin doğaları gereği kişisel veri olduğu ve kişilerin hak ve özgürlüklerine özgü belirli riskleri taşıdığı vurgulanmaktadır (Snijder, 2016). Sherman, bir kişinin parmak izi örneğinden o kişinin Down sendromu, Turner sendromu, Klinefelter sendromu gibi kromozomsal bozukluklarının olup olmadığının saptanabildiğini belirtmektedir (Sherman, 2017). Dolayısıyla biyometrik veri hassasiyet düzeyi oldukça yüksek bir kişisel sağlık verisidir ve işlenmesi için toplum yararı açısından niçin gerekli olduğu açıklanmalıdır. Biyometrik verinin ortaya çıkaracağı risklerin öngörülemeyecek düzeyde olması, bu veriye yaklaşımın daha hassas olmasını gerekli kılmaktadır. Daha önce de belirtildiği üzere verinin işlenebilmesi için toplum yararı açısından haklı çıkarılabilecek bir gerekçenin var olması gerekir. Toplumun yararını önceleyen bir gerekçenin varlığı halinde ise özellikle biyometrik veriler için aydınlatılmış onamın alınması ve istisnalara bırakılmaması gerekir. Diğer sağlık verileri, istenen amaçlara ulaşabilmek için halihazırda kullanılabilir. Biyometrik verinin işlenmesi için geçer bir nedenin yanı sıra aydınlatılmış onama dayalı olarak veri işlenebilir olmalıdır. Mevcut uygulama açısından aydınlatılmış onam alınsa bile *"kimlik doğrulamasının yapılması"* gibi bir amaç toplum yararı ilkesi açısından haklı çıkarılamamaktadır. Çünkü biyometrik verinin kimlik doğrulama amacıyla işlenmesi, toplum yararına nitelikli bir fayda üretmemektedir. Biyometrik veri işleme, bazı durumlarda gerekli ve yararlı görünebilir. Örneğin bir başkasının yerine muayenesiz ilaç yazdırmak gibi taleplerle hekime başvurulabilir. Bu durumda biyometrik veri, kesin bir doğrulama sağlayarak hekimin muayenesiz tedavi yapmama yükümlülüğüne yardımcı olabilir. Ancak bu durumda hastanın bu gibi taleplerinin nedenlerini sorgulamak gerekmektedir. Bu konuda sorgulanması gereken ilk konu ise sağlık sistemidir. Sağlık sisteminde hastanın sağlığa erişiminde bazı sorunlar olduğu çıkarımı yapılabilmektedir. Dolayısıyla biyometrik veri işlenmesindeki riskler ve kimlik doğrulamanın alternatif yöntemlerinin

[21] 6.12.2018 tarih ve K:2018/5420 sayılı karar

bulunduğu bilgisi göz önüne alındığında, bu verinin işlenmesinde yeterli bir gerekçenin oluşmadığı ileri sürülebilmektedir. Kimlik doğrulamanın alternatif yöntemleri bulunurken, biyometrik verinin kullanılmak istenmesi, biyometrik verilerin işlenmesinin çeşitli kurumların keyfi kullanımlarına bırakılması anlamına gelebilmektedir. İkinci sorun biyometrik verisini paylaşmayan kişilerin sağlık hizmetlerine erişim haklarının engellenmesidir. Sadece biyometrik veri değil, diğer sağlık verilerinin de paylaşılmaması durumunda bireyin koşula bağlanamayacak olan sağlığa erişim hakkı engellenmemelidir. Nitekim bu konuda TTB, özel hastanelerden sağlık hizmeti alınırken avuç içi ya da parmak izi vermek zorunda olunmadığına dair açıklama yapma ihtiyacı duymuştur (TTB, 2013). Sağlığa erişim engellendiğinde toplum yararı ile örtüşmeyen bir durum ortaya çıkmaktadır. Bununla birlikte onam sorunu da bulunmaktadır. Bireyler sağlık hizmeti alabilmek için onam vermeye zorlanmış olmaktadır. Bu durum ise KVK Kanununda belirtilen onam ile ilgili koşullara aykırı görünmektedir. Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun 67. maddesi başta olmak üzere biyometrik verinin işlenebileceğini belirten kanun ve yönetmeliklerin yeniden ayrıntılı olarak düzenlenmesi ve birbiri ile uyumlu hale getirilmesi gerekli görünmektedir.

Biyometrik verilerin işlenmesi ile ilgili olarak örneğin Türkiye'de çipli kimlik kartı uygulamasına geçilmektedir. Bu yeni kimlik kartlarının seyahat belgesi olarak kullanılabilmesi, elektronik imza özelliğine sahip olması gibi özelliklerin yanı sıra bankacılık, noter, tapu, sağlık ve sigorta işlemleri gibi birçok alanda güvenli doğrulama işlemlerinin yapılabileceğinden söz edilmektedir. Bu yeni kimlik kartının üzerinde ayrıca bireylerin elektronik imzalı fotoğrafı ve elektronik imzalı parmak izleri bilgileri bulunmaktadır. Bu durum göstermektedir ki yeni kimlik kartı uygulaması ile bireylerin biyometrik verisi işlenmekte, bunun için bireylerden herhangi bir aydınlatılmış onam alınmamaktadır. Toplum İçin Mühendislik Komisyonu, bu çipli kimlik kartlarının 10 metre mesafeden çalışabilir durumda olmasından kaynaklı olarak kişilerin devamlı üzerinde taşıdıkları bu kartlarla coğrafi konum olarak izlenmesine ilişkin endişelerini dile getirmişlerdir (Toplum İçin Mühendislik Komisyonu, 2017).

Tıp etiği açısından biyometrik veri işlenmesi, ilgili düzenlemelerde belirtildiği üzere "kamu düzeni", "güvenlik", "ekonomik güvenlik" ve "milli savunma" gibi değerler

karşısında hekimlik mesleği uygulanırken korunması gereken bir değer olan hekimin özerkliği ile özel yaşamın gizliliği ve beraberinde hasta özerkliği değerleri çatışmaktadır. Kamu düzeni, güvenlik, ekonomik güvenlik ve milli savunma gibi değerler karşısında, tıp etiğinin geleneksel olarak koruduğu bu değerler harcanmak istenmektedir. Biyometrik veri işlenmesindeki riskler dikkate alındığında korunması hedeflenen yukarıdaki değerlerin uzun vadede korunamayacağı ileri sürülebilir. Her ne kadar biyometrik kimlik doğrulama, kesin bir doğrulama yöntemi olsa da uzun vadeli düşünüldüğünde temel özgürlüklerden vazgeçilmesi ve sürekli bir gözetim anlamına gelmektedir. Dolayısıyla biyometrik veri işlemek yerine kimlik doğrulamanın alternatif yöntemlerine yönelmek daha makul bir yaklaşım olarak görünmektedir.

5.1.1.3.Kişisel verinin gerçek sahibinin bireyin kendisi olduğu düzenlemelerde açık olmalı

Bir diğer sorun başlığı da insan materyalinin mülkiyetinin kime ait olduğu üzerine yürütülen tartışmalardır (Ballantyne, 2020; Contreras, 2019; Martani, Geneviéve, Elger & Wangmo, 2021; Mikk, Sleeper & Topol, 2017; Montgomery, 2017). Bu çalışmalar verinin mülkiyetinin kime ait olduğu ile ilgili belirsizlikleri ele almakta ve ortak olarak verinin gerçek sahibini veri öznesi olarak belirtmektedir.

Kişisel sağlık verilerini mülkiyet açısından düşünmek, bilgiyi kontrol edenin sömürüsü ve kimin kontrol etme ve bundan fayda sağlama hakkına sahip olduğunu düşündürmektedir (Montgomery, 2017). Bu düşünceye özellikle biyolojik/genetik veriler bağlamında farklı yaklaşımlar bulunmaktadır (Rhodes, 2016). Kişisel verilerin korunmasına ilişkin dünyada farklı yaklaşımlar vardır. Örneğin Avrupa Birliği bir insan hakkı olarak temel hak ve özgürlükler bağlamında hukuka yansıtırken, Amerika Birleşik Devletleri, kişisel verilerin korunmasını bir mülkiyet hakkı olarak değerlendirmektedir. Başka bir deyişle Avrupa'nın yaklaşımı "sosyal değer" merkezli iken, Amerikan yaklaşımı "ekonomik-teknolojik" bir yapıdadır (Küzeci, 2010, s.60). Kişisel veriye mülkiyet hakkı biçiminde yaklaşılması, kişisel veriyi alınıp satılabilen bir meta haline getirirken, aynı zamanda verinin korunmasının da yeterli olmayacağı anlamına gelmektedir. Her ne kadar kişisel verinin ekonomik değeri olsa da, etik açısından bir insan hakkıdır ve bu hak gereği korunmalıdır. Çünkü kişisel verilerin korunması, insan onurunun korunması başta olmak üzere kişiliğin serbestçe

geliştirilmesi ve temel özgürlükler açısından da geniş bir alana sahiptir (Küzeci, 2010, s.67). Bununla birlikte sağlık hakkı, güvenlik hakkı, ifade özgürlüğü, din ve düşünce özgürlüğü ve ayrımcılığa maruz kalmama hakları ile doğrudan ilişkilidir.

Daha önce de belirtildiği üzere kişisel veri, kişiyi belirlenebilir kılan her türlü veri biçiminde tanımlanmaktadır. Kişiyi doğrudan belirlenebilir kılan özellikteki biyometrik veriler de hassas veri niteliğindeki kişisel veriyi oluşturmaktadır. Kişinin biyolojik materyali, biyometrik ve genetik verileri ve diğer sağlıkla ilgili bilgilerinin tamamı kişisel sağlık verilerini oluşturmaktadır. Dolayısıyla kişisel verinin mülkiyeti doğası gereği bireyin kendisine aittir. Kişi çeşitli anlaşma türleri yoluyla fayda sağlamak için kişisel bilgilerinin bir kısmını ilgili kurum veya kuruluşlarla paylaşabilir. Kişinin sağlık hizmeti alabilmek amacıyla bilgilerini paylaşması, mahremiyetinden vazgeçtiği anlamına gelmemektedir (Montgomery, 2017). Belirli bir hizmetin karşılığı olarak kişisel bilgiler paylaşılmaktadır. TTB Kişisel Sağlık Verileri Çalışma Grubu'nun da belirttiği üzere, "kişinin sağlık hizmeti aldığı kurumlar açısından sağlık hizmeti kurum ya da kişi (hekim) olma durumu kişisel sağlık verilerinin üzerinde sahip olma hakkı oluşturmaz. Çünkü sağlık hizmeti gerek kişinin doğrudan kendi ödemesi sonucu gerekse de vergilendirme yöntemi ile sunulmuş olsun her iki durumda da kurumsal haklar kişisel hakların önüne geçemez, aksine kurumlar ya da doğrudan sağlık hizmeti sunan hekimler bu bilgilerin korunması yönünde kişinin hakları açısından birinci derecede sorumludurlar." (TTB Kişisel Sağlık Verileri Çalışma Grubu).

İnsanların kendi bilgilerini kendilerinin sosyal medya gibi dijital ortamlarda paylaşması ise farklı bir konudur. Söz konusu sağlık verileri olmakla birlikte genel olarak insanlar verilerinin paylaşılmasının doğurabileceği risklerin bilincinde olmayabilir veya bu konuya duyarlı olmayabilirler. Örneğin bu konuda 22 ülkede yapılan bir araştırmanın bulgularına göre kişilerin DNA, genetik ve genomik kavramlarının farkında olmadığı veya bu kavramlara aşina olmadıkları saptanmıştır. Yanı sıra araştırma için kişinin DNA ve sağlık verilerini paylaşma istekleri düşük bulunmuş ve bu verilerin birden fazla kullanıcıyla paylaşılması sürecine olan güvenin de yeterli düzeyde olmadığı saptanmıştır (Middleton ve ark., 2020). Dolayısıyla günümüzde özellikle Büyük Veri'nin artık insanın tercihlerini bile etkilediği bir

dünyada, özellikle sağlık verilerinin elektronik ortama aktarılması konusunu etik açısından daha fazla tartışmak gerekmektedir.

Kişisel veriyi işleyen ve veriyi toplum yararına kullanacak olan ise veri sorumlusudur. Bu bağlamda Türkiye'de sağlık verisini işleyen kurum Sağlık Bakanlığı olduğu için veri sorumlusu da bu bakanlıktır. Sağlık Bakanlığı, tek bir merkezde toplamak istediği sağlık verisini genel olarak araştırma, planlama ve istatistik gibi amaçlar için kullanacağını belirtmektedir. Toplum yararı açısından sağlık verisi bu amaçlarla kullanılabilir ve bilgi üretimi açısından bu verilerin kullanılması gereklidir. Ancak sağlık verilerinin kullanılabilmesi için etik açısından bu çalışma kapsamında ileri sürülen ilkelerle uyumlu olması önerilmektedir. Toplum yararı ilkesi bağlamında mutlaka 'gerekli' olan veri toplanırken hak ihlallerine neden olunmamalıdır. Örneğin pandemi gibi olağandışı durumlarda, toplum sağlığının korunabilmesi için gerçekten hassas veriye ihtiyaç olabilmektedir. Dolayısıyla bu durum hassas verinin toplanabilmesi için haklı çıkarılabilir bir gerekçe oluşturmaktadır. Ancak bu gerekçenin açıklanmasının yanı sıra toplum katılımı sağlanmalı, bu bağlamda şeffaflığın korunmasına dikkat edilmeli ve hatta hassasiyet düzeyi yüksek olabilecek veriler için aydınlatılmış onam alınmalıdır. Dolayısıyla toplum içinde bireysel özerkliğin korunabileceği durumlar vardır. Ancak kişisel verinin gerçek sahibinin bireyin kendisi olduğu göz önüne alındığında, bu verinin bireylerin onurları ve kişilik özellikleri ile doğrudan ilgili olduğu görünmektedir. Dolayısıyla bilimin ve toplumun önünde korunması gereken değerler, bireylerin onurları ve kişilik haklarıdır. Kişisel sağlık verilerinin işlenmesindeki haklı çıkarılabilir gerekçe toplum yararı, toplum yararı ilkesi bağlamında kişisel verinin işlenebilir olmasındaki koşul bu değerlerin korunmasıdır. Bu bağlamda toplum sağlığı ve birey özerkliği değerlerinin çatışmaması için sağlık verisinin mülkiyetinin bireyin kendisine ait olduğu ilgili düzenlemelerde açıkça belirtilmelidir. Kişisel verinin mülkiyetinin kime ait olduğu tartışmalarına karşılık olarak verinin gerçek sahibi ne veri sorumlusu ne de sağlık hizmeti sunanların değil, kişinin kendisidir.

5.1.1.4.Toplum yararı ilkesi ile uyumlu bir Kişisel Sağlık Kaydı uygulaması nasıl olmalıdır?

Kişisel sağlık kaydı uygulaması kapsamında kişilerin sağlıklarını kontrol etmelerini sağlamak amaçlanmaktadır. Dünyada sağlık hizmetlerine entegre bir şekilde çeşitli kişisel sağlık kaydı uygulamaları kullanılmaktadır. Örneğin Kanada'da 'Access Health', Avustralya'nın 'My Health Record' ve Türkiye'de tez kapsamında incelenen e-Nabız uygulaması kullanılmaktadır. Dünya Sağlık Örgütü, elektronik sağlık kayıt sistemlerinin benimsenmesinde son 15 yılda istikrarlı bir büyüme ve son beş yılda ise %46 oranında küresel bir artış olduğunu bildirmektedir (WHO, 2019). Bu büyüme karşısında bu tür uygulamaların nasıl olması gerektiği konusu çeşitli açılardan tartışılmakta ve standart bir sağlık kaydı uygulaması bulunmamaktadır. Örneğin bir çalışmada ideal bir sağlık kaydının nasıl olması gerektiği sorgulanmaktadır (Kahn, Aulakh & Bosworth, 2009).

Kişisel sağlık kayıt sistemleri "bir bireyin ulusal olarak tanınan birlikte çalışabilirlik standartlarına uyan ve birey tarafından yönetilirken, paylaşılırken ve kontrol edilirken birden fazla kaynaktan alınabilen sağlıkla ilgili bilgilerin elektronik kaydı" biçiminde tanımlanmaktadır (Kahn ve ark., 2009). Çok çeşitli işlevleri bulunan bu sistemlerin en önemli özelliği, kişisel sağlık bilgilerini kaydetmeleridir. Sağlık hizmetlerinde entegre bir şekilde kullanılması ile birlikte, alınan her bir sağlık hizmetinin sonucunda elde edilen bütün veriler, bu sistemlere aktarılmaktadır. Böylece kullanıcı bütün tanı, tetkik, sigorta bilgileri, alerji bilgileri, radyolojik görüntüleri ve raporları gibi birçok verisine erişim sağlayabilmektedir.

Uygulamaların sahip olduğu işlevler çeşitlendikçe, daha fazla kişisel bilgi işlenmektedir. Bu durumun sağlayabileceği yararlar karşısında mahremiyet ve gizliliğin ihlal edilmesi veya verilerin kötüye kullanımı gibi geriye dönüşü olmayacak zararları da olabilmektedir. Örneğin e-Nabız kaydından kişisel bilgilerin sızdığına yönelik çıkan haberler daha sonra yalanlanmış olsa da her zaman böyle bir ihtimal vardır (Doğan, 2021). Bu nedenle tıp etiği açısından uygun bir kişisel sağlık kaydı uygulamasının nasıl olması gerektiğini tartışmak önemli görünmektedir.

E-Nabız uygulaması incelendiğinde kullanıcının sağlığına katkı sağlayabilecek birçok işlevinin bulunduğu belirtilebilir. Uygulamanın ana ekranında toplum sağlığını ilgilendirebilecek sağlık bilgilerinin kayıtlı olmasının yanı sıra sağlık kurumlarının konum bilgilerini görüntüleme, kardiyovasküler hastalık risklerini hesaplama, ilaç hatırlatması, alerji bilgilerine hızlı erişim, aşı çalışmaları için gönüllü olmayı destekleme, Covid-19 ile ilgili bilgilendirilme ve acil durumlarda ulaşılması istenen kişinin bilgilerinin kaydedilmesi gibi işlevler bulunmaktadır. Uygulamaya yeni eklenen Neyim Var? isimli uzman sistem de oldukça yarar sağlayabilecek bir özellik gibi görünmektedir.

Bir kişisel sağlık kaydı sisteminin amacı her şeyden önce toplum yararının korunması olmalıdır. Bu nedenle uygulama özelliklerinin çeşitlenmesiyle elde edilmek istenen yararlar kadar geriye dönüşü olmayacak riskleri de barındırmaktadır. Örneğin Neyim Var? sistemi, toplumda yaygın olarak kullanılan 'Google doktor' a göre daha güvenilir ve kontrollü olabilir. Böylece bireyler daha sağlıklı karar verebilirler. Öte yandan aynı zamanda kullanıcıyı yanlış yönlendirebilir veya hekimin koyduğu teşhis ile uygulamanın koyduğu teşhis çatışabilir. Bu durum örneğin hekime olan güvenin sarsılmasına neden olabilirken kullanıcı için bir zarara da yol açabilir. Dolayısıyla sisteme eklenen her bir işlevi çok iyi değerlendirmek gerekir. Bu bağlamda uygulamaya eklenmek istenen her bir işlevin hangi sağlık gereksinimlerini karşılaması gerektiği sorgulanmalıdır. Örneğin e-Nabız sistemini mobil uygulaması ile ilgili kullanıcı geri bildirimlerinin önemine vurgu yapan bir yüksek lisans tezinde, uygulamanın hangi özelliğinin daha çok kullanıldığı sorgulanmış ve %70,5 katılımcının uygulamayı randevu almak için kullandıkları saptanmıştır (Karakethüdaoğlu, 2019). Aynı yıl yapılan bir başka araştırma ise katılımcıların çoğu randevu almak için 182'yi arayarak (%49,1) ya da MHRS randevu sistemini (%49,1) kullanarak randevu alırken, e-Nabız sistemini kullananların oranı %8,1 olarak saptanmıştır (Ertaşı, Eroğlu & Çiftçi Kıraç, 2019). Dolayısıyla kullanıcıların e-Nabız kaydını hangi amaçlarla kullandıkları veya kullanmak istediklerinin daha fazla araştırılması gerekir. Bu bağlamda e-Nabız uygulaması hangi amaçla kullanılacaksa, o amaçla orantılı olacak şekilde kişisel bilgilerin kaydedilmesine izin verilmelidir. Kişisel sağlık kaydı uygulaması olarak kullanılacak olan e-Nabız sisteminin, bir sağlık gereksinimini karşılaması ve bu yönüyle sağlık hizmetlerinde tamamlayıcı bir rol

üstlenmesi ideal bir kişisel sağlık kaydı uygulamasının özelliği olarak belirtilebilir. Bu özellik, e-Nabız sisteminin toplum yararı açısından değerini oluşturmaktadır.

Toplum yararı ilkesi ile uyumlu olabilmesi için e-Nabız kaydında hangi kişisel bilgiler bulunmalıdır? Bu soruya yanıt verebilmek için ilk önce bir kişisel sağlık kaydı uygulaması, kullanıcıya ait bütün kişisel bilgileri toplamalı mı sorusunun yanıtlanması gerekli görünmektedir. Yukarıda belirtilen riskler dikkate alındığında, kişisel sağlık kaydı uygulamasının amacı bütün bilgilerin toplandığı bir yer olmamalıdır. Sağlık verisi gibi hassas bilgileri tek bir merkezde toplamak, kullanıcılara sağlayabileceği yararlar karşısında önemli riskleri göze almak anlamına gelir. Daha önce de belirtildiği üzere sağlık verisinin işlenebilmesi için toplum yararı açısından temellendirilebilen bir gerekçe olmalıdır. Bu gerekçenin yanı sıra toplumun bu sürece katılımı sağlanmalıdır. Mevcut durum incelendiğinde, tüm sağlık bilgileri e-Nabız kaydında toplanmaktadır. Uygulamaya iki yönlü bir veri akışı gerçekleşmektedir: kullanıcının kendisinin kaydedebildiği veriler (sensör verileri vs.) ve sağlık hizmeti aldığı kurum ve kuruluşların veri tabanlarından aktarılan sağlık bilgileri. Bu bilgiler daha ayrıntılı olarak incelendiğinde, kullanıcının kimlik bilgileri, adres, iletişim bilgileri, hamilelik testleri, alkol-madde-sigara kullanımı, eğitime devam etme durumu, gelir durumu, ailesinde intihar durumu, cinsel partner bilgileri, kişisel bakım, kişisel hijyen, mahkumiyet/tutukluluk durumu, 15-46 yaş arası kadınların doğum, düşük durumu ve sayıları, babanın kan grubu, doğum ya da düşükle sonuçlanan tüm gebelikler gibi bilgilerin kaydedildiği saptanmıştır. Bu bilgiler, söz konusu bir veri ihlalinde kullanıcıyı belirgin kılacak özel nitelikteki kişisel bilgilerdir. Bu bilgilerin işlenmesi ile mahremiyetin ihlal edilmesi riski doğmaktadır. Bireylerin mahremiyetinin ihlali ile sağlık hizmetlerine erişim sorunu, ayrımcılığa maruz kalma ve şiddete uğrama gibi bireyler açısından istenmeyen sorunlar ortaya çıkabilir. Tıp etiği açısından mahremiyet, korunması gereken bir değer olarak karşımıza çıkmaktadır. Dolayısıyla verilerin işlenmesi ile beklenen yarar karşısında ortaya çıkabilecek zararlar değerlendirildiğinde, zararların beklenen yarardan daha büyük olduğu ileri sürülebilir. Çünkü söz konusu korunması gereken değer mahremiyettir. Bu nedenle işlenecek bilgilerin doğrudan sağlık durumu ile ilgili bilgiler içermesi ve bilgilerin olası bir ifşası durumunda kişilerin mahremiyetine çok büyük zararlar getirmeyecek olan verilerden oluşması tıp etiği açısından daha uygun bir yaklaşım gibi görünmektedir. Örneğin

kişisel sağlık kaydı uygulamalarının uzun vadeli kullanımını araştıran bir çalışmaya göre hastalar kendi kendilerine bakım eylemleriyle ilgili bir durum söz konusu olduğunda uygulamayı kullandıkları saptanmıştır (Gu & Day, 2013). Dolayısıyla yukarıda yer alan oldukça hassas düzeydeki kişisel bilgiler yerine, uygulamaya kullanıcının sağlık bakımı ile ilgili bilgilerin kaydedilebilir olmasına izin verilmelidir. Bununla birlikte örneğin halk sağlığı hedeflerine katkıda bulunacak özellikteki aşı ve alerji bilgileri gibi toplum sağlığı açısından temellendirilebilen bilgiler de bu sistemde tutulabilir.

Literatürde e-Nabız ile ilgili olarak kullanıcı değerlendirmelerini ve farkındalığını araştıran çalışmalar bulunmaktadır (Ertaşı ve ark., 2019; İnal & Ercil Cağıltay, 2019; Karakethüdaoğlu, 2019; Kiraç & Yılmaz, 2019). Bu araştırmaların bulgularından da hareketle uygulamaların kullanım amacının kişiden kişiye değişebildiği görülmektedir. Bu nedenle kişisel sağlık kaydı uygulamaları, 'kişi'nin kullanımında olacak şekilde bir teknik altyapı oluşturulmalıdır. E-Nabız sisteminin amaç ve kapsamı dikkate alındığında "kişilerin de" kullandığı bir sistem konumundadır. Dolayısıyla uygulamanın önceliği birey ve bireylerin kullanım amaçları değil, sağlıkla ilgili bütün verilerin bu uygulama aracılığıyla toplanması amacı taşımaktadır. Toplum yararına kullanılacak verinin bu uygulama aracılığı ile toplanması hedefleniyorsa (ki öyle görünüyor), minimum veri ilkesi ile uyumlu bir tasarıma sahip olmalıdır (Bkz. s.213). Böylece tıp etiği açısından özerklik değeri korunabilir. Bununla birlikte e-Nabız mobil uygulamasını kullanan katılımcıların yorum ve puanlarını araştıran bir çalışmada, tüm yorum ve başlıklarda en sık geçen kelimeler saptanmış ve Buble çizelgesi şeklinde gösteriminin merkezinde "hata veriyor" ifadesi yer almıştır (Karakethüdaoğlu, 2019). Bu durum kişilerin sağlığa erişimleri açısından dikkate değer bir sorundur.

Özetle toplum yararı açısından ideal bir kişisel sağlık kaydı uygulamasının oluşturulabilmesi, kullanıcının hangi sağlık gereksinimi için uygulamayı kullanmak istediğinin daha fazla araştırılması ile belirlenebilir. Böylece toplum katılımlı ve kişilik haklarına saygılı bir kişisel sağlık kayıt sistemi inşa edilmiş olacak, uygulamanın yaygın olarak kullanılabilmesi söz konusu olacak ve beraberinde korunması gereken bir değer olarak özerklik korunabilecektir.

5.1.1.5.Veri tabanları toplum yararı ilkesi ile yeterince uyumlu değildir

Veri kayıt sistemleri ile ilgili tartışılması gereken bir diğer kayıt sistemi sağlık çalışanlarının kullandığı veri tabanlarıdır. Konuyla ilgili literatürün çoğunlukla "mahremiyet, özerklik, risk-fayda, insan ilişkileri ve sorumluluk" konuları üzerinde yoğunlaştığı belirtilmektedir (Jacquemard, Doherty & Fitzsimons, 2021). Etik açısından kabul edilebilir bir elektronik veri tabanı ile ilgili çeşitli görüşler mevcut olsa da standart bir veri kayıt sistemi bulunmamaktadır.

Günümüzde sağlık hizmeti alabilmek için kişisel bilgilerimizi paylaşmamız istenmektedir. Herhangi bir kişisel bilgiyi paylaşmadan, ücreti karşılığında dahi sağlık hizmeti alabilmek neredeyse mümkün değildir. Tez kapsamında incelenen Hızır AHBS ve MİA MED veri tabanları, hem veri kayıt sistemi olarak hem de idari işlerin yürütülmesi sürecinde kullanılmaktadır. Bu iki veri tabanı toplum yararı ilkesi ile uyumlu mu, bu ilke ile uyumlu bir veri tabanı nasıl olmalıdır?

Birinci basamak sağlık hizmetleri kapsamında Hızır AHBS sistemine işlenen kişisel bilgilerden bazıları şunlardır: Ad ve soyad, kimlik numarası, cinsiyeti, resmi doğum tarihi, yaş (ay ve gün olarak), anne ve baba adı, medeni durumu, kan grubu, telefon, adres, ölüm ve doğum tarihi bilgileri, sosyal güvencesi, öğrenim durumu, meslek, iş durumu, sigara-alkol-madde kullanımı, hükümlülük durumu, uyruk, ameliyat geçmişi, gezici hizmet durumu, evde bakım durumu, doğum yeri, özürlülük durumu, yaralanma geçmişi, 15-49 yaş kadınların gebelik durumları ile ilgili bilgiler ve cezaevi tipi. Bu veri tabanı, neredeyse sınırsız sayıda kişisel verinin işlenebileceği bir tasarıma sahiptir. Veri tabanına işlenen bilgiler Sağlık Net 2 merkezi sisteme gönderilmektedir. Verinin tek bir merkezde toplanmasına ilişkin sorunlara daha önce değinilmiş ve mutlaka gerekli olan sağlık bilgilerinin işlenmesi gerektiği vurgulanmıştı. Bu durumun ayrıca hekimin özerkliğine aykırı olduğu belirtilmişti. Birinci basamak sağlık hizmetleri kapsamında kullanılan Hızır AHBS sistemine kaydedilen bu bilgiler, toplum yararı açısından gerekli mi veya bu bilgilerin ne kadarı sağlık hizmetlerinin sunumu için gerçekten gereklidir? Sağlık hizmeti sunmak, hangi verilere bağlanabilir? Bu soruların yanıtı birinci basamak sağlık hizmetlerinin amacı ve kapsamı sorgulanarak verilebilir. Buna göre birinci basamak sağlık hizmetlerinin temel amacı hastalıkları ortaya çıkmadan önlemek ve koruyucu sağlık hizmetlerini ön plana çıkarmaktır. Bu amaç

dikkate alındığında Hızır AHBS sisteminde işlenmesi gereken bilgilerin toplum sağlığını ilgilendiren bilgilerden oluşması gerektiği belirtilebilir. Bu bağlamda örneğin bildirimi zorunlu hastalıklara ilişkin bilgiler, koruyucu sağlık hizmetlerinin ön plana çıkabilmesi için gereklidir. Buna göre bu bilgilerin Hızır AHBS sistemine kaydedilmesi ve Sağlık Bakanlığına gönderilmesi toplum yararı açısından haklı çıkarılabilmektedir. Oldukça hassas düzeydeki ailesinde intihar geçmişi olup olmadığı, intihar bilgisi, kadına yönelik şiddet bilgisi, gebelik ile ilgili bilgiler ve mahkumiyet/tutukluluk durumu gibi çok özel bilgilerin kullanılması da toplum yararı açısından gerekli olabilir. Hastaların yatırılarak teşhis ve tedavilerinin yapıldığı sağlık kuruluşlarında kullanılan veri tabanı örneği olarak incelenen MİA MED veri tabanında da hassas düzeyde veriler işlenmektedir. Örneğin her iki veri tabanına işlenen intihar verilerinin toplanma gerekçesi Ulusal Sağlık Veri Sözlüğünün "intihar girişimi ve kriz tespit veri seti" başlığı altında açıklanmaktadır. Buna göre sözlük incelendiğinde, "ailesinde psikiyatrik vaka bilgisi" nin toplanma gerekçesi "uygulanacak müdahale ve yardımın belirlenmesinde" kullanılacağı belirtilmektedir. İntihara ilişkin bir diğer bilgi "olay zamanı" dır. Olay zamanının niçin gerekli olduğu sorgulandığında "Acil servise başvuran hastanın olay saati ile kabul saati arasında geçen sürenin tespit edilmesi ve buna göre müdahalenin belirlenmesi açısından gereklidir. Zehirlenme vakaları için zehirlenme etkeni ile temas zamanından sonra geçen süreyi hesaplamada kullanılır." biçiminde ifade edilmektedir. Bu bilgi hekimin hastaya müdahale etmesi için gereklidir. Bu tür hassas veriler, Hızır AHBS ve MİA MED gibi veri tabanlarına kimlik bilgileri ile birlikte kaydedilmektedir. Bu verilerin işlenmesi gereklidir ancak kimlik bilgileri ile birlikte işlenmesinin gerekli olmadığı ileri sürülebilir. İstatistiki bilgi üretmek için kimlik bilgilerine ihtiyaç bulunmamaktadır. Dolayısıyla veri tabanlarına işlenen bu tür hassas bilgilerin işlenmesi, toplum yararına haklı çıkarılabilmektedir ancak kimlik bilgilerinin işlenmesi haklı çıkarılamamaktadır.

Özetle toplum yararı ilkesi açısından sürecin en başında, toplanan verilerin niçin işlendiğinin haklı çıkarılabilir bir gerekçesi olmalıdır. Böyle bir gerekçenin varlığı halinde veri tabanları aracılığıyla amaçla orantılı olacak şekilde, insanları kendi verileri hakkında söz sahibi olmaları sağlanarak ve istatistik amaçlı kullanılacak veriler kimlik bilgilerinden arındırılarak işlenmelidir.

5.1.2. Minimum veri ilkesi açısından

5.1.2.1.İlgili düzenlemeler minimum veri ilkesi ile yeterince uyumlu olmalı

Minimum veri ilkesi, toplum yararı açısından gerekli olan verinin toplanması sürecinde bir ölçüt olarak kendini göstermektedir. Kişisel sağlık verisinin korunabilmesi için bu ilke ile uyumlu bir veri toplama politikası izlenmelidir. Çünkü bu ilke veri toplama araçları ve veri toplamanın amaçları arasında bir denge görevi üstlenmektedir. Bunun yanı sıra anonimleştirme veya kimliksizleştirme gibi yöntemlerin yeterli olmadığı günümüz teknolojisinde, mahremiyet ve gizliliği korumak için etkili bir yöntem sunmaktadır.

Konuyla ilgili bir çalışma, kişisel bilgilerin toplanmasının katı bir minimumda tutulması gerektiğini vurgulamakta ve kişisel veri işleyen programların, bilgi teknolojilerinin ve sistemlerin tasarımının bu ilke ile uyumlu olması gerektiğini belirtmektedir (Cavoukian, 2011). Biyometrik verinin işlenme sürecini değerlendiren bir çalışmada aydınlatılmış onamın olması durumunda dahi belirli, açık ve meşru amaçlar için işlenen verinin amaçla bağlantılı, sınırlı ve ölçülü olması gerektiği vurgulanmaktadır (Erdinç, 2020). Tez kapsamında minimum veri kişisel veriler işlendiği amaçla bağlantılı, sınırlı ve ölçülü olma biçiminde tanımlanmakta ve yanı sıra kişisel verilerin işlenmesi gerekliliğinin ve bu kişisel verilerin uygunluğunun değerlendirilmesinin, takip edilen amaç(lar) ışığında yapılması gerektiği vurgulanmaktadır. Bu bağlamda ulusal düzenlemeler incelenmiş ve bu ilke ile uyumlu olmayan düzenleme maddeleri saptanmıştır.

KVK Kanunu minimum veri ilkesine, "b) Doğru ve gerektiğinde güncel olma. ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma. d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme." (Md.4) biçimlerinde yer vermektedir (2016). Kanunda yer verilen bu tanım, Avrupa Veri Koruma Yönetmeliği'nde belirtilen tanım ile aynıdır. Kişisel Veri Koruma Kurumu'nun yayımladığı Kişisel Veri Güvenliği Rehberi'nde minimum veri ilkesine "Verilerin Mümkün Olduğunca Azaltılması" başlığı altında yer verilmektedir. Rehberde minimum veri ilkesi kapsamında verilerin aynı zamanda işlendikleri amaç için gerekli olan süre kadar muhafaza edilmesi gerektiği belirtilmektedir. KVK Kanunu ve

kurumun yayımladığı bu rehber dışında minimum veri ilkesine vurgu yapan bir düzenleme maddesi saptanmamıştır. KVK Kanununda ve KSV Yönetmeliği'nde minimum veri ilkesi için gerekli olan teknik ve ayrıntıları belirleyen bir ifade bulunmamaktadır. Bunun yanı sıra Kanun kapsamında bu ilkeyi yalnızca tanımlamak veya rehbere atıfta bulunmak, kişisel verinin korunması için yeterli de değildir.

Sağlık Bilgi Yönetim Sistemleri Hakkında Yönetmelik'te minimum veriye karşılık gelecek şekilde "Minimum Veri Modeli (VEM)" kavramı tanımlanmıştır (Sağlık Bilgi Yönetim Sistemleri Hakkında Yönetmelik, 2022);

> "Sağlık hizmeti sunucularının yerel veri tabanlarında tutmuş oldukları verilere ait tablo ve alanların ulusal standartlara uyumunu sağlamak, veri kayıplarını asgari düzeyde tutmak, adaptasyonu hızlandırarak vatandaşların geçmiş verilerine erişimini kolaylaştırmak ve sürecin kesintisiz ilerlemesini temin etmek amacı ile Genel Müdürlük tarafından geliştirilen ve SBYS hizmeti alıcılarının SBYS değişiklikleri ile diğer veri aktarımı süreçlerinde kullanılan Minimum Veri Modelini"

Tanım incelendiğinde, bu ilkenin yönetmelik düzeyinde bir yöntem olarak açıklanması oldukça önemlidir. Ancak burada işlenecek verilerin amaçla bağlantılı, sınırlı ve ölçülü olmaları gerektiğine ilişkin bir vurgu yapılmamakta, verinin aktarımının kolaylaşabilmesi açısından bu model tanımlandığı görülmektedir. Bu bağlamda veri işlendikten sonraki süreç açısından bir yöntem tanımlamaktadır. Dolayısıyla tez kapsamında tanımlanan minimum veri ilkesine karşılık gelecek şekilde kanun ve KSV Yönetmeliği kapsamında bir tanım söz konusu ancak gerekli olmayan verilerin işlenmesi durumuna karşılık gelen somut, objektif ve denetlenebilir kurallar içeren bir düzenleme maddesi bulunmadığı vurgulanabilir. Bu durum hekimin hangi veriyi işleyeceği konusunda yaşayabileceği çatışmalara karşı yol gösterici değildir.

KSV Yönetmeliğinde ayrıca e-Nabız hesabı bulunmayan kişilerin verilerine, sağlık personelinin erişimini düzenleyen 6. maddesinin üçüncü fıkrası, bu ilkeye aykırıdır. Buna göre maddede belirtilen ifadeler şu şekildedir (Kişisel Sağlık Verileri Hakkında Yönetmelik, 2019);

> "a) Kişinin kayıtlı olduğu aile hekimi tarafından herhangi bir süre sınırı olmaksızın, b) Kişinin sağlık hizmeti almak üzere randevu aldığı hekim tarafından, randevunun alındığı gün ile sınırlı olmak kaydıyla ve alınan sağlık

> hizmeti ile doğrudan bağlantılı işlemler sonlanana kadar, c) Kişinin sağlık hizmeti almak üzere giriş yaptığı sağlık hizmeti sunucusunda görev yapan hekimler tarafından, yirmi dört saat süre ile sınırlı olmak kaydıyla, ç) Hastanın yatışının yapıldığı sağlık hizmeti sunucusunda görev yapan hekimler tarafından, hasta sağlık hizmeti sunucusundan taburcu olana kadar."

Bu maddenin, hekimin hastanın tüm sağlık verilerine ulaşarak hastaya nitelikli ve bütünlüklü bir sağlık hizmeti sunmayı amaçladığı düşünülebilir. Ancak mahremiyet açısından risklidir. Örneğin yanık nedeniyle sağlık kuruluşuna başvuran bir hastanın antidepresan kullandığı ya da intihar girişiminde bulunduğu bilgisi gibi hastalığı ile doğrudan ilgisi olmayan bilgilere ulaşılabilmesi söz konusu olabilir. Dolayısıyla sağlık personeli de olsa kişilerin sağlık verilerine ölçüsüz bir şekilde erişim riski söz konusudur.

Bunun yanı sıra Ulusal Sağlık Veri Sözlüğünü bu başlık altında da değerlendirmek gerekli görünmektedir. Çünkü bu metin sağlık hizmetlerinin tüm basamaklarında, hangi verinin niçin toplandığını açıklamaktadır. Minimum veriyi tanımlamayan ve 66 tane veri setini toplama gerekçelerini açıklayan bu metnin, bu ilke ile uyumlu olmadığı vurgulanabilir. Daha önce de belirtildiği üzere, metinde her verinin toplanma nedeni "takip ve istatistik çıkarılması" gibi genel bir ifade kullanılarak açıklanmış, metin bu yönüyle toplum yararı ilkesine aykırı bulunmuştu. Bu sözlükten anlaşıldığı üzere minimum veri ilkesi açısından bir ölçü gözetmeyen ve olası tüm risklere karşı, bütün sağlık verisini toplamayı amaç edinen bir politika hedeflendiği görülmektedir. Tıp etiği açısından bu sözlüğün amacı, toplum yararı açısından gerekli olan verinin neden toplandığını ayrıntılı bir şekilde açıklamak, kullanılmayan veriler hakkında bilgi vermek olmalıdır. Bu sözlük kapsamında Sağlık Bakanlığı, gerekli olan verinin amaca uygun olarak kullanılıp kullanılmadığını ve toplanan verilerin sağlık hizmetlerine nasıl yansıyacağını düzenli olarak raporlamalıdır. Yanı sıra verinin işlenmesi aşamasında, toplum yararına gerekli olduğu belirtilen verilerin veri kayıt sistemlerine kimlik bilgilerinden arındırılarak girilmesi yönünde bir politika izlenmelidir.

5.1.2.2.Veri tabanları minimum veri ilkesi ile uyumlu değildir

Veri kayıt sistemlerinin minimum veri ilkesi ile uyumlu olması, henüz zarar oluşmadan ihtiyatlı davranılması açısından oldukça önemlidir. Toplum yararı

açısından gerekli olan verinin ölçülü bir şekilde toplanması, minimum veri ilkesinin benimsenmesi ile mümkündür.

Kişisel sağlık kaydı uygulaması olarak kullanılan e-Nabız uygulamasını bu ilkeye göre değerlendirebilmek için toplanan kişisel bilgiler incelenmelidir. Uygulamada, kimlik bilgileri, adres, iletişim bilgileri, hamilelik testleri, sağlık geçmişi, özürlülük durumu, medeni hal, alkol-madde-sigara kullanımı, iş, meslek, öğrenim durumu, eğitim kurumuna devam etme durumu, gelir durumu, ailesinde intihar geçmişi, cinsel partner bilgileri, kişisel bakım, kişisel hijyen, mahkumiyet durumu, hastalık şikayetleri, hastanın anamnezi, tüm tetkik sonuçları, tetkik istenen kurumlar, 15-46 yaş arası kadınların, doğum, düşük türü ve sayıları, kadın sağlığı işlemleri, kullanılan aile planlaması yöntemi, son adet tarihi, babanın kan durumu, doğum ya da gebelikle sonuçlanan tüm gebelikler, ağız ve diş sağlığı ile ilgili tüm koruyucu hekimlik, teşhis ve tedavi işlemleri gibi birçok bilgi bulunmaktadır. Örneğin hamilelik testleri, ailesinde intihar geçmişi, mahkumiyet durumu, 15-46 yaş arası kadınların, doğum, düşük türü ve sayıları ve babanın kan durumu gibi özel nitelikteki bilgiler, e-Nabız kaydında bulunmalı mıdır? Bu soru toplum yararı ilkesi başlığı altında olası riskler dikkate alınarak tartışılmış ve literatürdeki e-Nabız uygulaması ile ilgili araştırmalardan hareketle uygulamanın hangi sağlık gereksinimi için kullanıldığının daha fazla araştırılması gerektiği vurgulanmıştı. Daha önce de belirtildiği gibi, ideal bir kişisel sağlık kaydı uygulaması bütün kişisel sağlık verilerinin kayıtlı olabileceği bir sistem olmamalıdır. Uygulamanın kullanım amacının toplum yararına göre belirlenmesi, aynı zamanda minimum veri ilkesi ile uyumlu hale getirilmesi demektir. E-Nabız uygulaması, "sağlık kuruluşlarından toplanan sağlık verilerine vatandaşların ve sağlık profesyonellerinin internet ve mobil cihazlar üzerinden erişebilecekleri bir uygulama" biçiminde tanımlanmaktadır. Bununla birlikte "muayene, tetkik ve tedavilerinizin nerede yapıldığına bakılmaksızın, tüm sağlık bilgilerinizi yönetebildiğiniz, tıbbi özgeçmişinize tek bir yerden ulaşabildiğiniz bir kişisel sağlık kaydı sistemi" olduğu belirtilmektedir. Buna göre uygulama ile tüm kişisel sağlık verilerinin tek bir uygulamada toplanması ve böylece kişilerin sağlık verilerine erişimini sağlamak görünen amaçtır. Bu amaç ve kapsam, kişilerin verilerine erişiminin sağlanması ve daha nitelikli ve bütünlüklü bir sağlık hizmeti sunulması açılarından yarar sağlayabilir. Diğer taraftan olası riskleri dikkate almak önemli

görünmektedir. Çünkü mevcut durumda e-Nabız uygulaması hem kullanıcıların erişim sağlayabildiği hem de Sağlık Bakanlığı'nın erişim sağlayabildiği bir teknik altyapıya sahiptir. Bu nedenle mahremiyet, kötüye kullanım ve yetkisiz erişim gibi risklerin önlenebilmesi için kişisel sağlık kaydı uygulamasına aktarılan verinin kullanıcının cihazında kalacak şekilde kaydedilmesi gerekir. Eğer bu sistem aracılığı ile toplum yararına veri toplanması hedefleniyorsa bu verinin minimum veri ilkesi açısından ölçülü bir şekilde ve kişisel bilgilerden arındırılarak toplanması daha makul bir yaklaşımdır. Söz konusu riskler nedeniyle uygulamanın amacı toplum yararına göre belirlenmeli ve bu amaçla orantılı olacak şekilde verilerin kaydedilebildiği bir sistem tasarlanmalıdır.

Sağlık hizmeti sunumunda kullanılan Hızır AHBS ve MİA MED veri tabanlarının toplum yararı açısından değeri, sağlık hizmeti basamağının amacına uygun olarak veriyi tutmasıdır. Bu yönüyle bu veri tabanları sağlık hizmeti sunumunda sağlık çalışanlarına yardımcı olmaktadır. Mevcut durumda veri tabanlarına işlenen her sağlık verisi, Sağlık Bakanlığının merkezi veri sistemine, kimlik bilgileri ile birlikte gönderilmektedir. Bu durumun yaratabileceği riskler açısından gerçekten toplum yararına kullanılabilecek verinin işlenmesi gerektiği daha önce vurgulanmıştı. Buna göre Ulusal Sağlık Veri Sözlüğünde belirtilen veri toplama gerekçeleri sorgulanmıştır. Örneğin Gebelik Sonucu Veri Seti için "gebe olduğu tespit edilmiş olsun ya da olmasın, doğum ya da düşükle sonuçlanan tüm gebelikler ile tespiti yapılıp izlemi yapılmakta iken sahte gebelik olduğu tespit edilen gebelikleri kapsadığı" belirtilmektedir. Bu veri setinin hem gebe hem de bebek sağlığı açısından önemli veriler sunduğu, toplanan verilerin, gebe ve bebek sağlığının takip edilmesinde, verilen hizmetin analizinde ve sağlık hizmetlerinin planlanmasında kullanılması nedeniyle verinin toplandığı açıklanmaktadır. Bu veri setinin toplum yararı açısından değeri sorgulandığında verinin işlenmesi haklı çıkarılabilir görünmektedir. Ancak verinin kapsamı dikkate alındığında, gebelik ile ilgili bilgi alanı oldukça geniş tutulmaktadır.

Bununla birlikte toplum yararına kullanılacak verinin kimlik bilgileri gerektirmemesi nedeniyle, belirtilen veri setinde kimlik bilgilerinin bulunması ve incelenen veri tabanlarında sonsuz sayıda verinin kimlik bilgileri ile işlenebildiği saptamasından

hareketle minimum veri ilkesi ile uyumlu bir yaklaşımdan söz edilemeyeceği vurgulanabilir.

5.1.3. Hassas veri ilkesi açısından

Bazı verilerin kişiyi mağdur etme ve ayrımcılığa yol açma potansiyeli daha yüksektir. Bununla birlikte sağlık verisinin ekonomik değeri, dünyada çeşitli kurum ve kuruluşları, verilerden kar ya da kazanç elde etme amacına yönlendirmektedir. Günümüzde buna devletler de dahil olmaya başlamıştır. Bu durum Büyük Veri kavramı ile bir araya geldiğinde farklı ve kötü amaçlar ortaya çıkabilmektedir. Bu tür sorunların önlenebilmesi için veriyi daha çok korumak ve bu tür verilere karşı daha temkinli olmak gerekir. Bu bağlamda tanımlanan hassas veri ilkesi, toplum yararına işlenen veriye nasıl yaklaşılması gerektiğini belirlemesi açısından oldukça önemlidir.

Hassas veri ilkesine göre verilerin hassasiyet düzeyi, doğrudan nasıl kategorize edildiklerinden çok, bağlamı ile diğer veriler, kişiler, kararlar ve eylemlerle ilişkisine göre değerlendirilmesi gerekmektedir. Buna göre sağlıkla ilgili toplanan tüm bilgiler hassas veri kabul edilmelidir. Bu bağlamda toplum yararı açısından toplanan hassas veriye yaklaşımın nasıl olması gerektiği sorusu, ilgili düzenlemelerde hassas verinin nasıl tanımlandığı, verinin nasıl kategorize edildiği ve hassas veriyi korumak için uygun güvenceler sağlanıp sağlanmadığının incelenmesiyle yanıtlanabilir.

5.1.3.1.Hassas verinin tanımına ilişkin sorunlar

Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme'nin 6. maddesi, "İç hukukta uygun güvenceler sağlanmadıkça, ırk menşeini, politik düşünceleri, dini veya diğer inançları ortaya koyan kişisel nitelikteki verilerle sağlık veya cinsel yaşamla ilgili kişisel nitelikteki veriler ve ceza mahkumiyetleri, otomatik bilgi işlemine tâbi tutulamazlar." biçiminde ifade edilerek hassas nitelikteki verilerin işlenmesini yasaklamaktadır (2016). Anayasa'nın 20. maddesinde kişisel verilerin korunmasına ilişkin esas ve usullerin kanunla düzenleneceği belirtilmektedir. Buna göre yürürlüğe koyulan KVK Kanunu, kişisel verilerin korunmasını güvence altına almayı amaçlaması gerekir.

Bunun yanı sıra bu konuda çıkarılacak düzenlemelerin sağlıklı bir şekilde yürütülebilmesi için ilk olarak tanımlar maddesinin kendi içinde tutarlı olması ve hangi ifadeden ne anlaşılması gerektiğinin net bir şekilde belli olması gerekir. Böylece tanımı esas alan devamı maddelerin doğru uygulanabilmesi sağlanabilir. Tanımlar maddesi ayrıca kanun, yönetmelik ve diğer alt metinlerle de uyumlu ve birbiri ile tutarlı olmalıdır.

KVK Kanunu, tanımlar başlığı altında kişisel veriyi "kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" biçiminde tanımlanmaktadır (2016). Bu tanım gereği ad, soyad, doğum tarihi ve doğum yeri gibi bireyin kimliğini ortaya koyan bilgilerinin yanı sıra telefon numarası, adres, sosyal güvenlik numarası, görüntü, ses kayıtları, parmak izi, DNA, e-posta adresi, IP adresi, sosyal medya hesapları, etkileşimde bulunulan kişi bilgileri, grup üyelikleri, aile bilgileri ve sağlık bilgileri gibi birçok bilgi kişisel veri kapsamındadır. Kanun ayrıca altıncı madde ile "özel nitelikli kişisel veri" yi tanımlamış ve bu tür verilerin işlenme koşullarını belirtmiştir. Bu maddenin birinci fıkrasına göre özel nitelikli kişisel veri, "kişilerin ırkı etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri" biçiminde tanımlanmıştır. Kanunun bu maddesinde kategorik bir yaklaşım olduğu belirtilebilir. Buna göre tanım bu verilerin, her koşulda hassas veri olduğunu kabul etmekte fakat veriyi bağlamına göre değerlendirmemektedir. Bu bağlamda örneğin cinsel hayatla ilgili verilerin bazen hassas olmayabileceği anlamı çıkarılabilmektedir. Hassas veri ilkesi açısından sağlık verileri her koşulda özel nitelikli veri kabul edilmelidir. Bununla birlikte veriyi bağlamına göre de değerlendirmek gerekmektedir. Örneğin hassas veri olmayan ancak bağlamı ile birlikte düşünüldüğünde özel nitelikli veri kategorisi içerisinde yer alabilecek kişisel veriler olabilir. Dolayısıyla kanunun bu maddesinde belirtilen tanımın kapsamı genişletilmelidir.

Avrupa Veri Koruma Yönetmeliği'ni (GDPR) inceleyen bir çalışmada, biyometrik ve genetik verilerin hassasiyet düzeyinin yüksek olduğu belirtilmiş ve hassas veri için belirlenen koruma önlemlerinin hassasiyet düzeyi yüksek olan veriler için yeterli olmayacağını vurgulamıştır (Jasserand, 2017). Buna göre KVK Kanunu

incelendiğinde kanun, biyometrik ve genetik verileri özel nitelikli veri kategorisi içerisinde tanımlamaktadır. Buna karşın bu verilerin hassasiyet düzeyi, KSV Yönetmeliğinde daha ayrıntılı olarak düzenlenmelidir. Nitekim bu konudaki yetersizlik nedeniyle Sağlık Bakanlığı, genetik verilerin yönetimi ve paylaşımına ilişkin Genetik Veri Paylaşımı[22] isimli bir genelge çıkarmıştır. Genelgede klasik ve ileri nesil dizileme yöntemleri kullanılarak gerçekleştirilen yüksek hacimli nükleik asit (DNA/RNA) dizileme işlemlerinin genetik tanı ya da bilimsel araştırma amacıyla yaygın olarak kullanılmaya başlandığı ve bu nedenle bu çalışmalar sonucu elde edilen bilginin depolanması ve paylaşılması ile ilgili bir düzenlemeye ihtiyaç olduğu belirtilmiştir. Hassas veri ilkesi açısından KSV Yönetmeliğinde diğer verilerden farklı olarak hassas veri tanımının ötesinde hassas verilere nasıl davranılması gerektiği de açıklanmalıdır. Örneğin Genelgede, genetik verilerin yurt içinde depolanacağı, uluslararası veri bankalarına eklenmeyeceği ve kontrollü ya da kamusal erişime açılmayacağı bildirilmektedir. Bu bağlamda bu ilke açısından Genelge, genetik veriye nasıl davranılması gerektiğini bildirmesi nedeniyle KSV Yönetmeliğini tamamlayıcı bir nitelikte olduğu ileri sürülebilir.

Bununla birlikte KVK Kanunun 6. maddesine dayandırılarak Sağlık Bakanlığı tarafından genetik verinin işlenebileceği, KSV Yönetmeliği'nin 16. maddesinde belirtilen anonimleştirme koşullarına uyularak, bilimsel araştırmalar kapsamında etik kurul izni alınması koşuluyla aktarım yapılabileceği belirtilmiştir. Genelgede ayrıca genetik verinin özel nitelikli kişisel veri olduğu için bireylerin açık rızası alınmadan işlenmeyeceği, ulusal ve uluslararası paylaşıma kesinlikle açılmayacağı vurgulanmıştır. Bireyin biyolojik kimliğini oluşturan genetik verinin hassasiyet düzeyinin oldukça yüksek olduğu açıktır. Genelgede açıkça belirtildiği üzere bu veri "gizlense dahi bireyin taşıdığı genetik çeşitlilik nedeniyle kişinin kimliğinin anlaşılmasına ve özel hayatın gizliliğinin ihlal edilmesine neden olabilmektedir". Yanı sıra "veri aktarılırken kimliksizleştirme işlemi yapılsa dahi verinin niteliği sadece ilgili kişinin değil aynı zamanda genetik bağı olan aile fertlerinin ve toplum menfaatinin de ciddi şekilde zarar görebileceği bir nitelik arz edebilmektedir." Bu iki temel nedenden dolayı genetik veri, sağlık hizmetleri kapsamında işlenmemelidir.

[22] Sağlık Bakanlığı, 2021/14 tarih ve 95966346 sayılı Genelge

Bununla birlikte aydınlatılmış onam alınmadan verinin kullanılması, araştırmacının Helsinki Bildirgesini ihlal ettiği anlamına gelmektedir. Bu bağlamlarda hassas verinin Sağlık Bakanlığı tarafından kullanılması durumu değerlendirildiğinde, Türkiye'de Sağlık Bakanlığı, tüm hastanelerin ve hastaların verilerini, Bakanlığın veri havuzunda toplamaktadır. Bu verilerin bilimsel araştırmalarda kullanılabilmesi için erişime açılması söz konusu olabilir. Bu durum her ne kadar bilimsel çalışmaların desteklenmesi için değerli bir yaklaşım gibi görünse de, verilerin araştırmacıların erişimine açılması hakkında hastaların bilgilendirilmesi ve aydınlatılmış onamlarının alınması gerekir.

KSV Yönetmeliğinde hassas veri ile ilgili olarak veriye erişim, verinin gizlenmesi, düzeltilmesi, imha edilmesi, aktarılması, anonimleştirilmesi, depolanması ve veri güvenliğinin sağlanması konularına yer verilmektedir. Yönetmelik hassas verinin korunması için yeterli koruma önlemlerini Kişisel Verileri Koruma Kuruluna bırakmaktadır. Buna göre verilerin güvenliğinin sağlanması, verilerin işlenmesi sürecinde yer alan çalışanların görevleri ve verinin aktarımına yönelik önlemler, Kurul kararı ile bildirilmektedir. Bununla birlikte sağlık hizmetlerinde kullanılan sağlık kayıt sistemlerine ilişkin Sağlık Bakanlığı tarafından yürürlüğe koyulan Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arşiv Hizmetleri Yönergesinde Değişiklik Yapılmasına Dair Yönerge (2007) bulunmaktadır. Bu Yönergede, veri güvenliğine ilişkin acil durum/kriz yönetimi, yedekleme, veri tabanı güvenliği, şifreleme, sunucu güvenliği, kimlik doğrulama ve yetkilendirme ile kişisel sağlık kayıtlarının güvenliği konuları düzenlenmektedir. Hassas veri ilkesine uyumluluk açısından bu düzenlemenin oldukça önemli olduğu vurgulanabilir.

Hassasiyet düzeyi yüksek kabul edilmesi gereken biyometrik verilerle ilgili bir haber kaynağında, Almanya'da Chaos Communication Congress'inde damardan ya da avuç içinden yapılabilen kimlik tespitinin, bal mumu ile yapılabileceğinin açıklandığı bildirilmektedir (Türk İnternet, 2019). Bu durum biyometrik veri ile yaşanabilecek yetkisiz erişimlere işaret etmektedir. Bununla birlikte biyometrik verinin işlenmesi başka sorunlara da yol açabilmektedir. Çünkü bu veriler, aynı zamanda gerçek kişinin fizyolojisi veya sağlığı hakkında biyolojik örneğinin analizi sonucunda eşsiz bilgiler de verebilmektedir (Örnek Büken & Zeybek Ünsal, 2017). Bu eşsiz bilgiler, kişilerin

çalıştırılmaması veya sigorta reddine sebep olması gibi ayrımcılık temelli sorunlar ortaya çıkarabilir (Akgül, 2015). Dolayısıyla ilgili mevzuat, bu verinin hassasiyet düzeyinin yüksek olduğunu kabul eden bir yaklaşıma sahip olmalıdır. Bu konudaki belirsizlik nedeniyle örneğin Türkiye'de bir spor salonunun biyometrik veri işlemesi dava konusu olmuştur. Konuyla Kişisel Verileri Koruma Kurulu ilgilenmiş ve çıkardığı karar yazısında, GDPR ve Danıştay'ın ilgili kararlarından hareketle parmak izi ya da yüz tarama gibi yöntemlerin özel hayatın gizliliği ilkesi kapsamında yer aldığını bildirmiştir. Yanı sıra Kurul, toplanan biyometrik verilerin ileride başka bir şekilde kullanılamayacağına dair bir güvence sağlanamayacağını ileri sürülerek uygulamayı hukuka aykırı bulmuştur (KVKK, 2019, 2020).

Etik açısından bir bütün olarak değerlendirildiğinde, bu konudaki en temel düzenleme KSV Yönetmeliğidir. Bu düzenlemenin hassas veri ilkesi ile uyumlu hale getirilmesi için hassas verinin ve özellikle hassasiyet düzeyi yüksek olan verilerin tanımları daha ayrıntılı olarak düzenlenmelidir.

5.1.3.2.Hassas verinin korunmasına ilişkin sorunlar

Kişisel sağlık verileri ile ilgili 20.10.2016 tarihinde 29863 sayılı Resmi Gazete'de yayımlanarak yürürlüğe girmiş olan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'in iptali için Türkiye Psikiyatri Derneği ve Türk Dermatoloji Derneği tarafından dava açılmıştır. Danıştay Onbeşinci Dairesinin 06.07.2017 tarih ve E:2016/10500 sayılı kararıyla 6698 Sayılı Kişisel Verileri Koruma Kanunu uyarınca Kişisel Verileri Koruma Kurulunun görüşü alınmadan, denetim ve kontrolünden geçirilmeden çıkarıldığı için yönetmelik bir bütün olarak hukuka aykırı bulmuş ve tümünün yürütmesi durdurulmuştur. Yönetmelik'in yürütmesi Danıştay tarafından durdurulmuş iken Yönetmeliğin bazı maddelerinde değişiklik yapılmasına dair 24.11.2017 tarih ve 30250 sayılı Resmi Gazete'de yayımlanan Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik yayınlanmıştır. Bu yönetmeliğin de yürütmesi durdurulmuş ve Sağlık Bakanlığı'nın yaptığı itiraz da reddedilmiştir. Daha sonra 21.06.2019 tarih ve 30808 sayılı Resmi Gazetede yayımlanarak yürürlüğe konulan KSV Yönetmeliği'nin bazı hükümlerinin hukuka aykırı olduğu ve iptali gerektiği gerekçesiyle Türkiye Psikiyatri Derneği adına dava

açılmıştır. Ancak açılan bu dava ise reddedilmiştir. Kişisel sağlık verilerini düzenleyen bir yönetmeliğin, kişisel veriyi koruyabilmesi için önlemlerin belirli, açık ve anlaşılır kurallardan oluşması gerekir. Bu bağlamda KSV Yönetmeliğini, hassas veri ilkesi açısından değerlendirmek gerekir. Bu yönetmeliğin toplum yararına toplanacak olan veri hakkında ilgili bakanlığın toplanan verileri daha sonra kullanıp kullanmayacağı, kullanılmayan verinin akıbetinin ne olacağı, amaca uygun olarak kullanılmasının topluma nasıl gösterileceği ve sağlık hizmetlerine nasıl yansıyacağı gibi sorular, yanıtsız kaldığı için toplum yararı ilkesi ile uyumlu olmadığı ifade edilmişti (Bkz. s.195). Eğer yönetmelik toplum yararı ilesi ile uyumlu olsaydı, hassas veri ilkesi açısından toplum yararına gerekli olan verinin güvenliğinin sağlanabilmesi için uygulamayı gösterir şekilde somut, objektif ve denetlenebilir kuralları içerip içermediğinin sorgulanması gerekirdi. Yine de bu bağlamda incelenen başta KVK Kanunu'nun (2016) hassas verinin işlenmesini düzenleyen maddesi, verinin "sağlık hizmetlerinin sunulması", "planlaması" ve "yönetimi" amaçlarıyla açık rıza aranmaksızın "sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar" tarafından işlenebileceğini belirtmektedir.

> "Madde 6, (3) Birinci fıkrada sayılan 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."

Hassas verinin işlenmesi için belirtilen tarafların "yetkili kurum ve kuruluşlar" ın belirsiz olduğu görülmektedir. Bununla birlikte veri işleme gerekçesi olarak öne sürülen genel anlamıyla kamu sağlığının korunmasıdır. Bu ifadenin de tanımı daha açık olmalıdır. Çünkü bu tanımdan örneğin "kamu sağlığı" nın korunması gerekçesi öne sürülerek her türlü verinin işlenebileceği anlamı çıkabilmektedir. Dolayısıyla kişisel veriyi koruyan bir kanunda, özellikle hassas veri konusunda belirsiz, esnek, açık uçlu düzenleme maddelerine yer verilmemelidir. Bununla birlikte kanun kapsamında işlenen hassas verinin kullanımı konusunda sınırlı yetkiler verilmeli, toplum yararına "gerekli" olan verinin toplanması ve veri sahiplerinin hangi bilgilerinin toplanacağı

hakkında bilgilendirilmesi ve sürece katılımlarının sağlanması yaklaşımları benimsenmelidir.

Bu bağlamda temel bir düzenleme olan KSV Yönetmeliğinin de benzer sorunları bulunmaktadır (Kişisel Sağlık Verileri Hakkında Yönetmelik, 2019);

> "Madde 6 … (4) Üçüncü fıkrada yer alan erişim kuralları, Bakanlığın sağlık hizmeti sunumu ihtiyaçlarına göre ve Kanunun 6 ncı maddesinin üçüncü fıkrası kapsamında Genel Müdürlük tarafından yeniden değerlendirilebilir. Böyle bir durumda aydınlatma yükümlülüğü kapsamında gereklilikler sağlanır."
>
> "Madde 6 … (6) Mahremiyet düzeyi daha yüksek olan, başkaları tarafından görülmesi ve bilinmesi halinde kişilerin sosyal hayatını ve ruh sağlığını olumsuz etkileme riski taşıyan kişisel sağlık verileri Bakanlıkça belirlenir ve sağlık personelinin bu verilere erişimine ölçülü kısıtlar getirilebilir."
>
> "Madde 12 (1) … Gizlilik kararlarının sadece görevi gereği bilmesi gereken kişiler tarafından bilinmesini sağlamak üzere gerekli her türlü teknik ve idari tedbirler alınır."
>
> "Madde 17 (1)… bu konuya özel olarak tahsis edilen bir internet sitesi üzerinden herkesin erişimine açılmasına ilişkin usûl ve esaslar Bakanlıkça belirlenir."
>
> "Madde 18 (1) Veri güvenliğine ilişkin yükümlülükler MADDE 18 – (1) Kanunun 12 nci maddesinde yer alan veri güvenliğine ilişkin yükümlülüklere riayet edilir. Teknik ve idari tedbirlerin alınmasında, Kurum tarafından hazırlanan Kişisel Veri Güvenliği Rehberi esas alınır. (2) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde veri sorumlusu tarafından Kurula yapılacak bildirimde Kanun hükümleri ile Kurulun bu hususa ilişkin düzenleyici işlemleri esas alınır."
>
> "Madde 19 (1) Bakanlık merkez birimleri ve taşra teşkilatı ile bağlı ve ilgili kuruluşlarda yürütülen bilgi güvenliği süreçleri, Genel Müdürlük tarafından hazırlanan Bilgi Güvenliği Politikaları Yönergesi ile belirlenir."
>
> "Madde 20 (1) Özel nitelikli kişisel verilerin işlenmesinde ayrıca, Kanunun 6 ncı maddesinin dördüncü fıkrası ile 22 nci maddesinin birinci fıkrasının (ç) bendi uyarınca Kişisel Verileri Koruma Kurulu tarafından yapılan ikincil düzenlemelerde yer alan yeterli önlemlere riayet edilir."

Yönetmeliğin bu maddelerinin ise hassas verinin güvenliğinin sağlanmasına yönelik uygulamayı gösterir nitelikte olmadığı belirtilebilir. Maddeler incelendiğinde işlenen hassas verinin korunması için yöntemler, yeterli ve somut önlemler ikincil düzenlemelere bırakılmış ve yanı sıra açık uçlu ve belirsiz ifadelere bu maddelerde de

yer verilmiştir. Hassas veriye ilişkin sağlık çalışanlarının uyması gereken kurallar ve tedbirlerin ise ikincil düzenlemelere bırakıldığı görülmektedir. Temel bir düzenleme olması nedeniyle yönetmelik kapsamında, hassas verinin nasıl işleneceği, korunabilmesi için hangi somut önlemlerin alınacağı ve sağlık çalışanlarının uyması gereken kuralların neler olduğu, yeterli ve belirli bir şekilde bu yönetmelikte yer almalıdır.

KSV Yönetmeliği'nde hassas verileri toplayan veri kayıt sistemlerine ilişkin olarak yalnızca yönetmeliğin 4. ve 6. maddeleri, e-Nabız uygulamasıyla ilgilidir. E-Nabız uygulamasının yanı sıra sağlık hizmetlerinin tüm basamaklarında kullanılan veri tabanları ve çok çeşitli mobil sağlık uygulamaları bulunmaktadır. KSV Yönetmeliği kapsamında sağlık hizmeti basamaklarında kullanılan veri tabanları ve mobil uygulamalara yönelik kurallara da yer verilmelidir. Kişisel sağlık bilgilerinin bu uygulamalarda işlenmesi, depolanması ve paylaşılmasına ilişkin standart kuralların oluşturulması, idari ve teknik tedbirlerin belirli olması ve aydınlatılmış onam alınması gibi konuların ikincil düzenlenmelere bırakılmaması, hassas veriye yaklaşım açısından önemli görünmektedir.

Anonimleştirme kavramı belirsizdir

İlgili düzenlemelerdeki bir diğer belirsizlik, hassas verinin nasıl anonim hale getirileceğine ilişkin yöntemlerle ilgilidir. Bu konuda Kişisel Verileri Koruma Kurumu tarafından yürürlüğe koyulan Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik bulunmaktadır. Anonim hale getirme, KSV Yönetmeliğinin 4. maddesinde "c) Kişisel verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi" biçiminde tanımlanmaktadır (2019). Yönetmeliğin aynı maddesinin k fıkrasında verilerin imha edilmesi kavramı "kişisel verilerin silinmesi, yok edilmesi veya anonim hale getirilmesini" şeklinde açıklanmaktadır. İki tanım incelendiğinde anonim hale getirme yönetmeliğin c fıkrasında daha açık, anlaşılır ve net bir şekilde açıklanırken, verinin imha edilmesi "…veya anonim hale getirilmesini" biçiminde tanımlanmaktadır. Buna göre kavramın içerikle uyumlu olmayacak şekilde tanımlandığını görmek mümkündür. İçeriğe dair bu uyumsuzluk, Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in

(2017) tanımlar başlıklı 4. Maddesinde imha (c fıkrası), kişisel veri saklama ve imha politikası (f fıkrası) ve periyodik imha işlemi (ğ fıkrası) "… veya anonim hale getirilmesi" biçimindeki tanımda da görülmektedir. Her iki yönetmelik de verinin imha edilmesi ile anonim hale getirilmesini bir tutmaktadır. Verinin imha edilmesi, silinmesi ve yok edilmesi içeriğine sahipken anonim hale getirme işlemi, veriyi silmez, yok etmez, veriyi kişisel bilgiden arındırma ve dönüştürme anlamları taşımaktadır. Anonimleştirmenin maskeleme, toplulaştırma, veri türetme ve veri karması gibi yöntemleri bulunmaktadır. Yönetmelik kapsamında hangi anonimleştirme yönteminin kullanılması gerektiği belirsizdir.

Türkiye'de yapılan bir doktora çalışması kapsamında özellikle Büyük Veri konusunda yeni bir anonimleştirme yöntemi olan Su-Mondrian modeli geliştirilmiştir (Yavuz, 2019). Bu model, fayda temelli ve veri güvenliği açısından test edilmiş yeni bir anonimleştirme modeli olarak ifade edilmektedir. Mahremiyet açısından riskli olabilecek verilerin gizliliğinin korunabilmesi için bu yöntemin oldukça önemli olduğu vurgulanmaktadır. Bu ve benzeri anonimleştirme modellerinin sağlık verileri açısından standardizasyon taşıması gerekir. Böylece anonimleştirme modeli bağımsız uzmanlar tarafından sürekli olarak denetlenmesi de mümkün hale gelecektir. Bu bağlamda anonim hale getirmenin yöntemi, ilgili düzenlemelerde belirtilmeli ve nasıl yapılacağı açıklanmalıdır.

Anonim hale getirme, Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik'te (2017) kapsamlı bir şekilde 10. madde ile tanımlanmıştır;

> "(1) Kişisel verilerin anonim hale getirilmesi, kişisel verilerin başka verilerle eşleştirilse dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesidir. (2) Kişisel verilerin anonim hale getirilmiş olması için; kişisel verilerin, veri sorumlusu, alıcı veya alıcı grupları tarafından geri döndürme ve verilerin başka verilerle eşleştirilmesi gibi kayıt ortamı ve ilgili faaliyet alanı açısından uygun tekniklerin kullanılması yoluyla dahi kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemez hale getirilmesi gerekir. (3) Veri sorumlusu, kişisel verilerin anonim hale getirilmesiyle ilgili gerekli her türlü teknik ve idari tedbirleri almakla yükümlüdür."

Yönetmeliğin bu maddesi incelendiğinde anonimleştirmenin nasıl yapılacağına ilişkin yöntemin ne olduğu açıklanmamıştır. Kullanılacak uygun yöntem "Madde 5. … Veri sorumlusu, Kurul tarafından aksine bir karar alınmadıkça, kişisel verileri resen silme, yok etme veya anonim hale getirme yöntemlerinden uygun olanını seçer. …" ifadeleri ile veri sorumlusuna bırakılmıştır. Veri sorumlusu "her türlü teknik ve idari tedbirleri almakla yükümlü" tutulmuştur. Anonim hale getirmeyi düzenleyen bir yönetmelikte, uygun yöntem veya yöntemlerin hangilerinin olduğu belirsiz olmamalıdır. Özellikle hassas verinin anonim hale getirilmesi konusunda uygun yöntemin belirli olması, verinin korunabilmesi için çok önemli bir yere sahiptir.

Buna karşın Sağlık Bilgi Yönetim Sistemleri Hakkında Yönetmelik'in (2022) gizlilikle ilgili 16. maddesinin beşinci fıkrasında, verilerin kim tarafından anonim hale getirilebileceği açıklanmaktadır. Buna göre yönetmeliğin ilgili maddesi şu şekildedir;

> "(5) Kişisel veriler, ancak SBYS[23] hizmeti alıcısı tarafından anonim hale getirilebilir. SBYS hizmeti alıcısı[24] veya Bakanlığın izni olmaksızın kişisel veriler, SBYS hizmeti sağlayıcısı tarafından anonim hale getirilemez. Kişisel verilerin, SBYS hizmeti sağlayıcısı[25] tarafından anonim hale getirilerek farklı amaçlarla işlendiğinin tespiti halinde başta 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ve 26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanunu olmak üzere ilgili mevzuat hükümleri çerçevesinde işlem tesis edilir."

Yönetmeliğin amacı ve kapsamı dikkate alındığında bu madde, anonim hale getirmenin uygun yöntemine işaret etmelidir. İdari açıdan bir tedbir olarak anonim hale getirmenin SBYS hizmeti alıcısı tarafından yapılabileceği belirtilmekte, buna karşın anonimleştirmenin nasıl yapılacağı konusu belirsizliğini korumaktadır.

5.1.3.3.Hassas ve hassasiyet düzeyi yüksek olan veriye yaklaşım nasıl olmalı?

Bilgi veya bilişim çağındaki gelişmeler sonucunda çok sayıda veri çok dar bir alanı kaplayacak şekilde işlenebilmektedir. Bunun yanı sıra birbirinden ilişkisiz şekilde

[23]Bu kavram yönetmelikte "Sağlık hizmeti sunucuları tarafından klinik, idari ya da yönetimsel amaçlarla kullanılan, gerektiğinde diğer bilgi yönetim sistemleri ile veri alışverişi yapabilen ve Sağlık Bilgi Yönetim Sistemleri olarak adlandırılan yazılımlar" biçiminde açıklanmaktadır.
[24]Yönetmelikte "SBYS hizmeti alıcısı: SBYS hizmetini alan idareleri ve sağlık hizmeti sunucuları" biçiminde tanımlanmaktadır.
[25]Yönetmelikte "SBYS hizmet sağlayıcısı: SBYS hizmeti sunmak üzere Kayıt Tescil Sisteminde kayıt edilerek yetkilendirilmiş olan gerçek veya tüzel kişiyi" biçiminde tanımlanmaktadır.

tutulan verinin merkezi olarak bir araya getirilebilmekte, veriler, veri eşleştirme ve veri madenciliği gibi ileri teknolojik imkanlarla analiz edilebilmektedir. Veriler artık çok kolay bir şekilde dünyanın herhangi bir yerine aktarılabilmektedir. Veriye dayalı bütün bu özellikler, verinin ülke ekonomilerinde temel belirleyici rol üstlenmesine sebep olurken, bu durumun yaratacağı riskler de önemli boyutlara taşınmaktadır.

Bütün bu süreçte kişisel verinin ve daha özel olarak hassas verinin korunması bir zorunluluk olarak kendini göstermektedir. Hastalıkların tanı ve tedavisi ve bu bağlamda sağlık hizmetlerinin gelişimi için gereksinim duyulan sağlık bilgisine bugün birçok farklı amaç gereği ihtiyaç duyulmaktadır. Özellikle sağlık bilgisinin ekonomik değeri ile tanışıldıktan sonra birçok sektör sağlık verisini elde etmek istemektedir. Ülkemizde sağlık hizmetlerinin özelleştirilmesi ile verilerimiz, Sağlık Bakanlığı, SGK ve özel sağlık sigorta şirketleri tarafından toplanmakta ve bu veriler ticari bir meta olarak değerlendirilebilmektedir. Kişisel sağlık verilerinin SGK tarafından satıldığı ve daha sonra bu bilginin kurum tarafından doğrulandığı bilinmektedir (Birgün, 2014; Erbaş, 2014). Dolayısıyla verinin nasıl elde edilmesi gerektiğinden veriye nasıl yaklaşılması gerektiğine ilişkin sınırların iyi çizilmesi gerekir.

Hassas ve hassasiyet düzeyi yüksek olan verinin işlenmesi ve korunması sürecindeki belirsizlikler, kişilerin sağlık hakkını ihlal edebileceği gibi verilerin gizliliğinin sağlanmasına güven duyulmaması nedeniyle sağlık hizmeti almaktan tereddüt duyulmasına sebep olabilir. Verilerin kötüye kullanılabilme olasılığı ise her zaman olacaktır. Genomik veri paylaşımına yönelik tutumları araştıran bir çalışmanın bulgularına göre, verilerin birden fazla kullanıcıyla (örneğin hekimler, araştırmacılar, hükümetler) paylaşılma sürecine olan güvenin düşük olduğu saptanmıştır. Aynı araştırma bulgularına göre kar amaçlı yapılacak olan bir araştırma için insanlar verilerini paylaşma konusunda daha az istekli oldukları bulunmuştur (Middleton ve ark., 2020). Dolayısıyla insanlar verilerini hangi amaçlarla kullanılacağını bilmek isterler. Verinin gizleneceğine duyulan güven eksikliği ise kişilerin hastalıklarını toplum sağlığı açısından önemli olduğu durumlarda da gizlemesine neden olabilir. Bu durumda toplum sağlığı tehlikeye girmektedir.

Öte yandan tıbbi araştırmalarda hassas verinin kullanılmasının ciddi zararlara yol açacağına dair çok az kanıt olduğu aktarılmaktadır (Davies & Collins, 2006). Bu

durum iki şekilde değerlendirilebilir: Birincisi yapılacak tıbbi araştırmalar için önceden etik kurul izni alınması zorunluluğu bulunmaktadır. Etik kurullar, yapılacak biyomedikal araştırmaların etik ilkelere uygun olup olmadığını inceleyerek çalışmanın yapılıp yapılmaması gerektiğine ilişkin karar vermektedir. Buna göre hassas verinin söz konusu araştırma için gerekli olup olmadığı, yönteminin uygun olup olmadığı, hasta veya deneklerden aydınlatılmış onam alınıp alınmayacağı ve amaç ile yöntemin uygun olup olmadığı gibi etik açısından uygunluğunu incelemektedirler. Dolayısıyla hassas verinin söz konusu kullanılmasında bir sorun bulunmamaktadır. İkinci olarak tıbbi araştırmalarda hassas veri kullanılmasının ciddi zararlara yol açmayacağı tam olarak öngörülemez. Örneğin genetik veri, bireylerin genetik yatkınlıklarını bildirir ve bu bilgi, gelişen tıp teknolojisi aracılığıyla önceden çok daha kolay bir şekilde saptanabilir. Bu bilginin gelecek kuşaklara kadar uzanabileceği ve bazı durumlarda tüm toplumları etkileme olasılığından söz edilmekte ve biyolojik örneklerin toplandığı zaman diliminde önemi henüz anlaşılamayan nitelikte olabileceği belirtilmektedir (TTB, 2020). Diğer bir deyişle genetik veriler, geleceğe ait bilgileri de içerebilmektedir. Dolayısıyla genetik verilerin bu değerleri nedenleriyle, kötü amaçlar için kullanımı, mahremiyetin ihlali ve beraberinde insan hak ve özgürlüklerinin yitirilebilmesi ve ayrımcılık gibi potansiyel riskler söz konusudur.

Biyolojik ve tıbbi alanlardaki ilerlemelerin kötüye kullanılmasına karşı insan yararını bilimin veya toplumun yararının önünde tutan ilk uluslararası metin İnsan Hakları ve Biyotıp Sözleşmesi, konuyla ilgili önemli sınırlamalar getirmektedir. Yasal bağlayıcılığı bulunan bu sözleşme, insan onurunu, haklarını ve özgürlüklerini korumaya yönelik ilke ve kuralları tanımlamıştır. Bu bağlamda sözleşmenin dördüncü bölümü, genetik çalışmalarla ilgili nelerin yapılıp yapılmayacağı konusunda sınırları çizmiştir. Dördüncü bölümünün ilk maddesi genetik kalıtım nedeniyle herhangi bir kimseye ayrımcılık yapılamayacağını belirtmektedir. Sözleşmenin 12. maddesi "Genetik hastalıkları teşhise yönelik veya ya kişinin bir hastalığa neden olan bir geni taşıdığını belirlemeye ya da genetik bir yatkınlığı veya bir hastalığa eğilimi ortaya çıkarmaya yönelik testler, sadece sağlık amaçlarıyla veya sağlık amaçlı bilimsel araştırma için ve uygun genetik danışmada bulunmak şartıyla yapılabilir." ifadeleri ile genetik testlerin kullanımını sınırlandırmıştır (2003). Bu madde ile genetik hastalıkları veya yatkınlığı testlerinin sadece sağlık amaçlı bilimsel araştırma için ve uygun genetik

danışmada bulunmak şartıyla yapılacağını vurgulanmaktadır. Uluslararası sözleşmenin bu maddesi hassasiyet düzeyi oldukça yüksek olan genetik veriye yaklaşımı önemli ölçüde sınırlandırmaktadır. Günümüzde genetik alanındaki araştırmalar, çeşitlenerek ilerlerken bu çalışmalardan nitelikli bilgiler üretilmesi kadar genetik verilerin işlenmesi, depolanması, saklanması ve paylaşılması gibi konuların sınırlarının belirli olması etik açısından gereklidir. Bu verilerin hassasiyet düzeyi oldukça yüksek olduğu için ortaya çıkarabileceği zararların telafisi mümkün olmayabilir. Bu nedenle bu veriler, mevzuat kapsamında güvence altına alınmalıdır. Buna göre incelenen KVK Kanunu ve uygulama alanında KSV Yönetmeliğinin bu konuda yeterli olmadığı belirtilebilir. Bu yetersizlik nedeniyle örneğin Sağlık Bakanlığı, Genetik Veri Paylaşımı başlıklı genelgeyi çıkarma gereği duymuştur.

Söz konusu bu etkenler dikkate alındığında, hassas veri kullanmanın potansiyel riskleri ve faydalarını dengelemek gerekir (Davies & Collins, 2006). Bir bütün olarak bakıldığında hassas veri ilkesi açısından sağlıkla ilgili bütün veriler hassas veri kabul edilmelidir. Bu kabul, kişisel sağlık verisini korumayı amaç edinen düzenleme metinlerinde kendini göstermelidir. Bununla birlikte biyometrik ve genetik veriler gibi bazı verilerin hassasiyet düzeylerinin yüksek olduğu kabul edilmeli ve işlenen bu tür verilerin kullanımı konusunda sınırlı yetkiler veren düzenleme maddeleri oluşturulmalıdır. Bu bağlamda bu düzenlemelerin hassas verinin korunması yönünde yol gösterici olmadığı ileri sürülebilir. Bu bakımdan tıp etiği açısından veri işleyen hekimlere, hassas verinin korunması için önemli bir sorumluluk düşmektedir. Buna göre hekimler tüm kişisel sağlık verilerine hassas veri niteliğinde kabul etmeli ve buna göre bir yaklaşım sergilemelidir. Hassas verinin tam bir koruma sağlanmasının tek gerçek yolu, o verinin işlenmemesidir. Bu bakımdan hekimler, hassas veriyi ve özellikle hassasiyet düzeyi yüksek olan veriyi korumak adına, toplum yararına gerekli olmayan ve ilgili düzenlemelerin yeterince yol gösterici olmadığı bu gibi durumlarda, veriyi işlememelidir.

5.1.4. Eşitlik ve adalet ilkesi açısından

Eşitlik ve adalet ilkesi toplum yararına işlenecek verinin, eşit ve adil bir şekilde toplanmasını, sağlık hakkı kapsamında veri kayıt sistemlerine herkesin erişebilmesini ve kullanılmakta olan veri kayıt sistemleriyle ilgili sosyoekonomik, coğrafi ve etnik

ayrımcılık yapılmamasını ifade etmektedir. Bunun yanı sıra eşitlik ve adalet ilkesi açısından kişisel sağlık kayıt sistemi başta olmak üzere sağlık hizmetlerinde kullanılan veri tabanları, damgalanmaya yol açmamalı, bilgi ve iletişim teknolojilerine erişim, kültür, dil, gelir düzeyi ve yaş gibi değişkenler açısından da sağlanmalı ve dezavantajlı grupların menfaatleri ve hakları korunmalıdır.

Bugün sınırsız sayıda sağlık verisi elde edilmekte ve bu veriler Büyük Veri analizi yöntemleri kullanılarak analiz edilmesi sonucunda "nitelikli" bilgi elde edilmesi amaçlanmaktadır. Bu amaç kapsamında modern tıbbın ve bu bağlamda sağlık hizmetlerinin nasıl bir dönüşüme uğrayacağı ve mikro düzeyde hasta-hekim ilişkisinin ne yönde etkileneceği gibi yanıtlanması güç sorular ortaya çıkmaktadır. Bu soruların yanıtı, teknolojinin ve bu bağlamda sağlık verilerinin nasıl kullanıldığı ile ilişkilidir. Bu bağlamda teknolojinin sağladığı yararlar ve ortaya çıkabilecek zararların hasta ve hekimlik mesleği açısından birlikte düşünülmesi önemli görünmektedir.

Bununla birlikte toplum yararı açısından gerekli olan verinin nasıl toplanması gerektiği de önemli bir sorundur. Veri toplamanın süreçlerinden biri olarak belirtilen eşitlik ve adalet ilkesinin önemi, sağlık verilerinden elde edilen faydaların bireyler arasında eşit bir şekilde dağıtılabilmesinde ortaya çıkmaktadır. Haklara dayalı bir etik anlayışını savunan John Rawls, 20. yüzyılın en önemli teorisyenlerinden biri olarak *Bir Adalet Teorisi* adlı kitabında, "Toplumun her bir üyesi, adaletin içinde bozulmazlık bulunduğunu veya bazıları da doğal hakların herkesin refahına aykırı olmadığını düşünür. Adalet, daha büyük iyiyi paylaşanlar tarafından birilerinin özgürlüğünün kaybının doğru olduğu düşüncesini reddeder. Kazançları ve farklı kişilerin kayıplarını dengeleyen gerekçe, eğer bir tek kişiyi dahi hariç tutarsa adil değildir. O nedenle, adil bir toplumda bahşedilmiş olan temel özgürlükler ve adalet tarafından korunan haklar, siyasal pazarlıklara veya sosyal çıkar hesaplarına konu edilemez." diye yazmaktadır (Rawls, 1971, s.57). Rawls, toplumsal görevlerin ve faydaların bireyler arasında eşit dağıtılması gerektiğini savunur. Bunun yanı sıra bir toplumda istisnai olarak eşitsiz bir dağılım yapılmasının biricik gerekçesi, toplumda en yoksul olanın yararına olması koşulu olabilir. Bu bağlamda toplum yararı açısından veri toplanırken, herkesten eşit bir şekilde veri toplanmalı, (eğer Büyük Veri analizi ile bir yarar elde edilmesi hedefleniyorsa toplumun savunmasız gruplarından başlayarak veri toplanmalı) ve

verisi toplanan savunmasız grupların haklarını korumak için daha temkinli bir hukuki zemin oluşturulmalıdır.

Sağlığa, hastalığa ve insana olan bakışının tarih boyunca değişiklik gösterdiği ve sağlık hizmeti anlayışının da bu değişikliklere göre biçimlenerek günümüzdeki halini aldığı belirtilmektedir (Bulut & Civaner, 2016). Günümüzde sağlığın sağlık hizmetlerinden çok daha fazlası olduğu, sağlık ve sosyal koşulların birbirine bağlı olduğu kabul edilmektedir. Buna göre genetik miras, erken çocukluk gelişimi, yaşam biçimi/bireysel seçimler, barınma koşulları, beslenme, iş ve çalışma koşulları, eğitim, kültürel değerler, toplumsal cinsiyet ve nitelikli sağlık hizmetlerine erişim sağlığın belirleyenlerini oluşturmaktadır. Sağlığın sosyal belirleyicisi olarak adlandırılan ve sağlığın sosyal belirleyicilerinin bir toplumun sağlığına etkisini konu alan birçok çalışma bulunmaktadır (Bunker, 2001; DeBolt & Harris, 2021; Jilani ve ark., 2021; Wilder ve ark., 2021). Bu çalışmalarda, sağlığın özellikle sosyo-ekonomik çevre faktörüne bağlı olduğu vurgulanmaktadır. Sağlığın çok sayıda etken tarafından belirlendiği ve sağlığı belirleyen etkenler içerisinde daha çok gelir eşitsizliğine dayalı ekonomik durumlar nedeniyle sağlığa ve sağlık hizmetlerine erişimin azaldığı bildirilmektedir (Barry, 2017). Dolayısıyla hastalıkların tedavisi yalnızca sağlık hizmetlerine erişim ile mümkün değildir. Örneğin bir insanın çalışmaması, o kişinin hasta olma ihtimalini artırmaktadır. Her ne kadar bugün sağlığın sosyal belirleyicilerinin önemi anlaşılmış olsa da sosyal belirleyicilere yönelik politikalar yaygınlaştırılmadığı için sağlıkta yaşanan eşitsizlikler, tüm dünyada en önemli sorunlardan biri olarak varlığını sürdürmektedir. Nitekim Dünya Sağlık Örgütü, 2005 yılında sağlık eşitsizliklerine yol açan sosyal faktörleri ve sağlıkta eşitliği teşvik için neler yapılabileceğini (küresel olarak) araştırmak için "Sağlığın Sosyal Belirleyicileri Komisyonu" nu kurmuştur (WHO, 2005).

Günümüz teknolojik gelişmeleri dikkate alındığında ve insanlığın geldiği "yapay zeka çağında", teknoloji tabanlı uygulamalara sağlık hizmetlerinde daha çok yer verilmektedir. Buna karşın sağlıkta eşitsizlikler, bilgi ve iletişim teknolojilerine erişim açısından da yaşanmaktadır. Buna göre bugün teknolojiye gelişigüzel erişim, toplumların sağlığını önemli ölçüde etkileyen belirleyenlerden biri olarak karşımıza çıkmaktadır. Dijital sağlık teknolojilerinin sağlık hizmetlerinde uygulanmasının

eşitsizlere neden olabileceği, yapılan araştırmalarla desteklenmektedir (Arun & Elmas, 2020; Henni, Maurud, Fuglerud & Moen, 2022; Mahajan, Lu, Spatz, Nasir & Krumholz, 2022; Yao ve ark., 2022). Türkiye'de yapılan bir çalışmada dijital teknolojiye erişim sorunu özellikle yaş faktörüne bağlı olarak incelenmektedir (Fiğan & Dede Özdemir, 2020). Söz konusu dijital teknoloji olduğu için, dijital eşitsizlik daha çok yaşlılık kavramı ile birlikte düşünülebilmektedir. Bunun yanı sıra dijital teknolojiye erişim, kültür, dil ve gelir düzeyi kavramları ile birlikte de incelemek gerekir. Sağlık hizmetlerinde dijital teknolojilerinin benimsenmesinin neden olduğu sağlık eşitsizliklerini araştıran bir çalışmaya göre eşitsizliğin ilk nedeni, kişilerin teknolojiyi elde edememesidir. Yaş, ırk, bölge, ekonomi, eğitim düzeyi, sağlık koşulları ve e-sağlık okuryazarlığı faktörleri de eşitsizlikleri etkilemektedir (Yao ve ark., 2022). Sağlık hakkı açısından sağlık hizmetlerinin kapsayıcı olması önemli görünmektedir. Dolayısıyla bu alandaki eşitsizliklerin derinleşmemesi için konuyla ilgili olarak herkesin, sağlık verisi işleyen veri kayıt sistemlerine erişimi olmalı, özellikle dezavantajlı gruplar için dijital sağlık teknolojilerine erişim ve kullanılabilirlik önem taşımalıdır.

5.1.4.1.İlgili düzenlemeler, eşitlik ve adalet ilkesi ile uyumlu olmalı

Sağlık hizmetinin adil ve etkin bir şekilde sunulması için ilgili yasal düzenlemeleri, veri kayıt sistemlerine erişim açısından incelemek gerekir. Buna göre KSV Yönetmeliği'nin 6. maddesinin üçüncü fıkrası, e-Nabız kaydı bulunmayan kişilerin haklarını düzenlemesi açısından önemlidir (2019);

> "… a) Kişinin kayıtlı olduğu aile hekimi tarafından herhangi bir süre sınırı olmaksızın, b) Kişinin sağlık hizmeti almak üzere randevu aldığı hekim tarafından, randevunun alındığı gün ile sınırlı olmak kaydıyla ve alınan sağlık hizmeti ile doğrudan bağlantılı işlemler sonlanana kadar, c) Kişinin sağlık hizmeti almak üzere giriş yaptığı sağlık hizmeti sunucusunda görev yapan hekimler tarafından, yirmi dört saat süre ile sınırlı olmak kaydıyla, ç) Hastanın yatışının yapıldığı sağlık hizmeti sunucusunda görev yapan hekimler tarafından, hasta sağlık hizmeti sunucusundan taburcu olana kadar."

E-Nabız kaydı bulunmayan kişilerin sağlık verilerine erişimini düzenleyen bu madde, sağlık personelinin sağlık kayıtlarını sınırsız erişimini sınırlandırması ve kişilerin sağlık hizmetine erişim hakkını gözetmesi bakımından eşitlik ve adalet ilkesi ile

uyumludur. Diğer taraftan bu maddenin hasta mahremiyeti açısından da tartışılması gerekmektedir. (Bu konuya tartışmanın ilerleyen bölümlerinde yer verildiği için burada tartışılmaması uygun görülmüştür.) KSV Yönetmeliği'ndeki bu madde dışında özellikle kişisel veri kayıt sistemlerine kültür, dil, gelir düzeyi ve yaş gibi faktörlere bağlı olarak yaşanabilecek erişim sorunları açısından bir düzenleme maddesi saptanmamıştır. Dolayısıyla ilgili mevzuatın dijital teknolojiye erişim açısından eşitlik ve adalet ilkesi ile uyumlu olmadığını vurgulamak gerekmektedir.

İlgili düzenlemeler, dezavantajlı grupların hakları açısından incelendiğinde, KSV Yönetmeliği'nin 8. maddesi ile çocukların sağlık verilerine erişim hakkı düzenlendiği görülmektedir. Bu madde, ebeveynlerin çocuklarının sağlık verilerine herhangi bir onaya ihtiyaç duymaksızın e-Nabız üzerinden erişebileceğini, ayırt etme yeterliğine sahip çocukların ise e-Nabız üzerinden ebeveynlerini izne tabi tutabileceklerini bildirmektedir. Anne ve babanın boşanması durumunda da çocuğun kişisel verilerine, velayet hakkı bulunmayan anne ya da babanın erişim sağlayabileceği belirtilmektedir. İlgili yönetmelik, savunmasız grup olarak sadece çocukların ve ölülerin kişisel sağlık verilerine erişimi düzenlemiştir. Ölmüş bir kimse, artık kişi sayılamayacağı için savunmasız veya dezavantajlı bir grup içerisinde nitelendirilemez. Ancak söz konusu kişisel veri olduğu için, yaşamın sona ermesinden sonra da ölen kişinin onurunu korumak gereği yönetmeliğin bu maddesine burada yer verilmiştir. İncelenen düzenlemelerde hakları korunan bir diğer savunmasız grup deneklerdir. Bu konuda HMEK'in 43. maddesi bilimsel araştırmalarda deneğin kimliğinin gizli tutulmasını vurgulamakta ve deneğin kişisel verilerinin korunması hakkını belirtmektedir. Aynı düzenlemenin 35. maddesi tutuklu ve hükümlülerin gizlilik haklarının korunması gerektiğini belirterek tutuklu veya hükümlünün kişisel verilerine vurgu yapmaktadır. Hem deneklerin hem de tutuklu ve hükümlülerin kişisel verilerinin korunması hakları, HMEK'ten başka bir düzenleme maddesinde yer almamaktadır.

Diğer savunmasız gruplar olarak kadınlar, LGBTQ+ bireyler, engelli bireyler, yaşlılar ve psikiyatrik desteğe ihtiyaç duyan kişilere yönelik olarak ne KVK Kanunu ne de KSV Yönetmeliğinde bir düzenleme maddesi bulunmamaktadır. Kadınlar erkek egemen bir toplumda ezilen bir grubu oluşturmaları ve devam eden kadına şiddet olayları nedeniyle dezavantajlı gruptadır. Kadına ait kişisel bilgiler, sadece kurum ve

kuruluşlara yönelik değil, potansiyel şiddet kaynağı olan başta eş, baba ve oğul statüsündeki bireylere karşı da korunması gerekebilmektedir. Bu nedenle kadının kişisel sağlık verilerini korumak için daha farklı bir politika izlenmelidir. Bu bağlamda kadının sağlık verileri de hassasiyet düzeyi yüksek veriler olarak kabul edilmelidir.

Bir diğer dezavantajlı grup LGBTQ+ bireylerdir. LGBTQ+ bireylerin toplumda ötekileştirilme, ayrımcılığa uğrama ve damgalanma gibi istenmeyen durumlara daha çok maruz kaldığı bilinmektedir (Keleş, Yılmaz Özpolat & Yalım, 2020). Bu nedenle özellikle cinsel yönelimle ilgili bilgilerin yasa tarafından daha hassas düzeyde korunması gerekir. Çocuklar, yaşlılar, engelli bireyler, denekler ve psikiyatrik desteğe ihtiyaç duyan bireylerin kişisel sağlık verileri çok daha önemli olabilmektedir. Bu durumun en uç örneklerinden biri, bir siyasi parti tarafından, kısıtlı seçmen listesinin elde edilmesi ve bu verilerin, seçim sonuçlarını etkilemek için kullanmasıdır (Öztürk, 2019). Bu örnek, verinin kötüye kullanımı açısından çok önemlidir. Dolayısıyla yukarıda belirtilen dezavantajlı gruplar ve varsa diğer gruplar açısından kişisel sağlık verilerinin korunması için özel hukuksal bir koruma alanına ihtiyaç bulunmaktadır. Bu bağlamda incelenen mevzuatın eşitlik ve adalet ilkesi ile uyumlu olmadığı ve mikro düzeyde hekimlerin dezavantajlı gruplara yaklaşımı açısından yol gösterici olmadığı vurgulanabilir.

Yasal düzenlemelerin yol gösterici olmaması, tıp etiği açısından hekimin eşit hizmet sunma ödevi açısından bir risk oluşturmaktadır. Cenevre Bildirgesi'nde hekimlere yaş, hastalık ya da engellilik, inanç, etnik köken, cinsiyet, milliyet, politik düşünce, ırk, cinsel yönelim ya da toplumsal konuma göre değerlendirmelerin göreviyle hastası arasına girmesine izin vermemesi gerektiği belirtilmektedir. Hekimlerin acil durumlar dışında hizmet sunmayı reddetmelerinde haklı çıkarılabilecek gerekçelerin varlığı ise halihazırda tartışmalıdır. Savunmasız veya dezavantajlı grupların kişisel sağlık verilerinin korunmasında yaşanabilecek insan hakları ihlalleri karşısında yasal düzenlemelerin yeterince yol gösterici olmadığı durumlarda meslek ahlakı açısından hekimlerin sorumlulukları bulunmaktadır. Buna göre hekimlerin verisi işlenecek dezavantajlı hastayı veri işleme süreci hakkında bilgilendirmek ve veri işlenmesi ile elde edilebilecek bir yarar varsa, önceliği dezavantajlı hastaya vermek gibi pozitif ayrımcılığa dayalı sağlık hizmeti sunabilir.

5.1.4.2.Eşit ve adaletli bir kişisel sağlık kaydı uygulaması nasıl olmalı?

Elektronik sağlık kayıt sistemleri, başlangıçta hastalar için sağlık hizmeti sunumunda klinik karar vermeyi kolaylaştırmak ve bakım kalitesini artırmak için tasarlanmıştır (Lee ve ark., 2020). Elektronik sağlık kayıt sistemlerinin tüm dünyada yaygınlaşması ile Dünya Sağlık Örgütü, iyi bir sağlık kayıt sisteminin üç bileşenine vurgu yapmıştır. Buna göre, sağlık kayıt sistemi, hastanın hastaneye ilk gelişinden veya hastaneye gelmesinden itibaren hastanın tüm sağlık bilgilerini içermeli, hastanın yaşamı boyunca sağlık bilgileri, sağlık hizmeti sunucuları tarafından girilmeli ve hastayla ilgilenen tüm sağlık hizmeti sunucularının bilgilere kolayca ulaşabilmesi sağlanmalıdır (WHO, 2019).

Günümüzde sağlık veri tabanları bireyin, hekim tarafından oluşturulan tıbbi kayıtları ile hasta tarafından oluşturulan kişisel sağlık kaydını entegre edecek şekilde tasarlanmaktadır (Garret & Seidman, 2011). Böylece hastanın toplam sağlığına odaklanılacak, standart klinik verilerin ötesine geçilecek ve hastanın bakımı konusunda daha geniş bir bakış açısı sağlanabilecektir (Garret & Seidman, 2011). Bu bakış açısına göre özellikle kişisel sağlık kayıt sistemlerinden adaletli bir şekilde yararlanmak için herkesin uygulamaya erişimi olmalıdır. Çünkü doğru ve etkili kullanım sağlandığında bu sistemlerin sağlık hizmetlerinde oldukça önemli yararları bulunabilmektedir. Örneğin birinci basamak sağlık hizmetlerinde toplanan bilgiler, acil servis hekimine hastanın yaşamı tehdit eden alerjisi hakkında bilgi verir ve böylece hasta bilinçsiz olsa bile tedavisi uygun bir şekilde planlanabilir (Garret & Seidman, 2011). Aynı zamanda hasta sağlık kurumunu değiştirdiğinde, kişisel sağlık kaydında kayıtlı olan sağlık verilerinden yararlanılması ile tedavi sürecinin etkin ve doğru bir biçimde yürütülmesi sağlanabilir. Yeni reçeteler yazılırken ilaç etkileşimlerinin kontrol edilebilmesi ve laboratuvar testlerinin gereksiz tekrarlarından kaçınılması gibi yararlar da sağlayabilir. Bugün e-Nabız üzerinden randevu alabilmek, sağlık bilgilerini görüntülemek, en yakın hastane ve eczane konumunu öğrenebilmek ve nöbetçi eczaneleri görebilmek mümkündür. Kişinin kendi sağlığını yönetebilmesi açısından bu özelliklerin çok değerli olduğu belirtilebilir. Bu ve benzeri özellikler dikkate alındığında, kişisel sağlık kayıt sistemi olarak kullanılan e-Nabız uygulamasının, toplumda yaygınlaştırılması önemli görünmektedir. Çünkü uygulama, sağlık

hizmetlerine erişim açısından sağlık hizmeti sunumunun bir parçası haline gelmiştir. Sağlık hizmetlerine olumlu değerler katan ve sağlık hizmetlerinde giderek daha fazla kullanım alanına sahip olan benzeri uygulamalara erişim giderek önem kazanmaktadır. Özellikle ulusal bir kayıt sistemi olarak e-Nabız uygulamasının olağan durumlar için kullanılmaya devam edecek olması nedeniyle, başta kişilerin sosyoekonomik durumlar ve coğrafi koşullar açısından erişim sorunları giderilmelidir. Buna göre örneğin uygulamanın internet bağlantısı olmadan da çalışabilmesi gerekir. Yanı sıra bazı dezavantajlı gruplar için de bazı özelliklere sahip olmalıdır. Bu bağlamda e-Nabız kullanıcı değerlendirmelerini araştıran bir çalışmada, uygulamanın tüm engelli kullanıcıları kapsayacak şekilde herkes tarafından eşit olanaklarla erişilebilir olması vurgulanmış ve özellikle görme engelli kullanıcılara yönelik sesli uyarı eklenmesi gibi çözümler önerilmiştir (İnal & Ercil Cağıltay, 2019).

Kişisel sağlık kaydı uygulamaları özellikle olağandışı durumlarda eşitlik ve adalet ilkesinin önemini daha çok hissettirmektedir. Mobil sağlık uygulamaları ile ilgili bir çalışmada, eşitlik ve adalet ilkesine vurgu yapılmış ve bu uygulamaların okur-yazar olmayanlar, düşük gelirli gruplar ve yaşlılar için zorluklar yaratacağı ileri sürülmüştür. Bu bağlamda sağlık hizmetlerine en çok gereksinimi olanların ulaşamayacağı belirtilmiş, daha genç ve varlıklı insanların daha çok erişim sağlayacağı ifade edilmiştir (Lucivero & Jongsma, 2018). Dolayısıyla sağlık hizmetleri kapsamında kullanılacak kişisel sağlık kaydı uygulamaları sağlıkta eşitsizlikleri derinleştirmemelidir. Bunun için ilk olarak uygulamaların güvenli ve etkili kullanımları üzerinde durulmalı, etkili ve güvenli olan uygulamalar sağlık hizmeti kapsamına alınmalıdır. Söz konusu olağandışı durumlarda ise herkesin eşit, adil ve uygun bir şekilde bu tür uygulamalardan yararlanabilmesi için erişim sorunları giderilmeli ve uygulamaların teknik sorunları çözümlenmelidir.

5.1.5. Özerklik ilkesi açısından

Sağlık verilerinin mahremiyet ve gizliliği konularından sonra en çok tartışma konusu özerklik hakkında olduğu belirtilebilir. Sağlıkta Büyük Veri, tıp etiği açısından önemli değer sorunları ortaya yaratabilmektedir. Özerklik bu değer sorunlarının içerisinde üzerinde en çok durulması gereken konulardan birini oluşturmaktadır. Özerklik ilkesi, toplum yararına gerekli olan minimum düzeydeki verinin, etik

açısından bu ilkenin korunarak toplanması gerektiğini ifade etmektedir. Özerklik bir kişinin başkaları tarafından kısıtlama olmaksızın uygun gördüğü şekilde yaşama özgürlüğüne atıfta bulunmakta ve birçok ahlaki ve politik teorinin temel bir değeri olarak ifade edilmektedir (Christman, 2015). Söz konusu hassas veri olduğunda en kısa tanımıyla kişinin verileri üzerindeki denetim ve kontrolünü ifade etmektedir. Bununla birlikte özerklik, hekimlerin hastalarını nasıl tedavi edeceklerine karar vermeleri anlamında da karşımıza çıkmaktadır.

Günümüz Büyük Veri çağında özerkliğin gerçekten mümkün olup olmadığı teorik olarak tartışmalıdır. Özerkliği korumanın en önemli koşulu ise aydınlatılmış onam alınmasıdır. Buna göre hangi kişisel veriler için mutlaka aydınlatılmış onam alınması gerektiği, önceden izin alınmasının mümkün olmadığı durumlar için daha önce toplanmış verilerin belli amaçlar için kullanılıp kullanılamayacağı, başlangıçta tanımlanan amaçlardan farklı olarak verilerin yeniden kullanılması durumunda onamın gerekli olup olmadığı gibi sorular oldukça tartışmalıdır. Yanı sıra karar verme yeterliği olmayan kişilerin aydınlatılmış onamlarının nasıl alınacağı sorunu da bir başka tartışma konusudur.

5.1.5.1.İlgili düzenlemeler özerklik ilkesiyle uyumlu olmalı

Teorik tartışma

Özerklik ilkesi, biyomedikal araştırmalarda kişinin özgür ve aydınlatılmış onamını vermesi ve bu onamı istediği zaman geri çekebilmesi biçiminde uygulanmaktadır. Sağlık alanında insan onurunun korunması, özerklik ilkesi ile sağlanmaya çalışılır. Biyomedikal araştırmalardan farklı olarak sağlık hizmetlerinin geliştirilmesi için toplanan kişisel sağlık verileri için özerklik ilkesi ise tartışmalıdır. Çünkü yapılacak çalışmalar, insan deneyi yerine verilerin analizini veya kayıtların incelenmesini içermektedir (Mann, Savulescu & Sahakian, 2016). Bu nedenle özerkliğin hakim olduğu anlayışın yerini ortak iyiyi uygulayan bir modelin alması gerektiği düşünülür (Hoffman, 2016). Bununla birlikte dijital bir dünyada kişisel sağlık verileri için kişilik haklarını korumak amacıyla alınan aydınlatılmış onamı, hakkıyla almak mümkün müdür sorusunu tartışmak gerekmektedir. Çünkü gizliliği koruyabilmek için verileri anonimleştirme ve veri güvenliğini sağlamaya yönelik araçlar gerekli olmakla birlikte

yeterli değildir. Örneğin Büyük Veri analiz yöntemlerinden biri kullanılarak birbirleriyle ilgisiz gibi görünen verilerin ilişkilendirilmesi sonucu kimlik bilgileri belirlenebilmektedir. Dolayısıyla dijital dünya, tam olarak veri güvenliğini sağlamaya izin vermemektedir. Bu konuda Avrupa Konseyi (2017), bir kişinin kişisel verilerini kontrol etme hakkına ve bu tür verilerin işlenmesine dayalı özerkliğin korunmasının güvence altına alınmasının gerekli olduğunu vurgulayarak Büyük Veri uygulamalarının karmaşıklığı ve belirsizliğinden dolayı özerkliğin Büyük Veri bağlamında dikkatle ele alınması gerektiğini belirtmektedir (Avrupa Konseyi, 2017). Bir çalışmada, kişisel bilgilerin işlenmesi için yasal bir dayanak olarak özerkliğin Büyük Veri çağında iyi işlemeyeceği ileri sürülmektedir (Cate, Cullen & Mayer-Schonberger, 2013). Bir başka çalışmada günümüzde yaptığımız, söylediğimiz, gördüğümüz, hissettiğimiz ve düşündüğümüz her şeyin izlendiği ve ölçüldüğü için özgür irademizi kullanamadığımız ve bu nedenle bizi rızaya zorlayan baskılara karşı kendi kararlarımızı alamadığımız vurgulanmaktadır (Leonhard, 2018). Dolayısıyla dijital dünyada bireysel olarak özerkliğin sürdürülebilmesi çok güç ve tartışmalı görünmektedir.

Bugün verilerin elektronik ortama aktarılması, bir hedef olarak seçildiğinde yetkisiz erişimlere açık hale getirilmesi riskini barındırmaktadır. Bir diğer sorun verilerin hem hükümetler hem de çeşitli şirketlerin kendi amaçları doğrultusunda kullanılabileceği yönünde riskler içermesidir. Özellikle sağlık verilerinin ekonomik değeri nedeniyle kişisel veriler, alınıp satılabilen bir meta olarak algılandığı için verilerin kötüye kullanım olasılıkları artabilmektedir. Türkiye'deki kötüye kullanımın en çok bilinen örneği, İstanbul yerel seçimlerinde e-Nabız kaydındaki verilere erişim sağlanmış ve zihinsel engelli ya da kısıtlılık gerekçe gösterilerek seçimlerin iptalinin istenmesi daha önce de belirtilmişti. Bu durum sağlık bilgisinin birer manipülasyon aracı olarak kullanılmasında çok önemli bir yeri olabileceğini göstermektedir. Dolayısıyla verinin dijital ortama aktarılması, veriyi aynı zamanda suiistimale açık hale getirmek demektir. İçinde bulunulan zaman dilimi içerisinde veri güvenliği temin edilse bile gelecekte veriyi elinde bulunduranlar veriyi kötüye kullanabilirler. Böyle bir gerçekliğin karşısında bireylerin onamını almak anlamlı mıdır yoksa bu durum bizler için sadece bir risk midir? Üstelik bu riskler göz önüne alındığında, bütün bunların risk olmanın ötesinde, gerçekleşeceği kesinliği kendini göstermektedir. Böyle bir durumda

aydınlatılmış onamı tartışmak, anlamını yitirmektedir. Bir çalışmada hasta bilgilerini tamamen güvenli tutma yeteneğine sahip olunmadan veri tabanlarına hassas sağlık bilgilerinin eklenmemesi gerektiği belirtilmektedir (Clemens, 2012). Bu sorunlar karşısında şu soruyu sormak gerekmektedir; eğer aydınlatılmış onamın amacı olan kişilik haklarını koruyarak veri toplamak mümkün değilse sağlık hizmeti nasıl verilecektir? Bu soruya yanıt verebilmek için sağlık verisine neden ihtiyaç olduğunu sorgulamak gerekir. Buna göre tıbbi bakımın iyileştirilmesi, bakım kalitesinin artırılması ve bir bütün olarak sağlık hizmetlerinin geliştirilebilmesi nedenleriyle sağlık verisine ihtiyaç vardır. Bu veriler kullanılarak bilimsel ve istatistiksel değerlendirmeler yapılabilir ve sağlık hizmetleri toplum yararına olacak şekilde planlanabilir. Bu durumda yukarıda sayılan kaygılar çok önemli olsa da sağlık hizmetlerinde belli verilerin toplanmasının artısını dikkate almak gerekir. Dolayısıyla sağlıkta bütüncül yaklaşımdan uzaklaşmamak adına özerkliğin teorik açıdan mümkün olduğu önermesini benimsemek gerekmektedir.

Tüm sağlık verileri için aydınlatılmış onam alınmalıdır

Daha önce sıklıkla belirtildiği üzere verinin mülkiyeti kişinin kendisine aittir. Bu nedenle kişisel sağlık verilerinin toplanma amacı ne olursa olsun hiç kimse verilerinin işlenmesini kabul etmek veya verilerinin işlenmesine izin vermek zorunda değildir. Bu bağlamda bireyin kişisel sağlık verilerinin işlenmesine izin vermediği durumlarda sağlık hizmetine erişim hakkı engellenmemelidir.

Konuyla ilgili yasal düzenlemeler incelendiğinde, Anayasa'nın 20. maddenin üçüncü fıkrası, bilgilendirilme, verilere erişim, verilerin düzeltilmesini veya silinmesini talep etme ve verilerin amaçları doğrultusunda kullanılıp kullanılmadığını öğrenme haklarını tanımlamaktadır (T.C. Anayasası, 1982).

> "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."

Yanı sıra bu madde ile kişisel verilerin ancak kanunlarda öngörülen hallerde veya kişinin açık rızası alınarak işlenebileceği belirtilmektedir. Anayasal güvence altına alınan kişisel verilerin korunmasını düzenleyen KVK Kanunun üçüncü maddesinde açık rıza, "Belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle açıklanan rıza" biçiminde tanımlanmaktadır. Kanunun 11. maddesinde, özerklik kapsamındaki temel haklar tanımlanmaktadır (2016);

> "(1) Herkes, veri sorumlusuna başvurarak kendisiyle ilgili; a) Kişisel veri işlenip işlenmediğini öğrenme. b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme. c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme. ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme. d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme. e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme. f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme. g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme. ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme, haklarına sahiptir."

Buna göre kişinin kendisiyle ilgili veri işlenip işlenmediğini öğrenme, işlenen verilerine ilişkin bilgi talep etme, verinin işlenme amacına uygun olarak kullanılıp kullanılmadığını öğrenme, verinin aktarıldığı üçüncü tarafları bilme ve verinin silinmesi veya yok edilmesini isteme hakları bulunmaktadır.

Kanunun (2016) 6. maddesinin üçüncü fıkrasında, hassas verinin açık rıza aranmaksızın işlenebilmesi için istisnai durumlar açıklanmaktadır.

> "…(3) Birinci fıkrada sayılan 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."

Kanunun bu maddesinde, verinin "sağlık hizmetlerinin sunulması", "planlaması" ve "yönetimi" amaçlarıyla "açık rıza aranmaksızın" sır saklama yükümlülüğü altında

bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından işlenebileceği açıklanmaktadır. Kanunun 6. maddesinin ikinci fıkrası, özel nitelikli kişisel verinin açık rıza olmaksızın işlenmesini yasaklamaktadır. Ancak hemen ardından gelen üçüncü fıkra ile aydınlatılmış onama istisna getirilmiş, sağlık ve cinsel hayatla ilgili verilerin, onam aranmaksızın işlenebileceği belirtilmiştir. Buna göre verinin işlenebilmesi için kamu sağlığının korunması, koruyucu hekimlik, tıbbî teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amaçları ileri sürülerek toplum yararına işaret edilerek Kanunun altıncı maddesinde özerklik değeri harcanmıştır. Bu bağlamda Kanunun bu maddesinde belirtilen amaçlarla sağlık verisinin "açık rıza olmaksızın" işlenebilir olması, haklı çıkarılabilir mi sorusu ortaya çıkmaktadır. Bu soru toplum yararı açısından sağlık verisine ihtiyaç olması nedeniyle haklı çıkarılabilir gibi görünmektedir. Ancak aydınlatılmış onam alınarak ihtiyaç duyulan veriyi elde etmek mümkündür. Biyotıp Sözleşmesi başta olmak üzere insan onuru ve kişilik haklarının korunması, toplum yararından önce gelmektedir. Bununla birlikte KVK Kanununda daha önce işaret edilen belirsizlikler ve yukarıda ifade edilen riskler dikkate alındığında veri toplamanın amacı ne olursa olsun verilerin aydınlatılmış onam alınarak işlenmesi bu bağlamda özerkliğin bir dereceye kadar korunması bir gereklilik olarak kendini daha çok göstermektedir.

Gerekli tüm bilgiler eksiksiz bir şekilde verilmeli

Özerklik ilkesinin en önemli bileşenlerinden biri kişisel veriler için aydınlatılmış onam alınmasıdır. Bununla birlikte aydınlatılmış onam ile ilgili çeşitli sorunlar vardır. Genellikle aydınlatılmış onam kavramı, Türkiye'de "bilgilendirilmiş onam" kavramı ile aynı anlamda kullanılmaktadır. Bu nedenle aktarılan bilgileri hastaların anladığı varsayılır ve onam formlarının imzalanması ile aydınlatışmış onamın alındığı düşünülür. Bu formlar, insanları gerçekten bilgilendirmek yerine kuruluşları sorumluluktan korumak için kullanılan uzun ve karmaşık listeler olabilmektedir (Mann ve ark., 2016). Bir başka sorun bu formlarda sunulan bilgilerin uzunluğu ve karmaşıklığı nedeniyle, bazı hastalar bunları okuyamamakta veya anlayamamaktadır (Gostin, 2006). Halihazırdaki bu sorunlarla birlikte kişisel sağlık verilerinin işlenmesi

ve çeşitli amaçlarla kullanılması için aydınlatılmış onam alınması, kişilere salt bilgi verilmesi düzeyinde kalabilmektedir.

Bilgi edinmek, bizim en temel haklarımızdan birisidir. Bu hak kapsamında özel bir düzenleme olarak Bilgi Edinme Kanunu bulunmaktadır. Bu kanunun 4. maddesine göre herkes kendi verileri hakkında bilgi edinme hakkına sahiptir. Bilgi edinmek KVK Kanunu'nda veri sorumlusunun aydınlatma yükümlülüğü kapsamında düzenlenmiştir. Buna göre Kanunun 11. maddesinde herkes kendi verisiyle ilgili olarak bilgi edinme hakkına sahiptir (2016);

> "(a) Kişisel veri işlenip işlenmediğini öğrenme. b) Kişisel verileri işlenmişse buna ilişkin bilgi talep etme. c) Kişisel verilerin işlenme amacını ve bunların amacına uygun kullanılıp kullanılmadığını öğrenme. ç) Yurt içinde veya yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri bilme. d) Kişisel verilerin eksik veya yanlış işlenmiş olması hâlinde bunların düzeltilmesini isteme. e) 7 nci maddede öngörülen şartlar çerçevesinde kişisel verilerin silinmesini veya yok edilmesini isteme. f) (d) ve (e) bentleri uyarınca yapılan işlemlerin, kişisel verilerin aktarıldığı üçüncü kişilere bildirilmesini isteme. g) İşlenen verilerin münhasıran otomatik sistemler vasıtasıyla analiz edilmesi suretiyle kişinin kendisi aleyhine bir sonucun ortaya çıkmasına itiraz etme. ğ) Kişisel verilerin kanuna aykırı olarak işlenmesi sebebiyle zarara uğraması hâlinde zararın giderilmesini talep etme."

Kanunun bu maddesi incelendiğinde, bilgilendirmenin yetersiz olduğu belirtilebilir. İlgili maddede verilerin işlenip işlenmediğini öğrenme, işlenmişse hangi bilgilerin işlendiğini talep etme, amacına uygun işlenip işlenmediğini öğrenme, üçüncü taraflarla paylaşımı gibi konular hakkında bilgilendirilme hakları gözetilmektedir. Ancak veri işleme sürecindeki riskler ve yüklerin neler olduğu, verilerin söz konusu olabileceği ticari kullanımları, bireylerin istedikleri zaman onamlarını değiştirip değiştiremeyecekleri, veri sahibi ve veri sorumlusu arasındaki güç dengesizliği durumlarında onamlarının etkilenip etkilenmeyeceği gibi konularda bir bilgilendirme söz konusu değildir. Bu konuların belirsiz olması, bilgilendirmeyi içerik açısından yetersiz kılmaktadır. Uygun bir aydınlatılmış onam için kanun kapsamında gerekli tüm bilgilerin eksiksiz bir şekilde verilmesi gerektiği belirtilmeli, ilgili yönetmelikler kapsamında ise onamın nasıl alınacağı ayrıntılı olarak açıklanmalıdır. Onamın nasıl alınacağına ilişkin Kişisel Verileri Koruma Kurumu'nun çıkardığı Aydınlatma

Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ oldukça değerlidir.

KVK Kanunu'nun 6. maddesinde, özel nitelikli verilerin sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından ilgilinin açık rızası aranmaksızın işlenebileceği belirtilmektedir. Bu maddedeki "yetkili kurum ve kuruluşların" belirsizliğine daha önce işaret edilmiş ve daha somut bir şekilde ifade edilmesi gerektiği belirtilmişti (Bkz. s.220). Bu belirsiz ifadenin aynı zamanda özerklik ilkesi açısından yeterli düzeyde bir bilgilendirme sağlamadığı ileri sürülebilir. Bilgilendirme kapsamında hangi kurum ve kuruluşların bu bilgilere erişim sağlayabileceği açık ve net bir şekilde belirtilmelidir. KVK Kanunun bütününe bakıldığında Md.6, Md.12, Md.18, Md.19 ve Md.20 maddelerindeki belirsizlikler nedeniyle (Bkz. s.221) bilgilendirme açısından yeterli bulunmamıştır. Buna göre gizliliğin nasıl sağlanacağı, hangi koşullarda aktarım yapılacağı, yurt dışına aktarımın koşullarının neler olacağı, verilerin depolanması ve kullanımındaki risklerin neler olduğu gibi konular, detaylı bir şekilde açıklanmalıdır. Kanunun altıncı maddesinde belirtilen istisnalar, sağlık verilerinin yurt içi ve yurt dışı aktarımı için de geçerlidir. Örneğin yurt içi aktarım ile yurt dışı aktarım durumunda farklı riskler ortaya çıkabilir ve bu durum karşısında özerklik açısından kişi verilerinin yurt içi aktarımına izin verebilirken yurt dışına aktarılmasına izin vermek istemeyebilir. Dolayısıyla Kanun, kişinin bu hakkını kullanabilmesi açısından elverişli olmalıdır.

> "Kişisel verilerin aktarılması MADDE 8- (1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın aktarılamaz. (2) Kişisel veriler; a) 5 inci maddenin ikinci fıkrasında, b) Yeterli önlemler alınmak kaydıyla, 6 ncı maddenin üçüncü fıkrasında, belirtilen şartlardan birinin bulunması hâlinde, ilgili kişinin açık rızası aranmaksızın aktarılabilir. (3) Kişisel verilerin aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır.
>
> Kişisel verilerin yurt dışına aktarılması MADDE 9- (1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz. (2) Kişisel veriler, 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede; a) Yeterli korumanın bulunması, b) Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması, kaydıyla ilgili kişinin açık rızası

aranmaksızın yurt dışına aktarılabilir. (3) Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilir."

Yukarıda kanunun veri aktarımını düzenleyen 8. ve 9. maddeleri incelendiğinde, 5. ve 6. maddede belirtilen istisnalara vurgu yapılarak özerklik sınırlandırılmakta ve kişinin özellikle yurt dışı aktarım için ret hakkını kullanabileceği açık ve net bir şekilde ifade edilmemektedir. Buna karşın kurulun çıkardığı Aydınlatılmış onam tebliği, bu konudaki açığı kapatmak için önemli görünmektedir. Buna göre tebliğin (2018) "f) Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı yerine getirilmesi gerekmektedir" biçimindeki 5. maddesi, açık rıza alınması ve bilgilendirme hakkını birbirinden ayırarak ifade etmiştir. Bu ifade aydınlatılmış onamın geçerliliği açısından oldukça önemli görünmektedir. Tebliğ bir bütün olarak incelendiğinde, bilgilendirme kapsamında veri sorumlusunun ve varsa temsilcisinin kimliği, verilerin hangi amaçla işleneceği, verilerin kimlere, hangi amaçla aktarılabileceği ve veri toplamanın yöntemi ve hukuki sebebi konuları hakkında bilgilendirme yapılması gerektiğini belirtmesi açısından ayrıntılıdır. Ancak bilgilendirme kapsamında ayrıca, verinin kullanımındaki riskler ve yükler, gizliliğin nasıl sağlandığı/korunduğu ve verinin varsa ticari kullanımı konuları hakkında da bilgilendirme yapılması gerektiğini belirtmemesi nedeniyle yetersizdir.

Gerekli bilgilerin verilmesi yeterli değildir, kişinin "anlaması" sağlanmalıdır

Bilgilendirme yapmanın yanı sıra kişinin verilen bilgileri anlamasının sağlanması uygun bir aydınlatılmış onamın en önemi özelliğidir. Böylece yapılan bilgilendirmenin tek taraflı olmasının önüne geçilebilir. Kişi, sağlık verilerinin işlenmesi sürecindeki tüm bilgileri öğrenmesinin ardından, verilerin işlenmesinin yararlarının olduğu kadar risklerini de anlamış olarak onam ya da ret verebilmelidir.

Konuyla ilgili KSV Yönetmeliği incelendiğinde, yönetmeliğin 6. maddesi, e-Nabız kullanıcısına gizlilik tercihleri konusunda kişinin özerkliğini korumaktadır. Buna göre, "(2) e-Nabız hesabı bulunan kişilerin sağlık verilerine, kendi gizlilik tercihleri çerçevesinde erişim sağlanır. İlgili kişiler, gizlilik tercihleri ve sonuçları konusunda ayrıntılı şekilde bilgilendirilir..." Bu madde ile kullanıcının bilgilendirilmesine de vurgu yapılmaktadır. Yönetmeliğin dördüncü bölümü sağlık verilerinin düzeltilmesini

isteme (13. Md.) ve kişisel verilerin imha edilmesini talep etme hakkını (14.Md.) düzenlemektedir. Yönetmelikte aydınlatılmış onam ile ilgili olarak Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ hükümlerine riayet edileceği belirtilmektedir.

Konuyla ilgili incelenen Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'in (2018) aydınlatılmış onam kapsamında kişinin anlamasını sağlamak için onamı alacak kişiye tanımladığı yükümlülükler tebliğin 5. maddesinde açıklanmaktadır.

> "g) Aydınlatma yükümlülüğü kapsamında açıklanacak kişisel veri işleme amacının belirli, açık ve meşru olması gerekir. Aydınlatma yükümlülüğü yerine getirilirken, genel nitelikte ve muğlak ifadelere yer verilmemelidir. Gündeme gelmesi muhtemel başka amaçlar için kişisel verilerin işlenebileceği kanaatini uyandıran ifadeler kullanılmamalıdır. ğ) Aydınlatma yükümlülüğü kapsamında ilgili kişiye yapılacak bildirimin anlaşılır, açık ve sade bir dil kullanılarak gerçekleştirilmesi gerekmektedir… ı) Aydınlatma yükümlülüğü kapsamında, kişisel verilerin aktarılma amacı ve aktarılacak alıcı grupları belirtilmelidir. i) Aydınlatma yükümlülüğü kapsamında kişisel verilerin, tamamen veya kısmen otomatik yollarla ya da veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yöntemlerden hangisiyle elde edildiği açık bir şekilde belirtilmelidir. j) Aydınlatma yükümlülüğü yerine getirilirken eksik, ilgili kişileri yanıltıcı ve yanlış bilgilere yer verilmemelidir."

Tebliğin bu maddesi aydınlatma kapsamında bilgilendirmenin nasıl yapılması gerektiğine ilişkin usul ve esasları belirtmesi açısından çok önemlidir. Bu maddenin özellikle (ğ) fıkrasında belirtildiği üzere bireye anlaşılır, açık ve sade bir dil kullanılarak bilgilendirilme yapılması gerektiği konusunda tanımlanan yükümlülük çok önemli olmakla birlikte yeterli değildir. Özellikle veri kayıt sistemleri açısından bu maddenin yeterli olmadığı ileri sürülebilir. Çünkü veri kayıt sistemi uygulamalarında tek yönlü olarak bilgi aktarımı gerçekleşir. Kişi anlayamadığı veya anlamını tam olarak kavrayamadığı bilgiler için soru soramamakta ve içsel olarak sorduğu soruları yanıtsız kalmaktadır. Dolayısıyla kayıt sistemleri ile ilgili pratikte onamın nasıl alınacağı önemli bir sorundur. Uygulamaların "Aydınlatma Metinlerinde" açıklanan bilgilerin altında "okudum, anladım" ifadesinin tek *–tık* ile işaretlenmesi ile alınan onay veya torba onam şeklinde alınan rızalar (onam değil, rızadır), açıklanan bilgilerin anlaşıldığını göstermemektedir. Kişinin hizmet alabilme

karşılığı olarak verilerini paylaştığına rıza gösterdiği anlamına gelmektedir. Bu nedenle özellikle sağlık hizmetleri kapsamında kullanılan veri tabanlarına veri girişi yapan hekimler, hastalarından aynı zamanda verilerinin işlendiği yönünde aydınlatılmış onam almalıdır.

Bu tebliğin uygun bir aydınlatılmış onam için yetersiz görüldüğü bir diğer nokta, kişinin "ret" olanağını kullanabilmesine ilişkin bir yükümlülük tanımlamamasıdır. Tıp etiği açısından aydınlatılmış onamın özelliklerinden biri de verilen bilgiler ışığında yapılacak işleme ret verebilmektir. Dolayısıyla bu olanağın bir kural olarak ilgili düzenlemelerde yer alması gerekir.

Verilerin kontrolü bireyin kendisinde olmalıdır

Özerklik ilkesi, kişinin kendi verilerinin yönetimini bireyin kendisinde olması gerektiğini belirtir. Buna göre verilerin silinmesi, düzeltilmesi ve yok edilmesi gibi işlemleri, veri sahibi olarak bireyler yönetebilmelidir.

Bu konudaki temel düzenleme Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'tir. Bu yönetmelik kapsamında kişisel sağlık verilerinin silinmesi (Md.8), verilerin yok edilmesi (Md.9) ve verilerin anonim hale getirilmesi (Md.10) konuları düzenlenmektedir. Yönetmelik bu konulara ilişkin olarak veri sorumlusuna önemli yükümlülükler vermektedir. Yönetmeliğin 12. maddesi, ilgili kişinin talep etmesi durumunda kişisel verinin silinmesi ve yok edilmesi hakkındaki süreleri düzenlemektedir. Bu maddeye göre kişisel verileri işleme şartlarının tamamı ortadan kalkmışsa, veri sorumlusu kişisel verileri silebilir, yok edebilir veya anonim hale getirebilir. Yanı sıra veri sorumlusu ilgili kişinin talebini en geç otuz gün içinde sonuçlandırmak durumundadır. Yönetmeliğin bu maddelerine göre verinin yönetiminde birey için oldukça önemli olsa da bireyi pasif kılmaktadır. Türkiye'deki uygulamaya göre örneğin kişinin kendi verisini silebilmesi için veri sorumlusuna başvuru yapması gerekmektedir. Bu durum veri işleyen birçok kurum ve kuruluş için bazı açılardan gerekli görülen bir uygulamadır. Ancak söz konusu sağlık verisi olduğundan, ulusal kişisel sağlık kaydı uygulamasının yönetimi konusunda farklı bir yaklaşım olması gerekir. Buna göre kişi, e-Nabız kaydından verilerinin silinmesi veya yok edilebilmesi için veri sorumlusu olarak Sağlık Bakanlığı'na başvuru yapmadan

istediği işlemleri yapabilmelidir. Birey aktif olarak kendi verisinin yönetimine katılabilmelidir. Bunun için verilerin bireyin kendisinde tutulması ve kendi verileri üzerindeki denetim ve kontrolüne izin veren politikalar oluşturulması önemli görünmektedir.

5.1.5.2.Kişisel sağlık kaydı uygulaması e-Nabız, özerklik ilkesi ile uyumlu olmalı

İdeal bir kişisel sağlık kaydı uygulamasının nasıl olması gerektiği sorgulandığında, ilk olarak uygulamanın en önemli özelliğinin birey tarafından yönetilmesine izin vermesi ve bu bağlamda özerklik ilkesi ile uyumlu olması gerektiği belirtilebilir. Kişisel sağlık verilerinin korunmasını sağlayacak en iyi yöntem bütün sağlık kayıtlarının kişinin kendisinde toplandığı ve bu kayıtlara ancak hasta izin verdiğinde erişim sağlanabildiği yöntemdir.

Kişisel sağlık kaydı uygulaması açısından özerklik ilkesine göre her birey kendi profiline ve veri denetleyicisinin kendileri hakkında sahip olduğu tüm bilgilere erişimi olmalıdır. Bununla birlikte uygulama üzerinde kullanıcı profili oluşturma veya karar verme için temel olarak hangi algoritmaların kullanıldığı bilgisine erişimi olmalı, bireyler, verilerin kullanımı hakkında bilgi talep edebilmeli, bunlarla ilgili hata veya eksikliklerin düzeltilmesini isteyebilmeli, istediğinde uygulamayı devre dışı bırakabilmeli ve tanımlanabilir verilerini silebilmelidir.

Özetle kişisel bir sağlık kaydı uygulaması için programın yönetimi kullanıcının kendisinde olmalıdır. Bu özelliklere göre e-Nabız incelendiğinde, uygulamanın özerklik ilkesi ile yeterince uyumlu olmadığı belirtilebilir. Bunun en temel nedeni, kişisel sağlık kaydı uygulamasında toplanan bilgiler, kişinin izni olmadan Sağlık Bakanlığı tarafından "hizmet" için kullanılabilmesidir. Dolayısıyla özerklik ilkesine aykırı olarak Türkiye'de kişisel sağlık verileri kişinin kendisinde değil, ilgili Bakanlığın merkezi veri toplama sisteminde depolanmaktadır.

E-Nabız sisteminin özellikleri açısından özerklik ilkesi ile uyumluluğu incelendiğinde, profil oluşturma (kayıt olmak), yeni kişisel bilgiler ekleyebilmek, hangi bilgilerin bulunduğu bilgisine erişim ve bilgilerin düzeltilmesini isteyebilmek gibi konularda bireyin kontrolüne izin vermektedir. Özerklik ilkesi açısından uygulamanın zayıf yönleri ise profil oluşturma veya karar verme için temel olarak hangi algoritmaların

kullanıldığı bilgisi ve kayıtlı sağlık verilerini silebilme özelliği bulunmamaktadır. Bir haber kaynağına göre e-Nabız üzerinden tanı silinebilmesinin mümkün hale getirildiği belirtilmektedir (Gürel, 2020). Uygulama buna göre incelendiğinde, uygulama üzerinde tanı silme işlemi yapılamadığı, "hastane ziyaretlerim" butonuna tıklandıktan sonra kurum bilgilerinin "profilimde görünmesin" seçeneğinin seçilmesi ile kurum bilgilerinin akışta gizlenebildiği saptanmıştır. Bu özelliğin özerklik ilkesi ile uyumlu olduğu söylenemez. Daha çok gizlilik ile ilgili olduğu belirtilebilir. Uygulamanın özerk olabilmesi için "silme" işlemine izin vermelidir. Özellikle kayıtlı bilgiler kişinin çalışma hayatını, özel yaşamını olumsuz yönde etkiliyor, kişinin damgalanması, ayrımcılığa uğraması gibi söz konusu mağduriyetler yaşayabilmesine sebep olabilecek türde ise kişinin kendisine ait sağlık kaydı sisteminden bu bilgileri silebilme hakkı olmalıdır. Aksi durumda kullanıcının özerk kararından söz edilemez.

Aydınlatma kapsamında "ret" hakkı da kullanılabilmelidir

Kişisel sağlık verileriyle ilgili özerklik sorunu, aydınlatılmış onam alınmasıyla çözümlenebilmektedir. Özerklik ilkesi ile uyumlu bir veri kayıt sistemi için Aydınlatılmış onamın geçerliliği de oldukça önemlidir.

E-Nabız uygulamasının Aydınlatma metni bilgilendirme açısından oldukça yetersiz bulunmuştur. Bununla birlikte e-Nabız kaydı için tek bir *–tık* ile alınan toplu onamın geçerliliğini sorgulamak gerekir. Bu şekilde alınan bir onam daha önce de belirtildiği üzere, onam değil rızadır. Çünkü belli bir hizmeti alabilmek için e-Nabız uygulamasını kullanmak isteyen kullanıcılar, doğru bir şekilde bilgilendirilmeden ve verilen bilgileri tam olarak anlamadan "okudum, anladım" seçeneğini işaretlemektedir. Dolayısıyla bu şekilde alınan aydınlatılmış onamlar, "onam" değil "rıza"dır ve bu şekilde alınan rızalar ile kişilik haklarının korunduğu savunulamaz.

Bir kişisel sağlık kaydı uygulaması kapsamında kişinin doğru bir şekilde bilgilendirilmesi ve verilen bilgileri anlaması nasıl sağlanabilir? Nasıl bir yöntem izlenirse aydınlatılmış onam uygun bir şekilde alınmış olur? Bu soruların yanıtı için ilk olarak verilen bilgilerin yeterli olup olmadığının yanıtlanması gerekmektedir. E-Nabız'ın Aydınlatma metni incelendiğinde, yukarıda belirtilen sebeplerle yeterli bir bilgilendirmenin söz konusu olmadığı ileri sürülebilir. İkinci olarak bilgilerin anlaşılır

olup olmadığını sorgulamak gerekir. E-Nabız uygulamasının Aydınlatma metni, okunduğu şekliyle anlaşılır bir metin olduğu söylenebilir. Üçüncü olarak "gerekli bilgilendirmenin yapılmasının ardından kişi ret olanağını kullanabiliyor mu?" sorusunu yanıtlamak gerekir. Aydınlatılmış onam kapsamında kişinin bir seçim yapmasına izin verilmelidir. Uygulamanın aydınlatma metninde bu olanağın kullanılabileceğine dair herhangi bir bilgilendirme yapılmamaktadır. İşlenen her bir veri için onamın ayrı ayrı alınması, geçerli bir aydınlatılmış onam için ilk adımlardan biri olabilir. Böylece kişi bazı kişisel verilerinin işlenmesine izin verirken, bazı verilerinin işlenmesine izin vermeyebilir. Dolayısıyla kişinin ret olanağını kullanabilmesine izin verilmiş olur. Clemens'e göre bireyler süreç ve riskler hakkında bilgilendirilmedikçe, bilgilendirmeyi anlamadıkça ve bilgilerinin paylaşılmasına izin vermekten "vazgeçmek" için aktif adımlar atamadıkça, mahremiyetleri ihlal edilecektir (Clemens, 2012). Dolayısıyla e-Nabız, özerklik ilkesine aykırı olarak veri işlenmesine izin vererek mahremiyeti ihlal etmektedir.

5.1.5.3.Karar verme yeterliği olmayan bireylerin verileri

Özerklik açısından tartışmalı bir diğer sorun, karar verme yeterliliği olmayan kişilerin verilerinin işlenmesi ve kullanılması konusundadır. Çocukların, psikiyatrik ya da nörolojik hastalara sahip kişilerin, geçici olarak bilincini yitirenlerin veya komada olan kişilerin karar verme yeterlikleri bulunmamaktadır. Genellikle bu kişilerin yerine eş, yetişkin kişi, anne-baba ve kardeş gibi başka birilerinin karar vermesi gerekmektedir.

Karar verme yeterliğine sahip olmayan kişiler için Hasta Hakları Yönetmeliği'nde (1998) "Sağlık Durumu ile İlgili Bilgi Alma Hakkı"na yönelik haklar düzenlenmektedir. Buna göre yönetmeliğin 16. maddesi "Kayıtları İnceleme Madde 16- Hasta, sağlık durumu ile ilgili bilgiler bulunan dosyayı ve kayıtları, doğrudan veya vekili veya kanuni temsilcisi vasıtası ile inceleyebilir ve bir suretini alabilir. Bu kayıtlar, sadece hastanın tedavisi ile doğrudan ilgili olanlar tarafından görülebilir." biçimindedir. Tıp etiği açısından yönetmeliğin bu maddesi oldukça yol göstericidir. Dolayısıyla yönetmeliğin bu maddesine göre "karar verme yeterliliği olmayan kişilerin yasal temsilcisi yoksa kişisel verilerinin işlenmesi konusunda aydınlatılmış onam gerekliliği var mıdır" sorusu yanıtlanabilir. Karar verme yeterliliğine sahip olmayan

kişilerin de olanaklar elverdiğince verileri hakkındaki görüşlerini öğrenmek önemlidir. Yasal temsilci yoksa kişinin mahremiyetine zarar vermeyecek düzeydeki verileri kimliksizleştirilerek işlenebilir. Ancak damgalanmaya sebep olabilecek düzeydeki çok hassas olan bilgiler için kişiden ve yasal temsilciden onam alınamıyorsa, hekimin bu verileri işlememesi daha makul bir yaklaşımdır.

Ayrıca hekim, yasal temsilciden aydınlatılmış onam almak için kişisel verilerin işlenmesi süreci ile ilgili gerekli olan bilgileri, yasal temsilciye vermelidir. Özellikle psikiyatrik ya da nörolojik hastalıklara sahip kişiler için önceliği hastanın kendi isteğine vermelidir. Çünkü bu kişiler yaşamlarının bazı dönemlerinde karar verme yeterliliklerine sahip olmuşlardır. Bu nedenle onlar adına karar verirken, dikkatli olunması gerekir.

Karar verme yeterliliği bulunmadığı kabul edilen çocuklar için daha farklı bir yol izlenebilir. Örneğin 16 yaşında bir çocuğa gerekli bilgilendirme yapılarak çocuğun anlaması sağlanabilir. Dolayısıyla çocukların yaşları ve özel çocuk olup olmama durumları dikkate alınarak kendi kaderlerini tayin hakkı hekim tarafından dikkate alınmalıdır.

5.1.6. Mahremiyet ve gizlilik ilkesi açısından

Sağlıkta dijitalleşmenin arttığı günümüz dünyasında mahremiyet daha fazla tartışılmaya başlanmıştır. Çünkü sağlıkta Büyük Veri'nin önemli yararları karşısında dijitalleşen sağlık alanında mahremiyet ve gizliliği korumak oldukça güçtür. Bununla birlikte sistemler doğru çalışırken bile sağlık alanında hasta mahremiyeti oldukça önemli bir sorundur.

Günümüzde Büyük Veri analiz yöntemlerinin gelişimi ile birlikte bireyin kişisel verileri üzerindeki kontrolü azalırken kişisel veriye erişimlerin bir sonucu olarak mahremiyetleri de sürekli olarak tehdit altındadır. Kişisel sağlık verilerinin internet ortamına aktarılması nedeniyle dünyada ve Türkiye'de mahremiyetin ihlaline yönelik birçok örnek bulunmaktadır. Cambridge Analytica davası, Edward Snowden'in ifşaları ve Türkiye'deki örnekler mahremiyete ilişkin sorunların boyutunu göstermektedir. Sağlık verisinin elektronik veri tabanları aracılığı ile işlenmesi ve saklanması, mahremiyete ve özel hayata ilişkin ihlaller yaşanması yönündeki kaygıları

artırmaktadır. Bir çalışma 2014 ve 2017 yılları arasında medyada yer alan haberler üzerinden sağlık verilerinin gizliliği konusundaki riskleri araştırmıştır (Eke, Çelik & Çetin, 2018). Buna göre HIV test sonuçları ve kürtaj bilgileri gibi çok hassas verilerin yayınlanması, bazı hastanelere yapılan siber saldırılar, kalp pillerinin uzaktan kumanda edilebilmesi, sağlık sigortası şirketlerinin siber saldırıya uğraması ve verilerin satılması gibi çeşitli örnekler bulunmuştur. Araştırmanın diğer çarpıcı bulguları arasında Amerika'da 5,6 milyon kişinin sosyal güvenlik numaraları, isimleri, adresleri, finansal ve sağlık bilgilerinin çalınması örneği vardır. İngiltere ise NHS'ye bağlı 16 sağlık kurumunun etkilendiği siber saldırı sonrasında NHS sağlık bilgi işlem ağının tamamen çökmesi ve Türkiye'nin de içinde bulunduğu 74 ülkenin 57 binden fazla bilgisayarı etkilediği belirtilmektedir (Eke ve ark., 2018). Bir başka örnek Miami Hacker Halted konferansında diyabet hastalarına ölümcül dozlar vermek için insülin pompalarının nasıl hacklenebileceği ve implante edilebilir kalp cihazlarından ve kalp pillerinden gelen tıbbi bilgilerin nasıl engellenebildiği, bu cihazların nasıl kapatılabildiği ve hayati tehlike içeren elektrik şoklar verilebildiği gösterilmiştir (Goodin, 2011). Bu örnekler, sağlık alanındaki mahremiyetin ihlaline yönelik risklerin büyüklüğünü ortaya koymaktadır. Mahremiyetin korunması ile ilgili dünyadaki genel yaklaşım, HIPAA (Sağlık Sigortası Taşınabilirliği ve Sorumluluk Talimatı) gereği, kimliksizleştirilmiş verilerin üçüncü taraflara paylaşımı kabul görmektedir (Hoffman & Podgurski, 2012). Ancak bu kuralda sağlık bilgilerinin tedavi, sağlık sigortası ödemesi veya sağlık hizmetleri amacıyla iletilmedikçe, hastanın onamının gerekli olduğu vurgulanmaktadır (Hoffman & Podgurski, 2012).

Büyük Veri analizinde mahremiyeti teknik olarak korumanın yolu anonimleştirme ilkesinden geçtiği beliritlebilir. Ancak Büyük Veri analizlerinde, bilginin miktarı ve çeşitliliği göz önüne alındığında kimliğin yeniden tespiti mümkündür (Mayer-Schönberger & Cukier, 2013). Bu durum anonimleştirmenin yeterli olmadığını göstermektedir. Clemens, hasta bilgilerini tamamen güvenli tutma yeteneğine sahip olunmadıkça, hassas sağlık bilgilerinin işlenmemesi gerektiğini savunmaktadır (Clemens, 2012). Bu durumda kişisel sağlık verilerinin işlenmesini etik açısından haklı çıkarılabilecek bir yaklaşımı belirlemeye çalışırken, veri işleme sürecinde mahremiyet ve gizliliğin korunması için gerekli koşulların baştan oluşturulması ve risklerin olabildiğince bertaraf edilmesi gerektiği yaklaşımının benimsenmesi gerektiği ileri

sürülebilir. Teorik olarak kişilik haklarını koruyarak veri işlemek mümkün ise bu durumda veri işleme süreci iyi bir şekilde yapılandırılması gerekmektedir.

Tez kapsamında bu ilke, veri işleme süreci tamamlandıktan sonra hassas verinin güvenliğinin sağlanması için nasıl bir süreç izlenmesi gerektiğinin çerçevesini çizmektedir. Buna göre verilerin işlenmesi için minimum veri ilkesi gözetilmeli ve anonimleştirme yapılarak sağlık verileri toplanmalıdır. Bilgiye yalnızca yetkili kişiler onam alarak erişim sağlamalı ve bilgilerin üçüncü taraflarla paylaşılmayacağı güvence altına alınmalıdır. Toplanan tüm veriler kayıp, bozulma, imha, kullanım, değiştirme veya ifşaya karşı korunmalıdır. Veri kayıt sistemlerinde şifreleme olmalı ve veri sızıntılarına yönelik siber güvenlik önlemleri alınmalı ve bağımsız firmalar aracılığı ile veri sızıntı denetlemeleri düzenli olarak gerçekleştirilmelidir.

Tez kapsamında tanımlanan bu ilkeye göre ayrıca çeşitli amaçlarla verilerin üçüncü taraflarla paylaşımı, verilere uygun olmayan şekilde erişilmesi ve uygulama alanında hassas verinin kötüye kullanımı konuları karşısında ilgili düzenleme maddelerinin bu ilke ile uyumlu olup olmadığı bu başlık altında ele alınmıştır. Bu bağlamda ilgili düzenleme maddelerinin, mahremiyet ve gizlilik ile ilgili haklar ve yükümlülükler açısından ne tür güvenceler sağladığı, verilerin güvenliği, verilerin çeşitli yollarla ifşa edilmesini önleyen teknik önlemler ve uygulanacak prosedürlerin neler olduğu ilgili düzenlemelerde incelenerek değerlendirilmiştir. Özellikle KVK Kanunu, KSV Yönetmeliği, GSS Verilerinin Güvenliği ve Paylaşımına İlişkin Yönetmelik ve Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik'in bu ilke kapsamında değerlendirmek önemli görünmektedir.

Mesleki gizlilik, sağlık çalışanlarının hasta bilgileriyle ilgili gizliliği korumaları ve hasta izni olmadan verileri açıklamamaları ilkesini ifade eder. Büyük sağlık verileri bağlamında mahremiyet ve gizlilik, sağlık verilerinin toplanması, saklanması ve kullanılması anlamında verilerin gizliliğini ifade etmektedir. Dolayısıyla mahremiyet, bilginin kim tarafından ve hangi koşullar altında elde edilip edilemeyeceği ve kullanılıp kullanılamayacağı ile ilgilidir (Hoffman & Podgurski, 2012). Bu bağlamda sağlık verilerinin işlendiği veri kayıt sistemlerinin bu ilke ile uyumluluğunu sorgulamak gerekir. Sağlık verilerini işleyen hekimler hangi durumlarda verileri paylaşabilir, mevzuata aykırı bir durum söz konusu olduğunda hekim sağlık verilerini

paylaşmalı mıdır, hekim hangi sağlık verilerini paylaşmalıdır soruları ilgili düzenlemeler veri kayıt sistemleri değerlendirildikten sonra tezin bu bölümünde yanıtlanmaya çalışılmıştır.

5.1.6.1.İlgili düzenlemeler mahremiyet ve gizlilik ilkesiyle uyumlu olmalı

İlgili metinlerde "veri güvenliği" teorik olarak sağlanmaktadır; temel düzenlemelerin KVK Kurulu'nun çıkarmış olduğu bir rehbere atıf yapması yeterli değildir

Mahremiyet ve gizlilik ilkesinin korunmasının en önemli koşulu veri güvenliğinin sağlanmasıdır. Veri güvenliği, gizliliğin sağlanabilmesi için daha çok teknik tedbirleri ifade etmektedir. Verinin işlenmesi sürecinin en başından itibaren mahremiyet ve gizliliğin korunmasına yönelik kurallar ilgili kanun ve yönetmeliklerde açık ve belirli olmalıdır.

Buna göre KVK Kanunu (Md.12), KSV Yönetmeliği (Md.17) ve GSS Verilerinin Güvenliğine İlişkin Yönetmelik'te (Md.6) veri güvenliğinden söz edilmekte ve bu bağlamda veri sorumlusunun yükümlülüklerine yer verilmektedir. KSV Yönetmeliği'nin 17. maddesinde açık sağlık verisi tanımlanmış, "şeffaflık" ve "hesap verebilirlik" korunarak veri güvenliğinin artırılması hedeflenmiştir. Genel sağlık sigortası verilerinin güvenliği ve paylaşımı, GSS Verilerinin Güvenliğine İlişkin Yönetmelik ile düzenlenmektedir. Yönetmeliğin ikinci bölümünde Sağlık Verilerinin Güvenliği düzenlenmektedir. Bu bölümde kişisel ve ticari sır niteliğindeki verilerin korunması, kurum veri tabanında yer alan bilgilerin güvenliğinin sağlanması, sağlık hizmet sunucularında kaydı tutulan verilerin güvenliğinin sağlanması, veri üreten birimin sorumluluğu ve alıcının sorumluluğuna ilişkin olarak sağlık verilerinin gizliliğini sağlamaya yönelik tedbirlere yer verilmektedir. Yönetmeliğin 10. maddesi paylaşılmayacak verileri düzenlemektedir (2012);

> "Paylaşılmayacak veriler MADDE 10 – … (2) Aşağıda yer alan bilgiler paylaşılmaz: a) Paylaşılması ulusal güvenliği tehdit edebilecek nitelikte olan bilgiler, b) Milli İstihbarat Teşkilatı Müsteşarlığı personeli ile bakmakla yükümlü oldukları kişilere ait her türlü veriler, c) Genel sağlık sigortalısına ait kişisel bilgileri içeren veriler, ç) Rekabet hukuku ilkelerine aykırılık teşkil eden firma, ürün, marka ve ilgili diğer bilgileri içeren veriler. (3) Sağlık hizmet

sunucularına ait veriler, ancak kurum adı belirtilmeden, doğrudan veya dolaylı tanımlamaya yol açmayacak şekilde bölge veya alan adı olarak verilebilir."

Bu maddenin c fıkrası, kişisel bilgilerin paylaşılmamasını özel olarak belirtmiştir.

Veri güvenliğini kapsamlı bir şekilde KVK Kurumu ele almaktadır. Kurumun çıkarmış olduğu Kişisel Veri Güvenliği Rehberi'nde, gizliliğin sağlanabilmesi için idari ve teknik tedbir yöntemleri açıklanmaktadır. Rehber ilk olarak, veri güvenliğine ilişkin "güvenli giriş katmanı (SLS), ilgili kişi, imha, kanun, kayıt ortamı, kişisel veri saklama ve imha politikası, veri kaybı/sızıntısı önleme (DLP) ve veri kayıt sistemi" kavramlarını tanımlamaktadır (Kişisel Verileri Koruma Kurumu, 2018a). Rehberin birinci bölümünde idari tedbirlere konu olarak, mevcut risklerin belirlenmesi, belirlenen risklerin gerçekleşme olasılıkları ve gerçekleşmesi durumunda yol açacağı kayıpların belirlenmesiyle alınabilecek tedbirlere vurgu yapmaktadır. Riskler belirlenirken "kişisel verilerin özel nitelikli olup olmadığı, önemi gereği hangi derecede gizlilik seviyesi gerektirdiği, güvenlik ihlali halinde ilgili kişi bakımından ortaya çıkabilecek zararın niteliği ve niceliği" nin dikkate alınması gerektiği gibi konular üzerinde durulmaktadır. Bu bölümde ayrıca kişisel veri güvenliğini zedeleyecek saldırılar ile siber güvenliğe ilişkin sınırlı bilgileri olabilecek olan çalışanların ilk müdahaleyi yapabilmeleri için çalışanlara eğitim verilmesi ve farkındalık kazandırılmasına vurgu yapılmaktadır. Rehberde, veriye erişim hakkı verilen çalışanlar için "Yasaklanmadıkça Her Şey Serbesttir" yerine, "İzin Verilmedikçe Her Şey Yasaktır" prensibine uygun hareket etmeleri belirtilmektedir. Rehberin ikinci bölümünde siber güvenliğin sağlanması, kişisel veri güvenliğinin takibi, kişisel veri içeren ortamların güvenliğinin sağlanması, kişisel verilerin bulutta depolanması, bilgi teknolojileri sistemlerinin tedariği, geliştirme ve bakımı ve son olarak kişisel verilerin yedeklenmesi konuları üzerinde durulmaktadır. Rehberin veri güvenliğini sağlamaya yönelik idari ve teknik yöntem önerileri ile oldukça yol gösterici olduğu belirtilebilir. Bu rehberde belirtilen tedbirler alındığında gizliliğe yönelik risklerin minimize edilebileceği belirtilebilir.

Bununla birlikte kişisel sağlık verisinin korunması yönündeki KVK Kanunu başta olmak üzere KSV Yönetmeliği, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik gibi temel düzenlemelerin, Kurul'un

çıkarmış olduğu bu rehbere atıf yapması yeterli değildir. Çünkü bu düzenlemeler, konuyla ilgili temel düzenlemeler ve rehberin yasal bir bağlayıcılığı bulunmamaktadır. Buna göre düzenleme metinlerinde veri güvenliğine yönelik uyulması gereken temel kurallar yer almalıdır. Veri güvenliğinin teminat altına alınması için başta KVK Kanunu olmak üzere veri güvenliğinin nasıl sağlanacağına ilişkin uygulamayı gösterir yönetmeliklerin düzenlenmesi esas olmalı, güvenliği sağlamak üzere çıkarılacak kurallar ise denetlenebilir olmalıdır. Dolayısıyla rehberde belirtilen tedbirlerin, temel düzenleme metinlerinde yer almasıyla gizliliğe yönelik risklerin minimize edilebileceği vurgulanabilir.

Yoruma açık ve belirsiz ifadeler, güvence yerine hak ihlaline neden olabilir

Kişisel sağlık bilgilerinin mahremiyetinin ve gizliliğinin korunması sağlık alanındaki önemli düzenlemelerden biri olan Hasta Hakları Yönetmeliği'nde çok açık bir şekilde düzenlenmiştir. Buna göre yönetmeliğin 21. maddesi mahremiyete saygı gösterilmesi hakkını ve 23. maddesi kişilik haklarının korunmasını düzenlemektedir (Hasta Hakları Yönetmeliği, 1998);

> "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. Eğitim verilen sağlık kurum ve kuruluşlarında, hastanın tedavisi ile doğrudan ilgili olmayanların tıbbi müdahale sırasında bulunması gerekli ise; önceden veya tedavi sırasında bunun için hastanın ayrıca rızası alınır.
>
> Bilgilerin Gizli Tutulması Madde 23- Sağlık hizmetinin verilmesi sebebiyle edinilen bilgiler, kanun ile müsaade edilen haller dışında, hiçbir şekilde açıklanamaz. Kişinin rızasına dayansa bile, kişilik haklarından bütünüyle vazgeçilmesi, bu hakların başkalarına devri veya aşırı şekilde sınırlanması neticesini doğuran hallerde bilginin açıklanması, bunları açıklayanın hukuki

> sorumluluğunu kaldırmaz. Hukuki ve ahlaki yönden geçerli ve haklı bir sebebe dayanmaksızın hastaya zarar verme ihtimali bulunan bilginin ifşa edilmesi, personelin ve diğer kimselerin hukuki ve cezai sorumluluğunu da gerektirir. Araştırma ve eğitim amacı ile yapılan faaliyetlerde de hastanın kimlik bilgileri, rızası olmaksızın açıklanamaz."

Dolayısıyla halihazırda Hasta Hakları Yönetmeliği, hasta mahremiyeti ve elde edilen kişisel sağlık verilerinin güvenliği yönünden mahremiyet ve gizliliği açık ve net bir şekilde koruyan bir düzenlemedir. Bu konudaki temel düzenleme maddeleri de mahremiyetin korunabilmesi için Hasta Hakları Yönetmeliği'nin bu iki maddesi ile uyumlu olmalıdır.

Bunun yanı sıra daha önce belirtildiği üzere KVK Kanunu, KSV Yönetmeliği ve Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'te saptanan belirsiz ifadeler daha açık olmalıdır. KVK Kanunu kişisel verilerin korunması hakkını düzenleyen en temel düzenleme olması nedeniyle bu hakkın korunabilmesi için ilgili maddelerinde yoruma açık, esnek ve belirsiz ifadelere yer verilmemelidir. Buna göre incelenen Kanunun 28. maddesinin birinci fıkrasının (b) ve (c) bendlerinin belirsiz ve yoruma açık olduğu belirtilebilir. Buna göre;

> "… kişisel verilerin resmi istatistik ile anonim hâle getirilmek suretiyle araştırma, planlama ve istatistik gibi amaçlarla işlenmesi…
>
> … 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…"

Bu ifadelere göre örneğin biyometrik veri işlenebilir anlamı çıkarılabilir. Çünkü biyometrik veri doğrudan kamu güvenliği ile ilişkilendirilebilmektedir. Bu ilişkinin kurulmaması ve verinin işlenebilir olması için açık bir şekilde haklı çıkarılabilir bir gerekçenin varlığına işaret edilmesi daha yerinde bir yaklaşımdır. Böylece özel hayatın gizliliğinin korunması için bir güvence oluşturulabilir. Bu kanun maddesinde bu ifadelerin muğlak kaldığını ve özellikle sağlık verilerine işaret edilmediğini vurgulamak gerekir. Kişisel veriyi koruyan bir kanun kapsamında verinin işlendikten sonra kötüye kullanım ve yetkisiz erişim risklerine karşı daha açık ifadeler bulunmalıdır. Verinin işlenmesi ile doğabilecek riskler karşısında bu ifadelerin sağlık

bilgileri açısından oldukça esnek olduğu vurgulanabilir. Bilgilerin hangi kurum veya kuruluşlar tarafından işlenebileceği, hangi verilerin nasıl işlenebileceği ve verinin işlenme sırasında anonim şekilde işlenip işlenmeyeceği gibi sorular açısından daha açık olması gerekir. Kanunun bu maddesinin bu haliyle, bireyi kamu otoritelerinin keyfi uygulamalarına karşı savunmasız bıraktığı yorumu yapılabilir.

Bir başka sorun kişisel sağlık verilerinin ekonomik değerinden kaynaklı olarak ticari amaçlarla kullanılabilmesidir. Kişisel sağlık verilerinin ekonomik değeri ön plana çıkarılmamalı, kişilerin onamı dahilinde ve anonim bir şekilde dahi olsa sağlık verileri bu değer üzerinden tanımlanmamalıdır.

Kavramsal açıdan belirli olmayan bir başka düzenleme Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'tir. Bu yönetmelikte "anonimleştirmenin" farklı şekillerde tanımlanması ve içerikle uyumlu olmayan bir tanımın yapılması (Bkz. s.222), bu kavramı yoruma açık hale getirmektedir. Özellikle düzenleme maddelerinde açıklanması gerekli olan tanımların yan anlamları kullanılmamalıdır. Bu yönetmelik kapsamında tanımlanan anonim, anonimleştirme, kimliksizleştirme ve maskeleme gibi kavramlar açık ve net bir şekilde tanımlanmalı, yoruma dayalı olmamalıdır. Tanımlanan kavram bir yöntem içeriyorsa, bu yönteme ilişkin standart olabilecek güvenilir yazılım veya programlar açıklanmalıdır. Yönteme ilişkin halihazırda kullanılmakta olan yazılım veya programlar belirtilmeli, bağımsız kullanıcılar tarafından denetlenebileceği açıklanmalıdır.

Özetle belirsiz, yoruma dayalı veya açık uçlu ifadelerin mahremiyet ve gizlilik yönünden güvence sağlamayacağı ve riskin kendisini doğuracağı vurgulanabilir. Temel düzenlemelerin somut, objektif ve denetlenebilir kurallar içermemesi durumunda yasalardaki esnekliklerin kullanılması söz konusu olabilir.

Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arşiv Hizmetleri Yönergesinde Değişiklik Yapılmasına Dair Yönerge, içerik açısından KSV Yönetmeliğine göre daha somut ve açıktır

Mahremiyet ve gizlilik ilkesi açısından incelenen Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arşiv Hizmetleri Yönergesinde Değişiklik Yapılmasına Dair Yönergenin

KSV Yönetmeliği'ne kıyasla daha ileri düzeyde bir içeriğe sahip olduğu saptanmıştır. Yönerge özellikle sağlık verilerinin güvenliği ve gizlilik konusunda kurumlara düşen yükümlülükleri belirtmesi açısından KSV Yönetmeliği'nden oldukça ileri düzeyde bir içeriğe sahip, daha sistemli ve kuralları daha açıktır.

Buna göre Yönergede (2007) bütün kişisel ve kurumsal bilgilerin (klinik, idari, mâli vb.) güvenliğinin sağlanması için şu genel kurallara yer verilmektedir:

- Veri güvenliği konusunda üç temel prensibin göz önünde bulundurulması gerekmektedir. Bunlar; 'gizlilik', 'bütünlük' ve 'erişilebilirlik'tir.
- Kurumda kimin hangi yetkilerle, hangi verilere ulaşacağı tanımlanmalıdır. Rol bazlı yetkilendirme yapılmalıdır ve yetkisiz kişilerin hastanın sağlık kayıtlarına erişmesi mümkün olmamalıdır.
- Sağlık kayıt bilgileri hastaya aittir. Yetkilendirilmiş çalışanlar ancak kendisine kayıtlı olan hastaların sağlık kayıtlarına erişebilmelidir. Ancak hastanın yazılı onayı ile diğer sağlık çalışanları bu veriye erişebilir.
- Hasta taburcu olmuş ise hiçbir kurum çalışanı hastanın sağlık kayıtlarına erişemez.
- Hastanın rızası olmadan hiçbir çalışan sözle de olsa hasta sağlık bilgilerini hastanın yakınları dışında üçüncü şahıslara ve kurumlara iletemez.
- Hasta sağlık bilgileri ticari amaçlı olarak üçüncü şahıslara iletilemez. Hastanın kullandığı ilaçlar, diyet programları vs. buna dahildir.
- Hasta dosyasının bir kopyası hastaya teslim edilmelidir. İlgili mevzuat hükümleri saklı olmak kaydıyla hiçbir hasta kaydı, elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilmemelidir.
- Hastanın dosyasının izlenmemesi için gerekli tedbirler alınmalıdır. Hasta dosyalarının gelişi güzel ortada bırakılmaması, bilgisayar ekranının başkalarınca okunabilecek şekilde bırakılmaması gibi.
- Telefon ile konuşurken hasta ile mahrem bilgilerinin üçüncü şahısların eline geçmemesine azami özen gösterilmelidir.
- Bütün hasta, sağlık kayıtları fiziksel olarak korunmuş mekanlarda saklanmalıdır.
- Elektronik hasta kayıtlarına internet ortamında erişim mümkün olmamalıdır.
- Hasta sağlık bilgileri bilginin üretildiği kurum tarafından veya Bakanlığımızın Bilgi Yönetim sistemleri tarafından araştırma, istatistik ve Karar Destek Sistemleri

için kullanılabilir. Bu durumda hasta sağlık bilgisi hasta tanımlayıcısı ile ilişkilendirilemez.

Yönergenin birinci maddesinde, sağlık kurumlarında kullanılmakta olan veri tabanları ve/veya kullanılan uygulama yazılımları ara yüzlerindeki geçmiş kayıtlardaki kapanmış, onaylanmış ve sonuçlandırılmış işlemlere ait verilerde değiştirme, silme ve ekleme yapılamayacağı bildirilmektedir. Bununla birlikte yönerge idari önlemlerden daha çok teknik tedbirler konusunda önemli bilgilere yer vererek veri güvenliğine bağlı gizlilik ilkesini kapsamlı bir biçimde korumaya çalışmaktadır. Yönerge ayrıca, acil durum kapsamındaki olayları risk seviyelerine göre gruplandırarak, oluşan risk seviyesine göre alınacak tedbirleri ve gerekli işlemleri açıklamıştır. Dolayısıyla gizliliğin korunabilmesi için bu yönerge örnek alınabilecek bir düzenlemedir.

Mahremiyet ve Gizlilik ilkesi açısından Sağlık Bilgi Yönetim Sistemleri Hakkında Yönetmeliğin (2022) de ilgili maddelerini değerlendirmek gerekmektedir. Buna göre mahremiyet ve gizliliğe ilişkin önemli hükümleri bulunan yönetmeliğin, kişisel verilerin korunması yönünde çok daha somut açıklamaları bulunmaktadır. Buna karşın yönetmeliğin Gizlilik başlıklı 16. maddesinin üçüncü fıkrasında kişisel sağlık verilerinin muhafaza edileceği veri ortamlarının talep üzerine denetlenebileceği ve onaylanacağı belirtilmektedir. Kişisel sağlık verilerinin muhafaza edilebilme sürecindeki denetimler, kurumların talebine bırakılmamalı, düzenli olarak denetlenmelidir.

> "MADDE 16- (3) Kişisel sağlık verilerinin muhafaza edileceği veri ortamları, talep üzerine Genel Müdürlük tarafından kurulan bir komisyon marifeti ile uzaktan ya da yerinde denetlenir ve onaylanır. Veriler yalnızca yurt içinde ve güvenli bir şekilde muhafaza edilir."

Bununla birlikte bu maddeye göre, verilerin yalnızca yurt içinde muhafaza edileceği açıklanmaktadır. Kişisel sağlık verilerinin yurt içi ve yurt dışı muhafaza edilme süreçlerinde farklı riskler bulunmaktadır. Verilerin yurt içi muhafaza edilmesi, riskin tamamen ortadan kaldırmasa bile gizliliğe ilişkin risk düzeyini azalttığı ileri sürülebilir. Dolayısıyla bu ifadenin, kişisel sağlık verilerinin korunması yönündeki uygulamaların güçlendirilmesi açısından oldukça önemli olduğu vurgulanabilir.

Dijital dünyada gizliliği korumak çok güçtür ancak imkansız değildir. Bu nedenle veri güvenliğinin sağlanabilmesi için gerekli olan bütün önlemler alınmalıdır. Bu bağlamda özellikle sağlık veri kayıt sistemleri intranet çalışan sistemler olmalı ve bağımsız firmalar aracılığı ile veri sızıntı testleri yaptırma gereklilikleri, veri güvenliğini düzenleyen ilgili düzenleme maddelerinde yer almalıdır. Bunun yanı sıra kötüye kullanım riski açısından özellikle denetlenebilir kurallara ve yaptırımlara ilgili düzenlemelerde yer verilmelidir.

Temel düzenlemeler, 3. taraflarla veri paylaşımının önünü açmamalıdır

Mahremiyet açısından kişisel sağlık verileri üçüncü taraflarla paylaşılmamalıdır. Kişiden alınan onam, veri toplama amacını belirten bir kuruma yöneliktir. Dolayısıyla mahremiyet hakkının korunabilmesi ve kişinin özerkliğine saygı gösterilebilmesi için veri talep eden üçüncü taraflarla veriler paylaşılmamalıdır.

Temel düzenleme maddeleri incelendiğinde alıcı olarak tanımlanan kamu kurum ve kuruluşlar veya özel sektör kuruluşları ile gerçek veya tüzel kişilerin veri taleplerinin karşılanmasını belirten düzenleme maddeleri bulunmaktadır. Bununla birlikte verilerin yurt içi paylaşımı mümkün olduğu gibi yurt dışı paylaşımı da mümkündür. Buna göre yurt dışı aktarım, KVK Kanunu'nun 9. maddesinde şu şekilde düzenlenmektedir:

> "(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz. (2) Kişisel veriler, 5 inci maddenin ikinci fıkrası ile 6 ncı maddenin üçüncü fıkrasında belirtilen şartlardan birinin varlığı ve kişisel verinin aktarılacağı yabancı ülkede; a) Yeterli korumanın bulunması. b) Yeterli korumanın bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması, kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir. (3) Yeterli korumanın bulunduğu ülkeler Kurulca belirlenerek ilan edilir. (4) Kurul yabancı ülkede yeterli koruma bulunup bulunmadığına ve ikinci fıkranın (b) bendi uyarınca izin verilip verilmeyeceğine; a) Türkiye'nin taraf olduğu uluslararası sözleşmeleri, b) Kişisel veri talep eden ülke ile Türkiye arasında veri aktarımına ilişkin karşılıklılık durumunu, c) Her somut kişisel veri aktarımına ilişkin olarak, kişisel verinin niteliği ile işlenme amaç ve süresini, ç) Kişisel verinin aktarılacağı ülkenin konuyla ilgili mevzuatı ve uygulamasını, d) Kişisel verinin aktarılacağı ülkede bulunan veri sorumlusu tarafından taahhüt edilen önlemleri, değerlendirmek ve ihtiyaç duyması hâlinde, ilgili kurum ve kuruluşların görüşünü de almak suretiyle karar verir.

> (5) Kişisel veriler, uluslararası sözleşme hükümleri saklı kalmak üzere, Türkiye'nin veya ilgili kişinin menfaatinin ciddi bir şekilde zarar göreceği durumlarda, ancak ilgili kamu kurum veya kuruluşunun görüşü alınarak Kurulun izniyle yurt dışına aktarılabilir. (6) Kişisel verilerin yurt dışına aktarılmasına ilişkin diğer kanunlarda yer alan hükümler saklıdır."

Benzer biçimde KSV Yönetmeliği'nde de kişisel sağlık verilerinin yurtdışına aktarılabileceği düzenlenmektedir. Buna göre ilgili 15. madde şu şekildedir:

> "(1) Kişisel sağlık verilerinin yurtiçinde aktarımında Kanunun 8 inci maddesine, yurtdışına aktarımında ise Kanunun 9 uncu maddesine riayet edilir. (2) Kişisel sağlık verilerinin, Kanunun 8 inci maddesinin ikinci fıkrasının (b) bendi ile üçüncü fıkrası ve 28 inci maddesi kapsamında kamu kurum ve kuruluşlarına aktarılması için protokol düzenlenir. Düzenlenen protokolde, kişisel veri koruma mevzuatının genel ilkeleri ile veri güvenliğine ilişkin hükümlere ve protokol kapsamında hangi verilerin aktarılacağına yer verilir. Verilerin aktarımı, teknik altyapının uygun olması hâlinde KamuNET üzerinden gerçekleştirilir. (3) Kişisel sağlık verilerinin aktarımı talepleri, talep edilen sağlık verilerinin ilgili olduğu Bakanlık birimi tarafından Kanun ve ilgili diğer mevzuat açısından değerlendirilir, değerlendirme sonucuna göre Genel Müdürlükçe işlem tesis edilir."

Verilerin yurtdışı aktarımını düzenleyen bu iki madde, mahremiyetin korunabilmesi için yeterli düzeyde bir güvence sağlamamaktadır. Özellikle Kanunun ikinci fıkrasının a bendinde belirtilen "yeterli koruma" ifadesi açısından yeterli koruma düzeyini belirlemenin her zaman mümkün olmayacağını belirtmek gerekir. Aynı fıkranın b bendindeki ifadenin sonunda ise kişinin açık rızası aranmaksızın yurtdışına aktarılabileceğinin belirtilmesi mahremiyet hakkı açısından ihlal oluşturmaktadır. Mahremiyet ve gizlilik ilkesi açısından kanunun bu maddesinde yeterli önlemlerin neler olacağı belirtilmelidir. Bunun yanı sıra kişinin "açık rızası" dahilinde diğer bir ifade ile aydınlatılmış onamı alınarak aktarım yapılabileceği bildirilmelidir. Kişinin sağlık verilerinin yurt içi aktarımına izin verebileceği, ancak yurtdışı aktarıma izin vermeyebileceği seçeneğinin kullanılabilir olması hakkı, kanun kapsamında tanınmalıdır. Söz konusu yurtiçi paylaşım için de kişilerin ayrıca onamı alınmalıdır. Çünkü veri işleyen kurum açısından potansiyel riskler farklı olabilir. Örneğin Sosyal Güvenlik Kurumu Kanunu'nun 35. maddesinde bilgilerin kurumlar arası paylaşılabilmesi söz konusudur (Sosyal Güvenlik Kurumu Kanunu, 2006).

> "Kurum, kişisel sağlık verilerini kamu sağlığının korunması, koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım hizmetlerinin yürütülmesi, verilen sağlık hizmetlerinin uygunluğunun ve yerindeliğinin takibi ve finansmanının planlanması amacıyla talebi halinde Sağlık Bakanlığı ile paylaşır."

Bu ifade açısından şu sorular sorulabilir; kurum başka bir kurum ile veri paylaşımı gerçekleştireceği bir durumda hasta bilgilendiriliyor mu, hastanın ayrıca aydınlatılmış onamı alınıyor mu bilinmemektedir.

KVK Kanunu'nun 8. maddesi ise verilerin yurtiçi aktarımını düzenlemektedir. Söz konusu kanun, verilerin hem yurtiçi hem de yurtdışı paylaşımını bu şekilde düzenleyerek mahremiyet hakkının ihlaline yol açabilir. Kanun kapsamında mahremiyetin korunabilmesi için veri aktarımı yasak olmalı, mutlaka aktarılması gerekiyorsa sağlam bir biçimde gerekçelendirilmeli ve kişilerin onamına bağlı olarak aktarılmasına izin verilmelidir. Aktarılacak sağlık verileri için özellikle aydınlatılmış onam bir gereklilik olarak ilgili kanun ve yönetmelikte belirtilmelidir.

Verilerin anonimleştirilmesi, mahremiyet ve gizliliğin korunabilmesi için yeterli değildir

Sağlık verilerinin mahremiyetinin korunabilmesi için başvurulan yöntem, verileri anonim hale getirmektir. Verinin anonimleştirilmiş veri niteliği kazanabilmesi için kişiyle hiçbir şekilde ilişkilendirilmemesi gerekir.

Sağlık verilerinin anonimleştirilmiş bir şekilde istatistiki çalışmalar için kullanılabilir olmasında herhangi bir etik sorun bulunmamaktadır. Ancak anonimleştirme kavramına ilişkin ilgili düzenlemelerde saptanan belirsizlikler ve beraberinde anonimleştirmenin teknik olarak geçersiz olabilmesi, sağlık verilerinin mahremiyetinin korunabilmesi için yeterli bir yöntem olmadığını göstermektedir. Daha açık bir şekilde ifade edilecek olursa teknik olarak sadece doğum tarihi ve posta kodu bilgilerinin bilindiği tıbbi kayıtlarla dahi kişiler tek tek saptanabilmektedir (KSV Çalışma Grubu). Bu durum özellikle Büyük Veri yöntemleri ve beraberinde yapay zekanın gelişimi ile birlikte düşünüldüğünde bu yöntemin mahremiyeti korumak için etkili olmadığını, aksine riskin kendisini yarattığını vurgulamak gerekir. Dolayısıyla kişisel sağlık verilerini

koruyan kanun ve yönetmeliklerin, Büyük Veri analiz yöntemleri ve yapay zekanın gelişmişliğini dikkate alması gerekir.

Hekimler 'mesleki gizlilik' ilkesine biçilen yüksek değeri korumalıdır

Mesleki gizlilik, hekimlik mesleğinde güvene dayalı ilişkinin var olabilmesi ve sürdürülebilmesinde yüksek bir değeri ifade eder. Hekimin bu değeri koruması, Hippokrates zamanından beri bir ödev olarak kabul edilmektedir. Hekimlik Meslek Etiği Kurallarının 9. maddesi mesleki gizliliği mutlak bir değer olarak belirtmektedir (TTB, 2012).

> "Hekim, hastasından mesleğini uygularken öğrendiği sırları açıklayamaz. Hastanın ölmesi ya da o hekimle ilişkisinin sona ermesi, hekimin bu yükümlülüğünü ortadan kaldırmaz."

Buna karşın Tıbbi Deontoloji Nizamnamesinin 4. maddesi ve Hasta Hakları Yönetmeliği'nin 5. maddesine göre hekim tıbbi zorunluluklar ve kanuni bir mecburiyet olduğu durumlarda hasta bilgilerini ölçülü bir şekilde açıklayabileceği ifade edilmektedir. Dolayısıyla her iki düzenlemeye göre hekimin mecburi bir şekilde bilgi açıklaması, meslek ahlakı yükümlülüğüne aykırı değildir (Tıbbi Deontoloji Nizamnamesi, 1960).

> "Tabip ve diş tabibi, meslek ve sanatının icrası vesilesiyle muttali olduğu sırları, kanuni mecburiyet olmadıkça, ifşa edemez.
>
> Kanun ile müsaade edilen haller ile tıbbi zorunluluklar dışında, hastanın özel hayatının ve aile hayatının gizliliğine dokunulamaz."

Hasta-hekim ilişkisinde mahremiyetin yüksek değeri Hasta Hakları Yönetmeliği'nin 21. ve 23. maddelerinde oldukça kapsamlı bir şekilde düzenlenmiştir. Buna göre yönetmeliğin 21. maddesi şu şekildedir (Hasta Hakları Yönetmeliği, 1998);

> "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. Eğitim verilen sağlık kurum ve kuruluşlarında, hastanın tedavisi ile doğrudan ilgili olmayanların tıbbi müdahale sırasında bulunması gerekli ise; önceden veya tedavi sırasında bunun için hastanın ayrıca rızası alınır." Yönetmeliğin 23. maddesinde "Sağlık hizmetinin verilmesi sebebiyle edinilen bilgiler, kanun ile müsaade edilen haller dışında, hiçbir şekilde açıklanamaz. Kişinin rızasına dayansa bile, kişilik haklarından bütünüyle vazgeçilmesi, bu hakların başkalarına devri veya aşırı şekilde sınırlanması neticesini doğuran hallerde bilginin açıklanması, bunları açıklayanın hukuki sorumluluğunu kaldırmaz. Hukuki ve ahlaki yönden geçerli ve haklı bir sebebe dayanmaksızın hastaya zarar verme ihtimali bulunan bilginin ifşa edilmesi, personelin ve diğer kimselerin hukuki ve cezai sorumluluğunu da gerektirir."

Yönetmelikte ifade edildiği üzere hukuki ve ahlaki yönden haklı bir sebebin varlığı halinde hekim, ölçülü bir şekilde bilgi paylaşabilir. Bu maddelerde görüldüğü üzere hastanın mahremiyeti, özerkliğine verilen değer ile birlikte ele alınmış ve kişilik haklarına verilen önem ön plana çıkmıştır. Ölüm olayı dahi mahremiyetin ihlali için geçerli bir sebep kabul edilmemiştir. Mahremiyet hakkına verilen bu yüksek değer nedeniyle hekimlere mesleğini yaparken, mahkemelerde tanık olarak dinlenmek ve bilirkişi olarak görevlendirilmekten çekilme hakkı dahi tanınmıştır.

Buna karşın mevcut durum incelendiğinde yasal gereklilikler karşısında mesleki gizlilik ilkesine verilen yüksek değerin göz ardı edildiği ileri sürülebilir. Bu durumda hekim, meslek ahlakının temelinde bulunan mahremiyeti koruma hakkı ile yasal zorunluluk nedeniyle verileri onam almadan Sağlık Bakanlığına gönderme zorunluluğu çatışmasını yaşamaktadırlar. Bu durumda hekimler, mesleki gizliliği korunması gereken üst bir değer olarak düşünerek veri gönderimini zorunlu tutan uygulamayı, meslek ahlakı açısından kabul edilip edilemeyeceğini sorgulamalıdır. Bu sorgulamayı yapabilmek için Bakanlığın veri toplama gerekçelerini incelemelidir. Yanı sıra sağlık verisinin nasıl toplandığı, hastaların özerkliği ve mahremiyetlerine saygı gösterilip gösterilmediği, paylaşımı gerçekleşecek bilgilerin mahremiyetinin ihlal edildiğinde ortaya çıkarabileceği zararların büyüklüğü gibi eleştirel değerlendirmelerinin ardından yasal gerekliliklere uymaya karar vermişlerse bu kararı

uygulamadan önce bunun gereklilikleri konusunda da hastalarını aydınlatmalıdır. Böylece hekimler, kendilerine ve dolayısıyla tıbba olan güveni koruyabilirler. Bununla birlikte özellikle biyometrik veri gibi hassasiyet düzeyi çok yüksek veriler toplanmak istendiğinde ve yasal gereklilikler buna göre oluşturulduğunda da aynı değerlendirmeyi yapmalı, biyometrik verinin toplum yararı açısından seçeneksiz bir biçimde gerekli olup olmadığını sorgulamalıdır. Bu tez kapsamında yapılan sorgulamada bu tür bir veriyi toplum yararı açısından gerekçelendirmenin çok zor olduğu ileri sürülmüştür (Bkz. s.199). Bu bağlamda Bakanlık istiyor olsa bile hekim biyometrik veriyi paylaşmamalıdır. İlgili kurum tarafından biyometrik verinin seçeneksiz bir biçimde gerekliliği açıklanmazsa, hekim bu veriyi kesinlikle işlememelidir. Bu bağlamda hekim, daha önce toplanmış olan sağlık verilerinin hedeflenen amaç için kullanılabileceğinin farkında olmalıdır. Toplum yararı amacıyla değil de kimlik doğrulaması yapabilmek gibi amaçlarla kurumsal olarak biyometrik verinin işleneceği söz konusu durumlarda, hekim verinin işlenmemesi yönünde gerekli girişimlerde bulunmalıdır. Buna göre biyometrik verinin hassasiyet düzeyi konusunda ve işlenmesi durumundaki olası riskler hakkında ilgili kurumun yöneticisini ve hastaları uyarmalıdır.

Özellikle Büyük Veri çağında hekim bu risklerin farkında olmalı ve mesleki gizlilik ilkesine verilen yüksek değeri korumalıdır. Diğer yandan sağlık hizmetinin ticarileştirildiği günümüz koşullarında hekimlerin halihazırda aydınlatılmış onam alma gibi temel sorunları karşısından ayrıca kişisel sağlık verilerinin mahremiyetinin korunması yönünde onamın tüm gerekliliklerini yerine getirmesi oldukça güç görünmektedir. Dolayısıyla kişisel verilerin toplanmasının yaratabileceği mahremiyete ilişkin riskler bertaraf edilmeden, hekimlerin veri paylaşmaması gerektiği pratik açıdan savunulabilir. Ancak özellikle halk sağlığı araştırmaları için gerekli olan kişisel sağlık verilerinin kullanılması söz konusu olduğunda hekimlerin orantısız bir engel oluşturmaması da önemli görünmektedir. Bu bağlamda istatistiki veri olarak kişisel bilgilerden arındırılarak paylaşım yapılabileceği göz önünde bulundurulmalıdır.

Çok değerli bir veri türü olan sağlık verileri günümüzde farklı amaçlarla kullanılmış, paylaşılmış, satılmış ve yetkisiz erişimlerin hedefi olmuştur. Gelecekte benzeri tehditlerin yaşanması kişi ve toplumlara çok büyük zararlar getirebileceğinden, etik

açısından hekimler, yasalara aykırı olsa dahi evrensel meslek ahlakı değerlerini ve insan haklarını korumalıdır. Makro düzeyde mahremiyetin asıl değeri özgür bir toplumun varlığını devam ettirmesinde ortaya çıkmaktadır. Bu nedenle mahremiyetin korunması, sadece bireyin özel alanı değil aynı zamanda toplumun gözetimden korunması demektir. Dolayısıyla veri toplama süreci mahremiyet, özel yaşama saygı, özerklik ve insan hakları gibi temel değerler korunacak şekilde yapılandırılmalı ve bu süreçte hekimler kişisel verilerin korunması hakkını tanımalı ve bu bağlamda hastanın mahremiyet hakkını ve mahremiyetleri üzerindeki özerk kararlarını korumalıdır.

5.1.6.2.E-Nabız, mahremiyet ve gizlilik ilkesi ile uyumlu olmalı

Kişisel sağlık kaydı uygulamaları, bireyin sağlık durumu ile ilgili tüm bilgilerine erişim ve hastaların daha nitelikli bir sağlık hizmeti alabilmesi açısından oldukça önemlidir. Halihazırda ideal özelliklere sahip bir kişisel sağlık kaydı uygulaması çeşitli açılardan sorgulanmaktadır (Bkz. s.204). Toplum yararı açısından ideal bir kişisel sağlık kaydı uygulamasının en önemli özelliği, çok sayıda verinin kaydedilebilmesi veya çok çeşitli amaçlara hizmet edebilmesi değil, kullanıcıların mahremiyetlerini koruyacak nitelikte bireyin sağlık gereksinimlerini karşılamasıdır. Bu bağlamda kişisel sağlık kaydındaki bilgilerin ilgili kişiden başka bir kimsenin bilmemesi ve bu bilgilere erişim sağlayamaması gerekir. Bunun yolu kişisel sağlık kaydı uygulamalarında toplanacak olan bilgilerin, kişinin kendi cihazında tutulmasından geçmektedir.

Tez kapsamında incelenen e-Nabız uygulamasının mahremiyet ve gizlilik ilkesi ile uyumlu olmayan bazı özellikleri saptanmıştır. Bunlardan ilki, uygulama amacı her ne kadar kişilerin kendi verilerine erişimini sağlamak biçiminde belirtilmiş olsa da toplanan veriler açısından birey merkeze alınmamaktadır. Diğer bir deyişle toplanan veriler kişinin kendi cihazında toplanmamaktadır. Çünkü sistem, Sağlık Bakanlığı'nın belirli amaçları doğrultusunda bilgilerin toplandığı bir veri tabanı biçiminde tasarlanmıştır. Buna göre web tabanlı tasarlanan e-Nabız sistemine "bireyler de" erişim sağlayabilmektedir. Başka bir ifadeyle uygulamanın kontrolü tam olarak bireyin kendisinde değildir. Bu açıdan da e-Nabız sistemi, mobil uygulaması da bulunan bir veri tabanıdır. Buna göre e-Nabız sisteminin salt mobil uygulama olarak kullanılması, uygulamayı daha çok kişiselleştirebilir. Teknik açıdan bunun mümkün olduğu temas takip uygulamaları bağlamında ileri sürülmüştür (Çayır, 2020a, 2020c, 2021). Buna

göre uygulamaya işlenecek veriler için merkezi olmayan sistemlerin kullanılması gerekmektedir.

Tez kapsamında belirlenen toplum yararı, özerklik ve eşitlik ve adalet ilkesi açılarından incelenen e-Nabız uygulamasında saptanan sorunlar, mahremiyet ilkesi ile de doğrudan ilişkilidir. Çünkü ilkeler birbirleri ile tutarlı ve tamamlayıcı nitelikte belirlenmiş ve tanımlanmıştır. Bu bağlamda toplum yararı açısından ideal bir kişisel sağlık kaydı uygulamasının tartışmalı olduğu, ancak belli gereksinimleri karşılayan ve özerklik, mahremiyet, eşitlik ve adalet ilkeleri ile uyumlu oldukça ideal olabileceği belirtilebilir. Veri toplamanın son adımlarından biri olarak tanımlanan mahremiyet ve gizlilik ilkesi, kişisel sağlık kaydında toplanan verilerin mahremiyetinin korunmasını ifade etmektedir. Bununla birlikte özerklik ilkesi açısından değerlendirilen e-Nabız sisteminde örneğin kişilerin kendi verilerini istedikleri zaman silememesi, mahremiyet ilkesi ile de ilgilidir. Çünkü verilerin silinememesi, bireyin mahremiyeti açısından risk oluşturabilecek bilgilerin bireyin özerkliğine aykırı olarak saklandığını göstermektedir.

İdeal bir kişisel sağlık kaydının özelliklerini araştıran bir çalışmaya göre hastalar arasında bu tür uygulamaların benimsenmesinin önündeki en temel engellerden biri bilgilerin korunmadığı veya koruma düzeyinin hassas olmadığı yönünde kaygılar olduğu belirtilmektedir (Kahn ve ark., 2009). E-Nabız kullanıcı değerlendirmelerini inceleyen bir çalışmaya göre kullanıcıların e-Nabız sisteminin özel hastanelerden de veri çekebilmesi, Google Fit gibi bazı bilindik sağlık uygulamalarından bilgi çekebilmesi ve günlük tüketilen yiyeceklerin eklenerek sağlıklı yaşam takibinin daha iyi yapılabilmesi gibi çeşitli özelliklerin eklenmesi raporlanmıştır (İnal & Ercil Cağıltay, 2019). Bu araştırmanın sonuçlarına göre kullanıcı gereksinimleri değişebildiği gibi kullanıcılar kişisel verilerinin korunması konusunda bilgili ya da duyarlı olmayabilecekleri yorumu yapılabilir. Dolayısıyla uygulamanın mahremiyet ve gizlilik ilkesi ile uyumlu olabilmesi için kişisel verilerin, kullanıcının cihazında tutulabileceği bir gizlilik tasarımına sahip olmalıdır.

Toplum yararı ilkesi başlığında belirtildiği gibi toplum yararına kullanılacak verinin bu uygulama aracılığı ile toplanması hedefleniyorsa, gerekli görülen bilgiler için kullanıcının ayrıca onamı alınmalıdır. Dolayısıyla mahremiyet ve gizlilik ilkesine

verilen değer, özerkliğe saygı gösterilmesinden beslenmektedir. Çünkü özerklik mahremiyet ile bilgilerin kişiye ait olması ve kişinin onamı olmadan başkaları tarafından bilinmemesi bakımından ilişkilidir. Bu bağlamda kişisel sağlık verilerinin işlenebilmesi için aydınlatılmış onam alınmalı ve verilerin mahremiyet ve gizliliğini korumak yönünde yeterli güvence verilmelidir.

E-Nabız uygulamasının Gizlilik, Kullanım ve Telif Hakları metninde mahremiyet ve gizlilikle ilgili olarak şu ifadeler bulunmaktadır;

> "Kişilerin E-Nabız'daki sağlık bilgilerini sadece kişilerin onayını alan hekimler ve/veya kişiler görebilir. Kişilerin, E-Nabız'da paylaşmış olduğu bilgiler, kişilerin onayı dışında ya da yargı kararı ve/veya yasal bir yükümlülük altında bulunmadığı sürece herhangi bir üçüncü şahıs, kurum ve kuruluş ile hiçbir nedenden ötürü paylaşılmayacak ya da verilmeyecektir. Yasal düzenlemelerle bu bilgilerin açıklanmasını gerektiren bir durum gerçekleşmediği sürece hiçbir istisna ile bu bilgiler açıklanmayacaktır."

E-Nabız sisteminin "güvenlik ayarları" ekranında "Hiçbir hekim verilerimi görmesin (SMS kodu veya şifrematik ile onay zorunlu)", "Aile hekimim verilerimi görsün (Önerilen)", "Muayene olduğum hekim verilerimi görsün (Önerilen)", "Muayene olduğum hastanedeki tüm hekimler verilerimi görsün" ve "Sağlık Bakanlığındaki tüm hekimler verilerimi görsün" biçiminde seçenekler mevcuttur. Bu seçenekler hekim de olsa bireyin onamı dahilinde kişinin sağlık bilgilerini görüntüleyebilecek olması mahremiyet ve gizlilik ilkesine uyumluluk açısından dikkate değerdir. Buna karşın uygulamanın bildirimler ekranı incelendiğinde, kullanıcının e-Nabız kaydına erişim sağlayan kişilerin (hekimlerin) erişim bilgileri listelenmektedir (Görsel 16). Bu liste, kullanıcıyı bilgilendirmesi açısından olumludur. Diğer yandan yetkisiz erişim sağlayan kişinin kullanıcının izni olmadan bir şekilde e-Nabız kaydına erişim sağlamış olduğunu göstermesi açısından mahremiyet ve gizliliğe yönelik soru işareti oluşturmaktadır.

Mahremiyet ve gizlilik ilkesi açısından e-Nabızda saptanan bir başka sorun, uygulamanın çok çeşitli özelliklere sahip olmasıdır. Uygulamanın özellikleri çeşitlendikçe, kişisel veri kaydedilmesi olanağı genişlemektedir. Bu durumda mahremiyete ilişkin risk oluşmaktadır. Kişisel veri kayıt sistemlerinde mahremiyete

yönelik riskleri minimize etmek ve kullanılacak uygulamaların etkinliğini maksimize etmek temel amaç olmalıdır.

5.1.6.3.Veri tabanları, hasta mahremiyetini korumaya elverişli olmalı

Sağlıkta geleneksel yöntemlerle tutulan tıbbi kayıtların bütünüyle elektronik veri tabanları ile gerçekleştirilmesi, sağlık çalışanlarının mahremiyeti koruyabilmesini güçleştirmektedir. Çünkü dijital alanda tıbbi kayıtların güvenliğinden tam olarak emin olmak mümkün değildir. Bununla birlikte veri güvenliğine ilişkin bazı temel önlemlerin alınması ile mahremiyet hakkının güvence altına alınması söz konusudur. Buna göre sağlık hizmetlerinin tüm basamaklarında kullanılan veri tabanları hasta mahremiyetini korumaya elverişli olmalıdır.

Tez kapsamında incelenen Hızır AHBS ve MİA MED veri tabanlarına başta hekim olmak üzere sağlık çalışanları tarafından birçok kişisel bilgi kaydedebilmektedir. Hızır AHBS sistemi koruyucu sağlık hizmetleri kapsamında sağlık verisi kaydedilmesinin yanı sıra bu kapsamda değerlendirilemeyecek türde kişisel bilgi kaydı yapılabilmektedir. Buna göre kişilerin kimlik numarası, adı ve soyadı, cinsiyeti, resmi doğum tarihi, yaş (ay ve gün olarak), anne ve baba adları, medeni durumu, aile kodu, kan grubu, telefon, adres, ölüm ve doğum tarihi, öğrenim durumu, sigara-alkol-madde kullanımı, hükümlülük durumu, yaralanma geçmişi ve cezaevi tipi gibi çok sayıda kişisel bilgi bulunmaktadır. Bu bilgilerin Hızır AHBS sistemine kaydedilmesi, aile hekiminin hastayı takip edebilmesi ve toplum sağlığı açısından gereklidir. Bu bağlam içerisinde kalan bilgiler veri tabanına kaydedilmeli, kaydedilen bilgiler ise Sağlık Bakanlığına anonim bir şekilde iletilebilmelidir. Hasta mahremiyetinin koruyabilmek için Ulusal Sağlık Veri Seti Sözlüğünde “Gizli Hasta Veri Seti” belirtilmekte ve bu veri setinin 1.2.3. Basamak Sağlık Kurumları tarafından HIV paketi ile gönderimi zorunlu tutulmaktadır. Yanı sıra gizli hasta veri setinin içeriğinde “hasta kodu” tanımlanmaktadır. Bu kod ile hastanın kimlik bilgilerinin gizlendiği ve hastanın tedavi ve izlem süreçlerinin takip edildiği ifade edilmektedir.

Bununla birlikte veri güvenliğinin tam olarak sağlanabilmesi ve hasta mahremiyetinin korunabilmesi için doğrudan kişinin sağlık durumu ile ilgili olmayan kişisel bilgi ayrımının yapılması ve hatta veri tabanına kaydının yapılamaması gerekir. Dolayısıyla

birinci basamak sağlık hizmetleri kapsamında hangi sağlık verilerinin sisteme kaydedilebilir olması gerektiği ve kaydedilen bilgilerden hangilerinin Sağlık Bakanlığı ile paylaşılabilir olması gerektiği belirli olmalıdır. Yanı sıra bu bilgilerin hastanın onamı dışında Sağlık Bakanlığı'na gönderilmesi, hastanın özerkliğine aykırı olduğu gibi hasta mahremiyetine de aykırıdır. Veri tabanı düzeyinde hasta mahremiyetinin korunabilmesi için Sağlık Bakanlığı'na gönderimi yapılacak bilgiler için hastanın onamı alınmadan veri gönderimine izin vermeyecek bir tasarıma sahip olmalıdır. Daha açık bir ifade ile hastanın tedaviye erişimini engellemeyen ve tedavisinin etkilenmeyeceği düşünülen bazı bilgiler veri tabanına hiç kaydedilmemelidir. Bildirim yükümlülüğü bulunan ve toplum sağlığını ilgilendiren hastalıklarda ise veri tabanı üzerinde onama ilişkin bazı istisnalar tanımlanabilir. Özetle hasta mahremiyetini korumak için elverişli bir veri tabanı için bilgiler güncel, yeterli, doğrudan sağlık durumu ile ilgili ve aşırı olmamalıdır. Buna göre örneğin Hızır AHBS veri tabanının hasta mahremiyetinin korunduğu durumlar söz konusudur. Bir aile hekimi veri tabanı üzerinden hastanın e-Nabız kaydına erişim sağlamak ihtiyacı hissettiğinde hastanın onamına ihtiyaç duymaktadır (Görsel 52). Sistem üzerinden hastanın cep telefonuna gönderilen kodun hasta tarafından hekim ile paylaşılması sonucu hekim belirli bir süre dahilinde hastanın kayıtlarını görüntüleyebilmektedir (Görsel 53). Ekranda ayrıca e-Nabız kaydının amacı dışında kullanılmaması yönünde bir uyarı da bulunmaktadır (Görsel 54).

Üçüncü basamak sağlık hizmetleri kapsamında kullanılan MİA MED, tedavi odaklı sağlık verilerinin kaydını tutmaktadır. Hastaneye ilk başvurudan kan alma birimine, poliklinik muayeneden yoğun bakım servislerine birçok işlem MİA MED üzerinden gerçekleşmektedir. MİA MED sisteminin hasta mahremiyetini korumak için taşıması gereken en önemli özelliği, farklı polikliniklerde kaydı açılan hastanın başvuruda bulunduğu poliklinik dışında diğer polikliniklerin hasta bilgilerine erişim sağlayamamasıdır. Örneğin kadın hastalıkları ve doğum polikliniğine başvuruda bulunmuş ve kaydı oluşturulmuş bir hastanın bilgilerine kulak burun ve boğaz hastalıkları bölümü erişim sağlayamamalıdır. İncelenen MİA MED sisteminin bu özelliği taşıdığı belirtilebilir.

Hasta mahremiyetine ilişkin bir diğer konu veri tabanlarına bağlı olarak çalışan muayene takip ekranlarında hastaların ad soyad bilgilerinin herkes tarafından görülecek şekilde ekranda yer alması konusu bulunmaktadır. Bu konu kişisel verilerin korunmasına ilişkin farkındalığın artması ile birlikte hasta mahremiyetine aykırı olduğu gerekçesiyle KVK Kurulu tarafından çıkarılan bir genelge ile muayene takip ekranlarında hasta bilgilerinin maskelenerek yer alması gerektiği sağlık kurumlarına iletilmiştir. Ancak kararın uygulanmasında hastaların muayene sıralarını takip edemedikleri ve randevu mekânında hazır olmakta güçlük çektikleri tespit edilmiştir. Bu durum hastaların sağlık hizmetine erişimini güçleştirmiştir. Bu nedenle gizlilik tercihinin e-Nabız kaydı üzerinden kişiye bırakılması veya hastaların sağlık kuruluşuna başvuru sırasında ad soyad bilgilerini maskelemeyi tercih edebilmelerine olanak tanınması düşünülmüştür. Bu doğrultuda oluşturulan teknik altyapı, Sağlık Bakanlığı tarafından hayata geçirilmiştir.

Sağlık Bakanlığı veri tabanlarının alım süreçleri, standartlarına ve tescil işlemlerinin belirlenmesine ilişkin usul ve esasları düzenleyen Sağlık Bilgi Yönetim Sistemleri Hakkında Yönetmelik ile sağlık bilgi yönetim sistemlerine Yetkinlik Puanı hesaplaması getirmiştir (Md.20). Bu hesaplamaya göre Personel Kapasite Puanı ve Teknik Değerlendirme Puanı olmak üzere iki ölçüt tanımlanmış ve bu ölçütlerin nasıl hesaplanacağı açıklanmıştır. Bu uygulamanın sağlık bilgi yönetim sistemlerinin iyileştirilmesi ve böylece mahremiyet ve gizliliğin korunması yönünde olumlu bir adım olduğu vurgulanabilir.

5.2.Mobil Uygulamaların İlgili Kılavuz Açısından Değerlendirilmesi

Tarih boyunca bulaşıcı salgınlar, toplumları olumsuz etkilemiş ve kolera, veba gibi bazı salgınlar kitleler halinde yaşamların son bulmasına neden olmuştur. Bu kapsamda 21. yüzyılın vebası da modern tıbbın, tıbbi teknolojinin ve bilimin yetersiz kaldığı Covid-19 hastalığı olmuştur. Solunum yoluyla bulaşan bu salgınla mücadele edebilmek için pek çok ülkede olduğu gibi Türkiye'de de çeşitli önlemler alınmış, özellikle cep telefonları ile insan hareketliliğinin ölçülmesi amaçlanmış ve çeşitli temas takip ve ön tanı koyma gibi mobil uygulama programları geliştirilmiştir. Dünyada ve Türkiye çeşitli özelliklere sahip uygulamalar kullanılmış olsa da mobil uygulamaların ortak özelliği kişisel bilgi işlemesidir. Kişilerin kimlik bilgileri, iletişim

bilgileri, konum bilgisi ve meslek bilgileri ile Covid-19 hastalığına ilişkin sağlık bilgileri diğer bir deyişle "kişisel veri" olarak adlandırılabilecek hemen her bilgi bu uygulamalarla toplanabilmektedir. Bu tür uygulamalara işlenen kişisel veriler ve bu verilerin güvenlik sorunları nedeniyle mahremiyetin sınırları dünya genelinde tartışmalı hale gelmiştir. Uygulamalar aracılığı ile çok hassas düzeydeki kişisel verinin işlenebilmesi, başta mahremiyet ve gizliliğe dayalı etik sorunları karşımıza çıkarırken halk sağlığı gerekçesi ile bu verilerin işlenmesi, insanların sürekli olarak izlenmesini mümkün hale getiren "gözetim" kavramını da ortaya çıkarmaktadır. Gözetim özellikle mobil uygulamalarla çok daha kolay olabilmektedir. Çünkü mobil uygulamalar hastane kayıtlarından farklı olarak tüm vatandaşları hedefleyen ve bireyleri kolaylıkla izleyen uygulamalar oldukları için çok daha tehlikelidirler. Bu uygulamaların olağandışı durumlarda kullanılması, hükümetler ve çeşitli kurum ve kuruluşlar da çok daha geçerli bir neden oluşturmaktadır. Dolayısıyla bu tür uygulamaların özellikle olağandışı durumlarda da amaç, kapsam ve sınırları belirli bir şekilde kullanılması önemli görünmektedir.

Bu konuda Covid-19 ile mücadele kapsamında çıkarılan mobil uygulamaların güvenilir ve hesap verilebilir kullanımına rehberlik etmesi amacıyla Avrupa Konseyi, "Guidance on Apps supporting the fight against COVID-19 pandemic in relation to data protection" başlıklı kılavuzu yayımlamıştır (European Commission, 2019). Bu metin mobil uygulamaların kullanımına yönelik uluslararası standartları belirlemesi açısından oldukça önemlidir. Kılavuza göre Türkiye'de kullanılan HES, Korona Önlem ve beraberinde HES kodu uygulamasını değerlendirmek ve kılavuz ile uyumlu olmayan özellikleri belirlemek tezin bu son bölümünün amacıdır.

Konum ve yakınlık verileri hakkında

Covid-19 pandemisinin kişisel sağlık verileri üzerine etkisi, özellikle konum verileri açısından oldukça tartışmalı olmuştur. Virüsten etkilenen kişileri izlemek ve virüslü kişi ile temas edenleri uyarabilmek için mobil uygulamaların konum verilerinden yararlanılması, pandemiyi kontrol altına almak için oldukça etkili bir yöntem olarak değerlendirilebilir.

Buna karşın konum bilgisinin işlenmesi ile gizlilik ve güvenliğe dayalı çeşitli sorunlar dile getirilmiştir (Çayır, 2021). Bir haber kaynağına göre Android kişi izleme uygulamalarının konum verilerini sızdırdığı açıklanmıştır (Leprince-Ringue, 2021). Bir çalışmada, Almanya, İtalya, İsviçre, Avusturya ve Danimarka'da kullanımda olan Google/Apple tabanlı kişi izleme uygulamalarında gizlilik ile ilgili boşluklar bulunduğu saptanmıştır (Leith & Farrell, 2020). Avrupa Birliği Veri Koruma Kurumu'na göre konum verileri, sağlık verileri ve diğer verilerle bütünleştirildiğinde çok tehlikeli olabilir (Çayır, 2021). Konum verileri bir cihazın temel işlevlerinin en önemli parçasıdır. Konum verilerinin cep telefonu operatörleri ve işletim sistemleri ile cihaza yüklenen mobil uygulamalar aracılığı ile aktif olarak bir ağa bağlı olmadan da izlemeye olanak tanıdığı ve tanımlayıcı bilgiler yayan akıllı eşya veya oyuncaklar gibi "Nesnelerin İnterneti" (IoT) cihazları tarafından tutulabildiği belirtilmektedir (Çayır, 2020c). Dolayısıyla konum verisinin tehlikesi, insanların sürekli olarak izlenmesini mümkün hale getirmesi nedeniyle bir gözetim uygulaması olarak kullanılabilmesidir.

Pandemi süreci boyunca Türkiye'de konum bilgisi, HES mobil uygulaması ile işlenmiştir (Görsel 75). Uygulamaya işlenen bu verinin kullanılıp kullanılmayacağı, mahremiyet ve gizliliği korumak için gerekli donanımlara sahip olsa bile işlenen bilgilerin bilimsel açıdan gerekli olup olmadığı, bu veri kullanılacaksa nasıl kullanılması gerektiği gibi soruları ilgili kılavuz ışığında yanıtlamak, temas-takip uygulamalarının getireceği kötü ihtimallere karşı hazırlıklı olmayı sağlaması açısından önemli görünmektedir.

Pandemi döneminde enfeksiyon zincirini kırmak ve risk durumunu kontrol altında tutabilmek çok önemlidir. Bu amaçla Avrupa Konseyi ilgili kılavuzda yakınlık temas ölçümü için coğrafi konum verilerinin (GPS veya hücresel konum verileri) yerine Bluetooth Low Energy (BLE) iletişim verilerinin kullanılmasını önermektedir. Çünkü BLE iletişim verileri, coğrafi konum verilerinin aksine izleme olasılığını ortadan kaldırmaktadır. Yanı sıra konum verilerinin minimum veri açısından gerekçelendirilmesinin zor olacağı, gizlilik ve güvenlik sorunları yaratabileceği ve hedefleri bireylerin hareketlerini takip etmek olmadığı için temas takip uygulamalarında konum verisinin gerekli olmadığı vurgulanmaktadır. Bluetooth servisi ile kişiler, riskli bireylerin kendilerine yaklaşması durumunda uyarı almakta,

gün içinde temas ettikleri kişi sayısına bakabilmekte ve bulundukları bölgenin yoğunluk haritasını kontrol edebilmektedirler. HES uygulaması incelendiğinde yakınlık verisi olarak Bluetooth servisi kullanılabilmektedir. Bu açıdan uygulamanın bu özelliği, Konsey'in önerdiği yaklaşımla uyumludur. Buna karşın Bluetooth servisinin kullanılmasına yönelik çeşitli kaygılar da bulunmaktadır. Dolayısıyla bu tez kapsamında bu servisin onam alınmadan kullanılması önerilmemektedir.

Uygulamanın kurulum aşamasında Türkiye çapında vaka yoğunluk haritası ve bulunulan bölgedeki risk durumunun görüntülenebilmesi için konum verisine ihtiyaç duyulduğu belirtilmekte ve hatta uygulama kapalıyken ya da kullanılmıyorken bile konum verisinin toplanabileceği açıklanmaktadır (Görsel 75). Dolayısıyla uygulamanın kurulumunun sağlanabilmesi için bu verinin işlenmesine izin verilmesi gereklidir. Uygulamanın kurulumu sağlandıktan sonra konum servisini kapatmak mümkündür ancak konum verisinin kullanıcı tarafından kapatılması durumunda sistem sürekli olarak kullanıcıdan konum verisine erişim talebinde bulunmakta ve hatta uygulamaya kurulum aşamasında verilen izin nedeniyle konum verisi kendiliğinden aktif hale gelebilmektedir. Uygulamanın bu özelliği özerklik açısından sorun oluşturmaktadır. Kişilerin uygulamayı gönüllü olarak cihazına yüklemesi özerklik ilkesi ile uyumlu iken zorunlu olarak konum bilgisinin işlenmesi, özerkliğe aykırı görünmektedir.

Konum bilgisi bireyin sürekli olarak hareketlerinin takip edilmesine izin veren bir veridir. Bu verinin toplanmasını, Covid-19 pandemisi gibi olağandışı durumlar açısından ayrıca değerlendirmek gerekir. Solunum yoluyla bulaşan Covid-19 hastalığının Dünya Sağlık Örgütü'nün (2020/21) raporlarında, küresel olarak aşırı ölüm hızının oldukça yüksek olduğu bildirilmiştir (WHO, 2021b). Solunum yoluyla bulaşması ve ölüm hızının yüksek olması Covid-19 salgının kontrol altına alınabilmesi için konum bilgisinden yararlanılması gerektiği bir zorunluluk olarak kendini göstermektedir. Yaşamsal tehlikenin yanı sıra Covid-19 salgını sosyal, ekonomik, fizyolojik ve psikolojik açılardan bütün dünyayı etkilemeye devam etmektedir. Dolayısıyla Covid-19 hastalığını olabildiğince hızlı bir şekilde kontrol altına alabilmek için konum verilerinin toplum yararı açısından gerekli olduğu belirtilebilir. Bu durumda konum verisinin işlenebilir olması haklı çıkarılabilmektedir. Ancak diğer

taraftan toplu ve anonimleştirilmiş konum verilerinden yapılan analizler, salgının kontrol altına alınmasında oldukça etkili bir yöntem olarak değerlendirilebilir. Dolayısıyla konum verisinin nokta veri olacak şekilde toplanması ile toplu hareket verilerini birbirinden ayırmak gerekir. Konum bilgilerinin HES uygulaması ile toplanabilmesinin alternatifi olarak doğrudan Telekom operatörlerinin kullanıcı konuşmalarından baz istasyonlarına yakınlıklarına göre anonim hareket verilerini yetkililerle paylaşabilmesi de mümkündür. Bunun yanı sıra Google, Facebook gibi şirketler, pandemi ile mücadele kapsamında devletlerle görüşmekte ve işbirliği içerisine girebilmektedir. Örneğin Google, konum verilerinin avantajlarını gösterebilmek için kullanıcıların hareket veri raporlarını https://www.google.com.tr/covid19/mobility/ adresinden yayınlamaktadır.

Hareket verileri, ne kadar insanın hangi saatte nereden nereye hareket ettiği bilgisini vermektedir. Bu bilgiden hareketle bulaş riskini artıran yerler saptanabilir ve buna göre çeşitli önlemler alınabilir. Bu verinin kişisel veri içermediği için mahremiyetin korunabilmesinde avantajlı olabileceği düşünülebilir. Büyük Veri analizi kullanılarak hareket verilerinden de bir kişinin kim olduğunu tespit etmek mümkündür. Salgınla mücadele kapsamında doğrudan konum bilgisinin toplanması yerine hareket verilerinden yararlanılması mahremiyet açısından dikkate değerdir. Hareket verilerinin yetersiz kalması durumunda mutlaka konum bilgisinin toplanması gerekiyorsa, bu durumda doğru bilgilendirme yapılmalı ve verinin belirlenen amaç doğrultusunda kullanılacağına ilişkin yeterli güvenceler sağlanmalıdır. Bu konuda HES, hareket verilerini yoğunluk harita bilgilendirmesi özelliği ile gerçekleştirmektedir. Uygulamanın bu özelliği ile noktasal verinin yanı sıra hareket verisinin de işlendiği görülmektedir.

HES uygulamasına işlenen yakınlık verisi ile ilgili olarak birtakım kullanım sorunları yaşandığı saptanmıştır. Uygulamanın kullanıcı yorumlarında saptanan sorunlar şunlardır; Bluetooth servisinin ve konum verisinin otomatik olarak açılması, bu işlevlerin açılması ile cihaz şarjlarının kısa sürede tükendiği, uygulama bildirimlerin kapatılamaması, kullanıcının bu servisleri kapatabilmek için uygulamayı cihazdan kaldırmak durumunda kalabilmesi. HES uygulamasının kullanıcılar tarafından benimsenmesi ile ilgili yapılan bir araştırmada, uygulamayı kullanmak istemeyen

katılımcıların (%11.8), uygulamayı kullanmama nedenleri arasında bu sorunlar belirtilmektedir (Alkış & Fındık-Coşkunçay, 2021). Bu sorunlar karşısında olağandışı bir durum söz konusu olduğu için çok hassas düzeyde kişisel veri işlemesine olanak tanıyan HES gibi bir mobil uygulamanın pilot uygulama olarak kullanılıp kullanılmadığı sorusu ortaya çıkmaktadır. HES mobil uygulamasının pilot uygulama olarak kullanıldığına ilişkin yazında ve Sağlık Bakanlığı açıklamalarında herhangi bir bilgi saptanmamıştır. Uygulamanın ilerleyen süreçlerinde bu sorunların çözümlenmesi için Sağlık Bakanlığı girişimlerde bulunmuş ve sürekli olarak uygulamayı takip etmiştir. Saptanan bu teknik sorunlar içerisinde en önemlisi, kullanıcılar uygulama üzerinde konum verisini açma-kapatma özelliklerini diledikleri gibi kullanamamasıdır. Bu durum konum verisinin birey özerkliğine aykırı olarak toplanmasına işaret etmektedir.

Bununla birlikte söz konusu temas takip uygulamaları için alınacak teknolojik önlemlerde ve hükümetler tarafından belirtilen tedbir ve vaatlere güvenmek yeterli değildir. Bu bağlamda veri işlenmesinde, ilk olarak gerçek bir koruma yöntemi, verinin sistemlere hiçbir şekilde işlenmemesi, mutlaka işlenmesi gerekli olan verinin ise kimlik bilgilerinden arındırılarak işlenmesidir. Bunun yanı sıra veri işlemede merkezi olmayan sistemler tercih edilmelidir. Merkezi olmayan sistemlerde hükümetlerin de veriye erişimi kısıtlı olacaktır. Böylece bireyin verileri üzerindeki kontrolü daha fazla olacaktır.

Temas takip uygulamaları kapsamında özellikle konum verileri bireyin onamı alınarak toplanmalı, otomatik işlemeye tabi tutulmamalıdır. Aksi durumda birçok yazarın belirtmiş olduğu gibi HES uygulaması, insanların sürekli olarak izlenmesini mümkün hale getiren bir gözetim uygulaması olarak değerlendirilecektir (Aşkin, 2021; Çayır, 2021; Polat, 2020; Zorer, 2021).

HES kodu uygulamasının kullanılmaması için güçlü nedenler

Konum verisinin işlenmesine bağlı olarak tartışmalı olan bir diğer konu HES uygulamasına tanımlı ve salgın yönetiminde zorunlu tutulan HES Kodu uygulamasıdır. Sağlık Bakanlığı bu kodu, “Kontrollü Sosyal Hayat kapsamında, ulaşım ya da ziyaret gibi işlemlerinizde kurumlarla ve kişilerle, Covid-19 hastalığı açısından herhangi bir

risk taşıyıp taşımadığınızı güvenli şekilde paylaşmanıza yarayan bir kod" biçiminde tanımlanmaktadır. Yanı sıra bu kodun paylaşılması ile mobil uygulama üzerinden ya da kurumlara sağlanan servisler aracılığı ile kişilerin risk durumlarının sorgulanabileceği bilgisi verilmektedir (https://hayatevesigar.saglik.gov.tr/hes.html).

Salgınlar olağandışı durumlar olarak tanımlandığı için hızlı bir biçimde eyleme geçmeyi gerektirmektedirler. Çünkü salgınlarda tıbbi kaynaklar yetersiz kalır ve sağlığı olumsuz etkilenen kişi sayısı fazladır. Bu nedenlerle bulaş riskini azaltmak salgını önlemenin en etkin yollarından biridir. Bu açılardan olağandışı durumlarda, HES gibi mobil uygulamalar ve beraberinde kullanılan HES kodunun geniş katılımlı bir şekilde kullanılması, enfeksiyon zincirini kırmak için oldukça etkili olabilecek bir yöntem gibi görünmektedir. Buna karşın literatürde yer alan çalışmalar, HES kodu uygulamasının uluslararası kılavuzlarda belirtilen ölçütlere aykırı bulmaktadırlar (Cangil, 2021; Çayır, 2021; Zorer, 2021). Tez kapsamında karşılaştırılan Avrupa Konseyi kılavuzuna aykırı bulunma nedenleri ise şu şekilde açıklanabilir; HES kodu kişinin sürekli gözetimine imkan vermekte, özel ya da kamu birçok kurum, alışveriş merkezleri, seyahat firmaları gibi sosyal hayatın her alanının kontrol edilmesine izin vermektedir. Yanı sıra kişilerin Covid-19 ile ilgili sağlık verilerini paylaşıma açtığı için mahremiyeti göz ardı etmektedir. Kişilerin istedikleri zaman bu kodu değiştirebilmeleri imkanı getirilerek mahremiyetin korunması amaçlanmıştır. Ancak bu özellik mahremiyeti korumak için yeterli değildir. Çünkü insanlar bu konuya karşı bilinçli ve duyarlı olmayabilir, olsa bile teknolojiyi yeterli düzeyde kullanamıyor olabilir. Mahremiyeti korumayı amaçlayan bir diğer özellik kişiye tanımlanan bu kodun belirli bir süre sonra değiştirilmesidir. Bu durumda ise sahip olduğu kodu değiştiremeyenler, istedikleri gibi hareket edememekte ve istediği kuruma girememek gibi çeşitli mağduriyetler yaşamaktadırlar.

HES kodunun bireye tanımlanması ve virüsün kaynağını araştırmayı mümkün kılması ile her bireyin virüs endeksli bir kimliklendirme ile gözetim altına alındığı ileri sürülmektedir (Aşkin, 2021). Salgın yönetiminde "evde kal", "sosyal mesafe", "fiziki temassız hayat" gibi kontrol söylemlerine uyulup uyulmadığının tespit ve takip etmeyi mümkün kılan uygulamaların veri bildirimine dayalı gözetim uygulamalarına dönüştüğü bir başka çalışma ile vurgulanmıştır (Polat, 2020). HES Kodu ile ilgili bu

sorunlar dikkate alındığında Covid-19 salgınının yönetiminde bu kodun kullanılması yine de haklı çıkarılabilir mi, haklı çıkarılabilirse hangi durumlarda haklı çıkarılabilir sorularını gelecek uygulamalar açısından tartışmak gerekmektedir.

Literatürde uygulamanın kötüye kullanımı konusunda herhangi bir denetiminin yapılmaması veya bu yönde bir açıklamanın bulunmaması, idari, teknik ve hukuki yönden alınan önlemlere ilişkin herhangi bir açıklama yapılmaması, sızma testlerinin yapılıp yapılmadığı ve kişinin izni olmadan HES kodunun paylaşılabilmesi gibi etik sorunlar dile getirilmektedir (Çayır, 2021). Yanı sıra HES kodunun kişilerin onamı alınmadan zorunlu olarak uygulanması özerklik açısından, Covid-19 hastalığı ile ilgili kişisel sağlık verilerinin kişilerin rızası alınmadan sorgulanabilir olması ve birey hareketlerinin sürekli olarak izlenmesine imkan vermesi mahremiyet açısından sorun oluşturmaktadır. Dolayısıyla halk sağlığı ile mahremiyet ve özerklik hakkı arasında orantısız bir denge kurulduğu ileri sürülebilir. Konum verisi ve beraberinde HES kodu uygulaması, diğer sağlık verileri ile bütünleştirildiğinde toplum gözetiminin derinleşmesi söz konusu olabilir. Bunun yanı sıra salgını kontrol altına alabilmenin alternatif yöntemleri, HES kodu uygulaması ile kıyaslandığında bu yöntemlerin daha etkili olduğu belirtilebilir. Buna göre salgın boyunca halk sağlığı uzmanları ücretsiz maske kullanımı, test yapılması, teste erişimin kolay olması ve son olarak aşı uygulamalarının yaygınlaştırılması gerektiğini ileri sürmüşlerdir. Dolayısıyla temel özgürlükleri kısıtlayan ve mahremiyeti korumaya yönelik özelliklerin yetersiz olduğu ve alenen bilgilerin paylaşılabildiği bir uygulama olarak karşımıza çıkan HES kodu uygulaması kullanılmamalıdır.

Mobil uygulamaların aydınlatma metinlerinde tüm bilgiler eksiksiz bir şekilde verilmeli

Özerklik ilkesinin en önemli bileşenlerinden biri kişisel sağlık verileri için aydınlatılmış onam alınmasıdır. Dijital dünyada aydınlatılmış onam alınabilmesinin oldukça kısıtlı olduğu, bununla birlikte teorik olarak yine de belirli kurallar çerçevesinde aydınlatılmış onam alabilmenin mümkün olduğu ve böylece özerklik ilkesinin korunabileceği daha önce ileri sürülmüştü (Bkz. s.234.). Bu bağlamda aydınlatılmış onam için bilgilendirmenin önemi ve kişinin anlamasının sağlanmasına dikkat çekilmişti.

Olağandışı durumlar açısından incelenen kişisel sağlık verilerini işleyen mobil uygulamaları onam açısından değerlendirmek istediğimizde, Avrupa Konseyi kılavuzuna aykırı özellikler saptanmıştır. Buna göre HES uygulamasının aydınlatma metni, bilgilendirme açısından yeterli bulunmamıştır. Pandemi boyunca HES uygulaması güncellenmiş ve buna paralel olarak uygulamanın aydınlatma metni de güncellenerek bilgilendirmenin kapsamı genişletilmiştir. Uygulamayı değerlendiren bir çalışma HES uygulamasının eski aydınlatma metnini incelemiş ve bilgilendirme kapsamında yeterli olmadığını ileri sürmüştür (Çayır, 2020c, 2021). Gelinen son noktadaki aydınlatma metni incelendiğinde Sağlık Bakanlığı tarafından güncellenmiş olsa da bilgilendirme açısından yine yeterli düzeyde olmadığı ileri sürülebilir. Buna göre uygulamanın aydınlatma metninde bilgilendirme kapsamında Covid-19 hastalığına ilişkin kimlik verisi, iletişim verisi, konum verisi, sağlık verisi, meslek verisi, Bluetooth verisi, kamera verisi, kişi listesi verisi ve dosya (video/ses/görüntü) verilerinin ne amaçla toplandığı açıklanmıştır. Bu açıklamalar, görünen amacı ifade etmesi açısından yeterli düzeyde olduğu belirtilebilir. İşlenen bu verilerin gerekli olduğu durumlarda kimlerle paylaşılabileceği de açıklanmaktadır. Buna karşın bu bilgilerin ne kadar süreyle saklanacağı, ne zaman yok edileceği, kullanıcının kendi bilgilerini silmek istemesi durumunda ne yapması gerektiği gibi soruların açık ve net bir şekilde karşılığının olmadığı saptanmıştır. Yanı sıra işlenen ancak kullanılmayan verilerle ne yapılacağı, işlenen konum verilerinin daha sonra yok edilip edilmeyeceği, yok edilecekse ne zaman yok edileceği ve toplanan bu verilerin salgın yönetimine yansımalarının açıklanıp açıklanmayacağı gibi güvene dayalı sorular açısından da metin oldukça yetersiz bulunmuştur. Bilgilendirme kapsamında ayrıca uygulamanın etkili ve güvenli olmasına ilişkin uzman denetiminin olup olmadığı, hangi teknik önlemlerin alındığı, sızma testlerinin yapılıp yapılmadığı gibi sorular açısından da metin yeterli görünmemektedir. Açıklanması gereken bu sorulara ilişkin Sağlık Bakanlığı tarafından herhangi bir açıklamada da bulunulmamıştır. Özellikle olağandışı durumlarda kullanılacak olan temas takip uygulamalarının aydınlatma metinlerinin açık, anlaşılır ve çok daha detaylı olması beklenir. Çünkü olağandışı bir durum söz konusudur ve bu durumda çok daha hassas veriler işlenecektir. Dolayısıyla şeffaflık ve buna bağlı olarak yapılacak doğru bilgilendirme ile uygulamaya olan güven çok önemlidir. Bu nedenlerle uygulamaların aydınlatma metinleri, yukarıda belirtilen

sorulara açıklık getirebilecek bir içeriğe sahip olmalı, aydınlatma metnine eklenemeyen bilgiler ilgili Bakanlık tarafından topluma açıklanmalıdır. Bununla birlikte bireylerin istedikleri zaman onamlarını değiştirebileceği ile ilgili bilginin de metin içinde yer almadığı tespit edilmiştir.

Bunun yanı sıra bilgilendirme tek taraflı olan bir durumdur. Buna göre daha önce de vurgulandığı üzere uygulamalar aracılığı ile alınan tek *–tık* onam, geçerli bir onam değil, rızadır. Hakkıyla alınması gereken Aydınlatılmış onamda, yapılacak doğru bilgilendirmenin yanı sıra bu bilgileri kullanıcıların "anlamasını" sağlamak gerekir. Ancak böylece toplum katılımlı bir aydınlatmadan söz edilebilir.

Aydınlatma kapsamında ret hakkı kullanılabilmeli

Aydınlatılmış onamın geçerli olabilmesi için kişi ret hakkını da kullanabilmelidir. Buna göre kullanıcılar, bir uygulamanın tüm özelliklerini kullanmak zorunda olmadıkları için bazı kişisel verilerinin işlenmesi konusunda ret haklarını kullanabilmelidir.

Aydınlatılmış onam açısından HES uygulamasında saptanan en önemli sorun uygulamaya işlenen konum ve Bluetooth servisi verileri uygulamanın kurulum aşamasında zorunlu olarak kullanıcıdan alınmasıdır. Kullanıcı konum servisine izin vermeden uygulamanın diğer işlevlerini kullanamamaktadır. Alkış & Fındık-Çoşkunçay'ın araştırmasına göre uygulamayı kullanmak istemeyen %11.8 katılımcının %3.3'ü, uygulama konum bilgisine erişim isteğinde bulunulduğu ve bu özelliği aktifleştirmeden uygulamayı kullanmanın mümkün olmadığı için HES'i kullanmak istememektedir (Alkış & Fındık-Coşkunçay, 2021). Uygulamanın bu özelliği, Avrupa Konseyi'nin farklı uygulama işlevleri için kullanıcıdan tek tek onam alınması gerektiği ve onam verilmeyen uygulama özelliklerinin uygulamanın genel kullanımına engel oluşturmaması gerektiği yönündeki görüşüne aykırıdır. Aydınlatılmış onam kapsamında uygulama özellikleri açısından istenmeyen bir özellik için ret hakkı uygulamada kullanılabilir olmalıdır. Bu bağlamda HES uygulamasına zorunlu olarak işlenen konum verisi ve Bluetooth servisi erişim isteklerine karşı kullanıcının ret hakkının korunabilmesi için kullanıcı tarafından uygulamanın bu

özellikleri devre dışı bırakılabilmeli ve kişi uygulamanın diğer özelliklerinden faydalanabilmelidir.

Mahremiyet ve gizliliğin korunabilmesi için HES uygulaması doğru kurulmamıştır

Mahremiyetin korunması özerkliğin sürdürebilmesi için çok önemli bir yere sahiptir. Bu nedenle mahremiyetin ne zaman ihlal edilip edilemeyeceğine kişinin karar vermesi bir kural olarak kabul edilmesi gerekir. Diğer taraftan istisna olarak kabul edilebilecek toplum sağlığı, kamu düzeni ve güvenliği gibi durumlarda kişi mahremiyetinin korunması yerine topluma öncelik verilmesi bu konudaki temel tartışmayı oluşmaktadır. Bu tartışma ise genellikle toplum sağlığı ve korunması gereken bir değer olarak mahremiyet arasında bir dengenin kurulabilir olacağı yönünde aşılmaya çalışılmaktadır. Bunun yanı sıra olağandışı durumlarda toplanan kişisel sağlık verilerinin mahremiyet ve gizliliğini koruyabilmek amacıyla uygulamaların aydınlatma metinlerinde salt bilgi vererek özerkliği ve bağlantılı olarak mahremiyetin korunabileceğini ileri sürmek yanlıştır. Toplanan tüm verinin mahremiyet ve gizliliğini gerçekten korumak ve güvence altına almak gerekir.

Küresel Gizlilik Birliği (GPA) bu konuda bir açıklama yapmış ve kişisel verilerinin işlenebilmesi için kamu yararı gerekçesi güçlü olmakla birlikte mahremiyeti korumak ve toplumun beklentilerine uygun hareket etmeyi çözüme ulaşmanın bir parçası olarak nitelendirmiştir. Bunun yanı sıra veri koruma kurumlarının verilerin gizliliği ve korunması için farkındalık oluşturması ve aktif olarak görev alması gerektiğine vurgu yaparak özellikle temas takip uygulamalarının tasarımda gizlilik ilkesi yaklaşımına uygun olması gerektiğini belirtmiştir (GPA, 2020). GPA'ya göre mahremiyetin değeri, halk sağlığını korumak adına yeni teknolojiler geliştirilirken mahremiyetin dikkatli bir şekilde düşünülmesinde yatmaktadır (GPA, 2020). Tez kapsamında incelenen HES uygulamasının mahremiyet ve gizliliğin korunabilmesi için yeterli özelliklere sahip olmadığı saptanmıştır. Bu saptama, Avrupa Konseyi kılavuzunda belirtilen görüşler ışığında bulunmuştur. Türkiye'de yapılan araştırmalar incelendiğinde de aynı görüş mevcuttur. Buna göre HES uygulamasını kişisel verilerin korunması açısından analiz eden bir çalışmada, uygulama tasarımının gizlilik ilkesine aykırı olduğu ileri sürülmüştür (Çayır, 2020a).

Genellikle dünyada temas takip mobil uygulamaların insanların tanımlanabilmesi ve izlenebilmesi için kullanıcı verilerini merkezi sunucularda depolanması gerekliliği, gizliliğe yönelik en temel endişelerden biri olarak dile getirilmektedir (Zastrow, 2020). Bu konuda Avrupa Konseyi kılavuzu, yakınlık verisi kullanılacaksa bu verilerin kişinin cihazında kalması gerektiğini ileri sürmektedir. HES uygulaması bu bağlamlarda incelendiğinde, uygulamaya işlenen tüm kişisel bilgiler, kullanıcının cihazında kalmamakta ve merkezi bir sistemde depolanmaktadır (Kasapoğlu, 2020). Merkezi sistem, verilerin hükümet kurumlarının doğrudan erişimine ve kontrolüne açabilmek demektir. HES uygulamasının GPS ve konum bilgisi, kamera, rehber, kablosuz bağlantılar ve Google hizmet yapılandırması erişimi ile Bluetooth ayarları gibi erişim sağladığı özellikler dikkate alındığında, mahremiyet ve gizliliğin güvence altında olmadığı ileri sürülebilir. Mahremiyet ve gizlilik açısından endişe veren bir diğer uygulama özelliği, uygulamaya tanımlanan HES kodu uygulamasıdır. Bu kod ile kişinin tüm hareketleri izlenmekte ve kontrol edilmekte, bu kod aracılığı ile HES koduna sahip olan herkes, dilediği gibi HES kodu sorgulaması yaparak başkalarına ait kişisel bilgileri sorgulayabilmektedir. Dolayısıyla HES kodu, özel yaşama müdahale eden bir uygulama olarak karşımıza çıkmaktadır.

Mahremiyet ve gizlilik ile ilgili bir diğer sorun HES uygulamasının bağımsız uzmanlar tarafından denetiminin yapılıp yapılmadığına ilişkin herhangi bir rapor bulunmamasıdır (Çayır, 2020a). Çayır'ın çalışmasında ayrıca, alınan idari, teknik ve hukuki önlemlerin neler olduğunun belirsizliği ve sızma testlerinin yapılıp yapılmadığı gibi gizliliğin korunmasında alınması gereken en temel önlemler hakkında bilgi verilmemesi gibi şeffaflığın söz konusu olmadığı vurgulanmaktadır. Bu konuda Alkış&Fındık-Coşkunçay'ın (2021) araştırmasına göre, HES uygulamasını kullanmak istemeyen katılımcıların (%11.8), uygulamayı kullanmak istememesinin öne çıkan nedeni "HES uygulamasında verilerimin gizli kalacağını düşünmediğim için kullanmıyorum." düşüncesi olmuştur (Alkış & Fındık-Coşkunçay, 2021). Toplumun güveni, salgınla mücadele etmek için oldukça önemlidir.

Avrupa Konseyi kılavuzu, kullanılan uygulamanın her işlevi için bir amaç olması gerektiğini ve işlenen verilerin Covid-19 ile mücadele kapsamı dışında kullanılmaması gerektiğini vurgular (Md.3.5). Buna göre HES uygulamasına işlenen T.C. kimlik

numarası, baba adı ve doğum tarihi, konum, adres, telefon ve sağlık bilgilerinin yanı sıra uygulama aracılığı ile rehberde kayıtlı kişiler, kamera, fotoğraf, video ve Bluetooth gibi çok sayıda bilgi işlenmektedir. Bu bilgilerin işlenmesinde görünen amaç toplum sağlığının korunmasıdır. Ancak toplum sağlığını korumak için hangi bilgilerin gerekli olduğu sorgulandığında, bu kadar ayrıntılı hassas verinin işlenmesinin gerekli olmadığı görüşü savunulabilmektedir.

Tartışmanın ilk bölümünde ileri sürüldüğü üzere verinin işlenebilir olması için amaç toplum yararı olmalı ve bu amaç için gerekli olan veri işlenmelidir. Diğer bir deyişle minimum veri ilkesine uygun olarak veri işlenmelidir. Çünkü işlenen her bir bilgi, mahremiyet ve gizlilik açısından risk oluşturmaktadır. Mahremiyet ve gizliliği koruyabilmenin tek gerçek yolu, verinin işlenmemesidir. Dolayısıyla sağlık hizmetlerinin yürütülebilmesi ve mahremiyet ve gizliliğin korunabilmesi dengesi, minimum veri ilkesi yaklaşımının benimsenmesi ve buna uygun veri işlenmesi ile mümkün görünmektedir. Buna göre Türkiye'de salgın boyunca kişisel sağlık verilerinin işlenmesi gerekliliğinin yeterince temellendirilmediği ve işlenen verilerin minimum düzeyde olmadığı ileri sürülebilir.

Bununla birlikte işlenecek veriler, verilerin daha sonraki kullanımı, veri işlemenin riskleri, kullanılmayacak verilerle ne yapılacağı gibi çok temel sorular hakkında yeterli düzeyde bilgi verilmemiştir. En temel bilgiler verilmediği gibi HES'in Aydınlatma metni incelendiğinde uygulamanın sızma testi bilgisi, aktarılacak bilgiler için şifreleme gibi gizliliğe dayalı bir bilgilendirme de saptanmamıştır.

Dolayısıyla Türkiye'deki salgın yönetiminde aktif bir rol üstlenen HES mobil uygulaması bir bütün olarak değerlendirilecek olursa, mahremiyet ve gizlilik ile toplum yararı dengesinin kurulamadığı ve korunması gereken mahremiyet değerinin harcandığını belirtmek yanlış olmayacaktır.

HES uygulamasının mahremiyet ve gizlilik açısından sorun oluşturan bir başka özelliği uygulamanın "ihbarda bulun" eklentisidir. Buna göre kurallara uymayan kişilerin, fotoğraf ve video görüntüleri uygulama üzerinden paylaşılarak ihbar edilebilmektedir. Buradaki temel sorun, kişilerin onayı olmadan görüntülerinin alınması, ihbarın yalan olabilmesi ve hatta bilerek kötü amaçlarla yapılan bir suçlama olması ile insanları

kutuplaştırabilmesi gibi sorunlar barındırmaktadır. Uygulama kapsamında böyle bir özelliğin salgın yönetiminde etkililiğini sorgulamak gerekir.

Korona Önlem uygulamasına kimlik bilgilerinin işlenmesi gerekli değildir

Korona Önlem uygulaması, Covid-19 ile mücadele kapsamında ön tanı koyan ve kişinin pozitif çıkması durumunda bir sağlık kurumunu ziyaret etmesi gerektiği yönünde tavsiye veren bir mobil uygulama olarak tasarlanmıştır. Buna göre uygulamanın amacı, kişinin Covid-19 pozitif olma durumuna ilişkin ön tanı koymak ve kişiyi bir sağlık kurumuna yönlendirmektir. Bu uygulamanın yanlış tanı koyması ve bu bağlamda kişiyi yanlış yönlendirmesi söz konusu olabilir. Örneğin uygulamanın algoritması özellikle yüksek ateş bilgisine daha çok duyarlıdır. Bu durum uygulamanın etkililiği açısından soru işareti oluşturmaktadır.

Uygulamanın amacı tanı koymak, koyulan tanıya göre tavsiyede bulunmak ve işlenen bilgilerden istatistiki çalışmalar yapmaktır. Bu amaçlar göz önünde bulundurulduğunda, tanı koyabilmek için Covid-19 ile ilgili sağlık bilgileri gereklidir. İstatistiki çalışma yapabilmek için hangi bilgilerin gerekli olduğu sorgulandığında, cinsiyet, yaş, son 14 günde en uzun süre bulunulan il bilgisi ve sağlık sektöründe çalışan biri olup olmadığı bilgilerinin gerekli olduğu belirtilebilir. Buna karşın T.C. kimlik numarası/Yabancı numarası, baba adı, doğum yılı, telefon numarası, adı ve soyadı bilgileri ile IP adres bilgisi gerekli görünmemektedir. Dolayısıyla ön tanı koymayı hedefleyen bir uygulama olarak Korona Önlem uygulamasına bu bilgiler işlenmemelidir.

6. SONUÇ VE ÖNERİLER

6.1.Sonuçlar

Bu tez çalışmasında Büyük sağlık verisi etiği açısından uluslararası etik kılavuzlar temel alınarak sıfır noktasında veriye niçin ihtiyaç duyulduğundan hangi sağlık verisinin toplanması, toplanırken dikkat edilmesi gereken kurallar ve toplandıktan sonra veri güvenliğinin nasıl sağlanabileceğine ilişkin bir sürecin adımlarını oluşturacak şekilde altı ilke belirlenmiştir. Bu ilkeler dikkate alınarak Büyük sağlık verilerinin yaratabileceği etik sorunlarının saptanabilmesi için iki aşamalı soyut bir analiz gerçekleştirilmiştir. Buna göre Türkiye'deki kişisel verilerle ilgili ulusal düzenlemeler ve sağlık veri tabanları incelenmiştir. Bu inceleme sonucunda Türkiye'deki kişisel verileri korumayı amaç edinen temel düzenlemeler ve sağlık hizmetlerinde kullanılan veri tabanlarının toplum yararı, minimum veri, hassas veri, eşitlik ve adalet, özerklik ile mahremiyet ve gizlilik ilkesi ile uyumlu olmadığı sonucuna ulaşılmıştır.

6.1.1. Toplum yararı ilkesi:

Sağlık verisine duyulan ihtiyacın toplum yararı ilkesine göre işlenmesi, verinin niçin gerekli olduğunun bildirilmesi açısından veri toplama eylemine önemli bir sınır çizmektedir. Buna göre temel düzenleme metinlerinde veri toplamanın gerekçeleri sorgulanmıştır. KVK Kanunu başta olmak üzere KSV Yönetmeliği ve ilgili diğer düzenleme maddelerinde veri toplamanın gerekçeleri oldukça yüzeysel ifadelere yer verilerek belirtilmiştir. Bununla birlikte ilgili düzenleme metinlerinde, biyometrik veri gibi çok hassas bir verinin kimlik doğrulama amacı ile işlenebileceği saptanmış ve bu durum toplum yararı ile bağdaştırılamamıştır. Dolayısıyla **ülkemizde bu ilke uyumlu bir veri işleme politikası izlenmemekte, kişisel sağlık verisi işlemenin sınırları toplum yararına göre çizilmemektedir.** Buna ek olarak toplum yararı açısından toplanan verilerin toplum yararına kullanılıp kullanılmadığı, bu verilerin hangi amaçlarla kullanıldığı, işlenen verilerden ne gibi yararlar elde edildiği gibi sorular, veri sorumlusu Sağlık Bakanlığı tarafından yanıtsız bırakılmaktadır. Bu durum **toplumun, veri toplama sürecine dahil edilmediğini gösterirken aynı zamanda kişisel verinin gerçek sahibinin bireyin kendisi olarak görülmediğine işaret etmektedir**. Bu

görüşü temel düzenleme metinlerinde verinin mülkiyetinin bireyin kendisinde olduğunu gösteren bir ifadenin bulunmaması da desteklemektedir.

Toplum yararı ilkesi açısından ulaşılan bir başka sonuç veri kayıt sistemleri ile ilgilidir. Buna göre kişisel sağlık kaydı uygulaması olarak kullanılmakta olan e-Nabız sisteminin halihazırda toplum gereksinimlerine uygun olmadığı sonucuna ulaşılmıştır. Bu nedenle **toplum tarafından uygulamanın daha çok hangi amaçla kullanıldığı veya kullanılmak istendiği araştırılmalıdır**. Beraberinde uygulama, **gereksinime uygun ve amaçla orantılı olacak şekilde kişisel bilgilerin kaydedilebileceği bir tasarıma sahip olmalıdır**. E-Nabıza işlenecek bilgiler doğrudan sağlık durumu ile ilgili bilgiler içermeli ve bilgilerin olası bir ifşası durumunda kişilerin mahremiyetine çok büyük zararlar getirmeyecek olan verilerden oluşmalıdır. Ek olarak e-Nabız uygulamasının içinde ayrı bir program olarak bulunan ***Neyim Var?*** **gibi tanı koyucu nitelikteki bir özelliğin yarar-zarar dengesi iyi kurulmalıdır.**

6.1.2. Minimum veri ilkesi:

Bu ilke kapsamında incelenen ulusal düzenlemelerden özellikle KVK Kanununda ve KSV Yönetmeliği'nde minimum veri ilkesine karşılık gelen, teknik ve ayrıntıları belirleyen bir ifade bulunmamaktadır. Minimum veri ilkesi açısından **gerekli olmayan verilerin işlenmesi durumuna karşılık gelen somut, objektif ve denetlenebilir kurallar içeren bir düzenleme maddesine ihtiyaç bulunmaktadır**. Kanun kapsamında bu ilkeyi yalnızca tanımlamak veya Kurumun rehberine atıfta bulunmak kişisel verinin korunması için yeterli ve gerçekçi değildir. Bu konuda çıkarılan yeni yönetmelik Sağlık Bilgi Yönetim Sistemleri Hakkında Yönetmelik'te bu ilkeye karşılık gelen "minimum veri modeli" kavramının tanımlanmış olması hukuksal boşluğun giderilmesi açısından çok önemlidir. Ancak ifade incelendiğinde veri aktarımını kolaylaştıran bir model tanımlandığı saptanmıştır. Bu yönetmelikte tanımlanan minimum veri modelinin, sağlık verisinin işlenme gerekçelerini açıklayan Ulusal Sağlık Veri Sözlüğünde uygulamayı gösterir bir karşılığı olmalıdır. **Tıp etiği açısından bu sözlüğün amacı, toplum yararı açısından gerekli olan verinin neden toplandığını ayrıntılı bir şekilde açıklamak, kullanılmayan veriler hakkında da bilgi vermek olmalıdır. Böylece veri işleyen hekimler açısından oldukça yol gösterici olacaktır.** Bu sözlük kapsamında **Sağlık Bakanlığı, gerekli olan verinin**

amaca uygun olarak işlenip işlenmediğini ve işlenen verilerin sağlık hizmetlerine nasıl yansıdığını düzenli olarak raporlamalıdır.

KSV Yönetmeliğinde e-Nabız hesabı bulunmayan kişilerin verilerine, sağlık personelinin erişimini düzenleyen 6. maddesinin üçüncü fıkrası bu ilkeye aykırıdır. Bu madde kişinin hastalığı ile doğrudan ilgisi olmayan bilgilere sağlık personelinin erişimine izin vermektedir. **Sağlık personeli de olsa kişilerin diğer sağlık verilerine erişim sağlayabilmesi bu ilke açısından bir ölçüsüzlüktür.**

6.1.3. Hassas veri ilkesi:

Kişisel sağlık verilerinin korunmasını sağlamak, bu türdeki veriye farklı bir yaklaşımı gerekli kılmaktadır. Bu ilkeye göre incelenen düzenlemeler, sağlık verisinin hassas nitelikte olduğunu kabul ederek "özel nitelikli veri" kategorisinde tanımlamaktadır. Buna karşın verinin hassasiyeti, verilerin nasıl kategorize edildiğinden çok, kullanıldıkları bağlama ve diğer bilgilerle, kişilerle, kararlarla ve eylemlerle olan ilişkisine bağlı olduğu göz ardı edilmektedir. Bu bakımdan özellikle **KSV Yönetmeliği'nde bütün sağlık verileri hassas veri niteliğinde kabul edilmeli,** toplum yararı açısından gerekli olan verilerin işlenebilir olması için **toplumun bu sürece dahil edilmesi gerektiği özellikle belirtilmelidir.**

Hassas veri ile ilgili bir diğer önemli sonuç, bu verinin korunmasıyla ilgilidir. Buna göre, KSV Yönetmeliğine kıyasla Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arşiv Hizmetleri Yönergesinde Değişiklik Yapılmasına Dair Yönerge (2007) veri güvenliği açısından daha somut düzenleme maddeleri içermektedir. Ancak bu yönerge de dahil olmak üzere diğer düzenleme maddelerinde, **hassas verinin anonim hale getirilmesi konusunda uygun yöntem belirli değildir.**

Hem düzenleme maddelerinde hem de uygulama alanında hassas verinin diğer verilerle bağlamına göre değerlendirilmemesi ve veriye kategorik bir yaklaşım sergilenmesi, korunması gereken bu veriyi olası tehlikelere karşı savunmasız bırakmaktadır.

6.1.4. Eşitlik ve adalet ilkesi:

Toplumlarda kadınlar, çocuklar, LGBTİ+ bireyler, engelliler, yaşlılar, psikiyatrik desteğe ihtiyaç duyanlar, denekler, tutuklu ve hükümlüler gibi dezavantajlı gruplar vardır. Adaletli bir toplumda, bu kişilerin hassas verilerini daha çok korumak gerekmektedir. Çünkü bu gruplar, ezilen, ayrımcılığa maruz kalan ve ötekileştirilmek gibi sorunlarla baş etmek durumundadırlar. İnceleme kapsamında kişisel veriyi düzenleyen yasal mevzuatımızda bu kişilerin verileri ile ilgili özel bir düzenleme maddesinin olmadığı saptanmıştır. Dolayısıyla **dezavantajlı grupların hassas verilerinin işlenmesi sürecine yönelik hakları, yasal mevzuatta yer almalı ve daha çok görünür olmalıdır.** Eşitlik ve adalet ilkesi açısından dezavantajlı grupların menfaat ve haklarını korumak adına, bu grupların işlenen sağlık verileri hassas veri kategorisinde değerlendirilmelidir.

Bu ilke açısından ulaşılan bir diğer önemli sonuç, veri kayıt sistemlerinin dijital teknolojiye erişimle ilgilidir. Sağlık hakkı kapsamında sağlık veri tabanlarına herkes kendisiyle ilgili bilgilere erişebilir olmalıdır. Bu bağlamda kişisel sağlık kaydı uygulaması olarak kullanılmakta olan **e-Nabız uygulaması, toplumun gereksinimleri ile uyumlu hale getirilmeli, özellikle Covid-19 pandemisi gibi olağandışı durumlarda salgın hastalıklarla hızlı müdahale edebilmeyi sağlayabilmelidir.** Böylece olağandışı durumlarda ayrıca farklı bir uygulama ihtiyacı olmayacak, herhangi bir salgın ile mücadelede kapsamında gerekli donanımlara sahip, herkesin erişebileceği bir uygulama niteliğine sahip olacaktır.

6.1.5. Özerklik ilkesi:

Veri işleme sürecinde korunması gereken bir değer olarak özerklik, günümüz Büyük Veri çağında bu değerin korunmasının gerçekten mümkün olup olmadığı teorik bir tartışma konusudur. Buna karşın sağlık hizmetlerinde belli verilerin toplanmasının artıları dikkate alındığında ve bazı kurallara dikkat edildiğinde özerkliğin sürdürülebileceği önermesi, bu çalışma kapsamında kabul edilmektedir.

Bu bağlamda incelenen düzenleme ve veri kayıt sistemlerinde, kısmi bir özerklik söz konusudur. Diğer bir deyişle kişisel sağlık verisinin yönetimi, tam olarak bireyin kendisinde değildir. Buna göre KVK Kanunu ve KSV Yönetmeliği'nde sağlık verileri

için tanımlanan açık rızaya istisna getirilmesi, aydınlatılmış onam kapsamındaki bilgilendirmelerin yeterli olmaması ve işlenmiş verilerin yurt dışı aktarımlarına ilişkin olarak veri ilgililerinin ret haklarının kullanılabilmesine elverişli olmaması nedenleri başta olmak üzere özerkliğe saygı gösterilmediğini açıkça ortaya koymaktadır. **Özerkliğin korunabilmesi, uygun bir aydınlatılmış onam almaktan geçmektedir**. Aydınlatılmış onam kapsamında incelenen Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ'de yapılan bilgilendirme yeterli olmadığı ve bu metinde veri tabanları açısından onam almanın nasıl gerçekleşeceğinin belirsiz olduğu bulunmuştur. Bu metinde **özerkliğin korunabilmesi için özellikle aydınlatılmış onama kapsamında kişilerin "ret" olanağını kullanabilmesine yönelik bir yükümlülük tanımlamalıdır**. Böylece aydınlatılmış onama dair tanımlanan bu sorunlar, teori düzeyinde de olsa iyileştirilmiş olacaktır. Aydınlatılmış onamın uygulama alanında karşılığı, verinin birinci ve ikinci-üçüncü basamak sağlık hizmetlerinde işlenmesi sürecinde kendini göstermektedir. Buna göre **Hızır AHBS ve MİA MED veri tabanlarına işlenen veriler için hastadan onam alınmalı, onam alındığına yönelik veri tabanları ekranlarına her bir bilgi için "onam alındı" seçeneğine yer verilmelidir.** Bu uygulama halihazırdaki sağlık sistemi içerisinde pratik açıdan uygulanabilir hale geldiğinde Sağlık Bakanlığı bu verileri, toplum yararı amacıyla toplayabilir.

Özerklik ilkesi açısından ilgili düzenlemelerde "tüm sağlık verileri için aydınlatılmış onam alınmalı" kuralı belirgin olmalı, bireyin kişisel sağlık verilerinin işlenmesine izin vermediği durumlarda sağlık hizmetine erişim hakkının engellenemeyeceği açıkça ifade edilmelidir. Bilgilendirme kapsamında gerekli olan tüm bilgiler eksiksiz bir şekilde verilmeli, bunun için gerekli durumlarda veri sorumlusu tarafından yapılacak açıklamalarla toplumun sürece dahil edilmesiyle de sağlanmalıdır. Bilgilendirme yapmanın yanı sıra kişinin anlaması sağlanmalıdır. Böylece gerekli bilgilendirmenin tek taraflı olmasının önüne geçilebilir.

6.1.6. Mahremiyet ve gizlilik ilkesi:

Veri toplamanın son adımı olarak ele alınan mahremiyet ve gizlilik ilkesi açısından ilgili düzenlemeler incelendiğinde, düzenlemelerde bu ilkeye sıklıkla "veri güvenliği" başlığı altında ele alınmakta ve temel düzenlemelerin Kurul'un çıkarmış olduğu

rehbere atıf yapılmaktadır. Kişisel sağlık verisinin tam olarak korunabilmesi için KVK Kanunu başta olmak üzere KSV Yönetmeliği, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik gibi temel düzenlemelerin bu rehbere atıf yapması, mahremiyet ve gizliliğin korunması açısından yeterli değildir. Özellikle KVK Kanunu ve KSV Yönetmeliği'nde veri güvenliğinin nasıl sağlanacağına ilişkin uygulamayı gösterir düzenleme maddelerine ihtiyaç bulunmaktadır. Veri güvenliğini sağlamak üzere çıkarılacak bu kuralların denetlenebilir nitelikte olması, mahremiyet ve gizlilik ilkesinin korunması yönünde bir güvence verebilir.

Mahremiyet ve gizlilik açısından incelenen düzenleme maddelerinde yoruma açık, belirsiz ve muğlak ifadeler bulunmaktadır. Buna karşılık mahremiyeti çok açık ve net bir şekilde düzenleyen metin Hasta Hakları Yönetmeliği'nin 21. ve 23. maddeleridir. Buna göre bu konudaki temel düzenlemeler olan KVK Kanunu ve KSV Yönetmeliği'nin mahremiyet ve gizliliğe yönelik maddelerinin Yönetmeliğin bu iki maddesi ile uyumlu olmalıdır.

Temel düzenleme maddeleri incelendiğinde KVK Kanunu'nun özel nitelikli kişisel verilerin işlenme şartlarını belirten 6. ve 28. maddeleri açık bir şekilde mahremiyete aykırıdır. Bu iki maddenin mahremiyet ve gizliliğin korunabilmesi için yeniden düzenlenmesi gerekmektedir. Bu maddeler, esnek, belirsiz, yoruma dayalı, bireyi kamu otoritelerinin keyfi uygulamalarına karşı savunmasız hale getiren ifadeler olmaları açısından mahremiyet ve gizlilik yönünden güvence sağlamasına engel oluşturabileceği gibi mahremiyete ilişkin riskin kendisini doğurabilir. Mahremiyet ve gizlilik açısından saptanan bir başka sorun, KVK Kanunu ve KSV Yönetmeliği'nin veri aktarımıyla ilgili maddelerine ilişkindir. Kişisel verilerin yurt dışı aktarımına izin veren bu maddeler, yeterli düzeyde bir koruma sağlamamaktadır. Maddelerde belirtilen "yeterli koruma düzeyi" ifadesine karşılık, özellikle yurt dışı aktarım için yeterli koruma düzeyini belirlemenin her zaman mümkün olmayacağını belirtmek gerekir. Bu nedenle veri aktarımı ile ilgili koruma düzeyi açısından daha ayrıntılı düzenleme maddelerine ihtiyaç bulunmaktadır.

Bununla birlikte temel düzenleme metinlerinde bazı kavramsal tanımlamalar yanlıştır. Buna göre, özellikle Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale

Getirilmesi Hakkında Yönetmelik'teki "anonimleştirme" kavramına ilişkin aynı düzenleme içerisinde farklı biçimlerde tanımlamalar yapılmış veya açıklanması gerekli olan tanımların yan anlamları kullanılmıştır. Bu durum düzenleme maddesini yoruma açık hale getirir. Kavramı doğru tanımlamak her zaman yeterli de olmayabilir. Açıklanan kavram bir yöntem gerektiriyorsa, uygun olan yöntem veya yöntemler de ilgili düzenlemelerde belirtilmelidir. Buna göre **verinin korunabilmesi için anonimleştirme kavramına ilişkin belirsizlikler giderilmeli ve anonimleştirmeyle ilgili kullanılacak yöntem veya yöntemlere ilişkin standart olabilecek güvenilir yazılım veya programlar açıklanmalıdır.** Ayrıca anonimleştirmenin literatürdeki çalışmalardan da hareketle teknik olarak mahremiyet ve gizliliğin korunabilmesi için yeterli bir yöntem olarak nitelendirilemeyeceğini göz önünde bulundurmak gerekir.

Mahremiyet ve gizlilik ilkesi kapsamında değerlendirilen Hızır AHBS ve MİA MED uygulamalarına hekim tarafından işlenen kişisel sağlık bilgilerinin hastanın onamı dışında ve Sağlık Bakanlığına gönderme zorunluluğu karşısında hekimin mesleki gizlilik ilkesine verilen yüksek değerin göz ardı edilmesine sebep olunduğu sonucuna ulaşılmıştır. Mesleki gizlilik, hekimlik mesleğinde güvene dayalı ilişkinin var olabilmesi ve sürdürülebilmesinde çok yüksek bir değeri ifade etmektedir. **Dolayısıyla hekimlerin mesleki gizliliği çiğneyecek durumda bırakan ve veri gönderimini zorunlu tutan bu uygulama meslek ahlakı açısından kabul edilemez.**

Dijital dünyada mahremiyeti korumak çok güçtür ancak bazı kurallar çerçevesinde imkansız değildir. Buna göre **ülkemizde kişisel verilerle ilgili mevzuatın ve veri tabanlarında saptanan sorunların bu çalışma kapsamında belirtilen ilkelerle uyumlu hale getirilmesi, gelecekte özellikle Büyük Veri analizinin ortaya çıkarabileceği tehlikelere karşı yol gösterici olacaktır.** Bu bağlamda **sağlık verisi toplum yararı amacıyla, gerektiği kadar, eşit ve adil bir şekilde, insanların özerklik haklarını koruyarak toplanmalı, mahremiyet ve gizlilik açısından gerekli tüm önlemler alınmalı ve güvenceler sağlanmalıdır**. Mahremiyet ve gizliliği korumak için uygulama alanında veri tabanlarının intranet sistemler olmasına, bağımsız firmalar aracılığı ile veri sızıntı testlerinin yapılmasına ilişkin gerekliliklere veri güvenliğini düzenleyen metinlerin ilgili maddelerinde yer verilmelidir.

6.1.7. Mobil uygulamalarla ilgili sonuçlar

Olağandışı durumlar açısından ele alınan HES ve Korona Önlem mobil uygulamaları, Avrupa Konseyi kılavuzuna göre incelenmiş ve HES uygulamasının birçok özelliğinin bu kılavuz metni ile uyumlu olmadığı belirlenmiştir. Buna göre Sağlık Bakanlığı, salgın döneminde uygulamaya soktuğu HES uygulaması ile toplum sağlığını korumayı amaçlamış ancak halk sağlığı ile mahremiyet ve özerklik arasında orantısız bir denge kurarak korunması gereken bu değerleri göz ardı etmiştir. Özellikle salgın yönetiminde uygulanan **HES kodu uygulaması, temel özgürlükleri kısıtlayan ve Covid-19 hastalığına ilişkin kişisel bilgilerin bu kod aracılığı ile herkes tarafından sorgulanabilir olması, mahremiyet hakkının açıkça ihlal edildiğini göstermektedir.**

Mobil uygulamalarla ilgili ulaşılan bir diğer önemli sonuç, uygulamaların aydınlatma metinlerinde tüm bilgilerin eksiksiz bir şekilde verilmediğidir. Özellikle olağandışı durumlarda şeffaflık çok önemli bir yerdedir. Bu bakımdan yapılacak bilgilendirmeler, detaylı ve sürekli olmalıdır. Aydınlatma kapsamında kullanıcılar ret haklarını kullanabilmelidir. HES uygulamasında olduğu gibi uygulamaların aydınlatma metinlerinde hangi bilgilerin toplanacağı, kimlerle paylaşılacağı vs. gibi konularda salt bilgi vermek, mahremiyet ve gizliliği korumak için yeterli değildir. **Toplanan tüm verinin mahremiyet ve gizliliğini gerçekten korumak ve güvence altına almak gerekir.** Bu hem kişisel verilerle ilgili temel düzenlemelerle uygulanacak yaptırımlarla hem de mobil uygulamaların şifrelenmesi, sızma testleri, denetim vs. gibi gizlilikle ilgili konulardaki bilgilendirmelerle mümkündür.

HES uygulaması ile ilgili bir başka önemli sonuç uygulamaya işlenen bilgilerle ilgilidir. Buna göre uygulamaya T.C. kimlik numarası, baba adı ve doğum tarihi, konum, adres, telefon, sağlık bilgileri, rehberde kayıtlı kişiler, kamera, fotoğraf, video, konum ve Bluetooth erişimi olmak üzere çok hassas düzeydeki verilerin hepsi aynı anda işlenmektedir. **Tez kapsamında yapılan sorgulama ile bu bilgilerin gerçekten halk sağlığı açısından öncelikli olmadığı sonucuna ulaşılmıştır.** Gerekli olmayan verinin işlendiği bir diğer uygulama, tez kapsamında incelenen Korona Önlem uygulamasıdır. Uygulamanın amacı tanı koymak, koyulan tanıya göre tavsiyede bulunmak ve işlenen bilgilerden istatistiki çalışmalar yapmaktır. Bu amaçlar göz

önünde bulundurulduğunda, tanı koyabilmek için Covid-19 ile ilgili sağlık bilgileri gereklidir. İstatistiki çalışma yapabilmek için kişilerin kimlik bilgileri, iletişim bilgileri ve IP adresleri gerekli görünmemektedir.

6.2.Öneriler

Tezin bu son bölümünde saptanan sorunlar ışığında, kişisel veri ile ilgili temel düzenleme maddelerinin nasıl geliştirilebileceği, hangi maddenin nasıl ifade edilmesi gerektiği, kanun ve yönetmelik kapsamında hangi kurallar ve tanımlara yer verilebileceği ve halihazırda işlenen sağlık verilerine yönelik öneriler geliştirilmiştir. Bununla birlikte sağlık hizmetleri kapsamında kullanılan sağlık veri tabanları ve olağandışı durumlar açısından incelenen mobil uygulamaların geliştirilmesi yönünde önerilerde bulunulmuştur.

6.2.1. Temel düzenleme ve veri tabanlarının geliştirilmesine yönelik öneriler:

Toplum yararı ilkesi açısından: Toplum yararı ilkesi sağlık verisinin işlenmesine önemli bir sınır çizmektedir. Bu sınırın temel düzenleme maddelerinde görünür olması gerekir. Bu nedenle Kişisel Verileri Koruma Kanun'unda istisnaları belirten 28. maddenin çok genel söylemlerine karşılık bu madde, sağlık verilerinin önemine vurgu yapmalıdır. Beraberinde bu maddeye sağlık verilerinin işlenebilmesi için tek koşulun **"sağlık verisinin toplum yararı açısından seçeneksiz bir biçimde işlenmesi gerektiği"** biçiminde bir ifadeye yer verilebilir.

Hassasiyet düzeyi oldukça yüksek olan parmak izi, avuç izi tanıma, damar izi tanıma, yüz tanıma, iris ve retina tanıma, ses tanıma ve imza/el yazısı tanıma gibi biyometrik verilerin "kamu düzeni", "güvenlik", "ekonomik güvenlik" ve "milli savunma" gibi gerekçelerle işlenmesi yasaklanmalıdır. Buna göre biyometrik verinin kanun düzeyinde toplanabileceğini bildiren Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun 67. maddesine "…biyometrik yöntemlerle kimlik doğrulamasının yapılması…" gibi verinin işlenebileceğine işaret eden bir ifade kanun maddesinden çıkarılmalıdır. **Biyometrik veriye, özel nitelikli veri kategorisinde ayrıntılı bir şekilde yer verilmeli, içeriği KVK Kanunu kapsamında ayrıntılı bir şekilde tanımlanmalı ve bu verinin işlenmesi kati bir şekilde yasaklanmalıdır.** Buna göre

kanunun 6. maddesine GDPR'ın tanımı alınarak kanun maddesi yeniden düzenlenmelidir. Buna göre GDPR'ın 4. maddesi biyometrik veriyi şu şekilde tanımlanmıştır; **"yüz görüntüleri veya daktiloskopi (parmak izine dayanarak kimlik belirleme) veriler gibi bir gerçek kişinin özgün bir şekilde teşhis edilmesini sağlayan veya teyit eden fiziksel, fizyolojik (parmak izi, retina, avuç içi, yüzü, el şekli, irisi vs.) veya davranışsal (kişinin yürüyüşü, araba sürüş şekli, klavye kullanış biçimi vs.) özelliklerine ilişkin olarak spesifik teknik işlemeden kaynaklanan kişisel verilerdir."** Bu tanım paralelinde diğer ilgili kanun ve yönetmelikler, biyometrik veriyle ilgili ayrıntılı bir şekilde düzenlenmeli ve ilgili maddeler birbiri ile uyumlu hale getirilmelidir. Bununla birlikte Türkiye'de uygulamaya geçilen yeni kimlik kartı uygulaması ile işlenen parmak izlerinin niçin toplandığı ve işlenen bu verinin nasıl korunacağı açıklanmalıdır.

Toplum yararı ilkesi açısından e-Nabız uygulamasının hangi sağlık gereksinimi için kullanılmak istendiği daha fazla araştırılmalıdır. Uygulamanın amacı toplum yararına göre belirlenmeli ve bu amaçla orantılı olacak şekilde verilerin kaydedilebildiği bir sistem tasarlanmalıdır. Böylece toplum katılımlı ve kişilik haklarına saygılı bir kişisel sağlık kayıt sistemi inşa edilmiş olacak ve uygulamanın yaygın olarak kullanılabilmesi söz konusu olacaktır.

Minimum veri ilkesi açısından: Veri işlemenin sınırını bir kural olarak belirleyen minimum veri ilkesi, temel düzenleme maddelerinde yeterince görünür değildir. Bu nedenle KVK Kanunu'nun "tanımlar" başlığı altında bu ilke; **"Kişisel veri işlendiği amaçla bağlantılı, sınırlı ve ölçülü olmalıdır."** biçiminde tanımlanmalıdır. KSV Yönetmeliği'nde ise tamamlayıcı bir ifade olarak **"Minimum veri işleme: Kişisel verilerin işlenmesi gerekliliğinin ve bu kişisel verilerin uygunluğunun değerlendirilmesi, belirlenen amaç(lar) ışığında yapılmalıdır."** biçiminde yer almalıdır. Böylece kanunda temel bir tanım yapılırken yönetmelikte sağlık verisi açısından daha özel bir sınır çizilmiş olacaktır. Bununla birlikte minimum veri ilkesi, Sağlık Bakanlığı'nın Ulusal Sağlık Veri Sözlüğünde ayrıca yer verilmelidir. Bununla birlikte bu sözlük ile açıklanan verilerin toplanma gerekçeleri, uygulama alanında karşılık bulmalıdır. Buna göre tez kapsamında incelenen e-Nabız, Hızır AHBS ve MİA MED veri tabanlarına sınırsız sayıda sağlık verisi yarı yapılandırılmış bir şekilde

işlenmektedir. Bu veri tabanları, bu sözlükte tanımlanan veri toplama gerekçeleri ile uyumlu bir tasarıma sahip olmalıdır. **Özellikle e-Nabız kişisel sağlık kaydı uygulaması, bütün kişisel bilgilerin kayıtlı olduğu bir veri tabanı olarak değil, uygulama hangi sağlık gereksinimi için kullanılacaksa bu yönde bir veri işlemesi yapılabilmelidir.**

Hassas veri ilkesi açısından: Hassas veriyi Kişisel Verileri Koruma Kanunun 6. maddesi "özel nitelikli kişisel veri" başlığı altında veriyi kategorik bir yaklaşımla tanımlamıştır. Veriyi kategorik bir yaklaşım ile tanımlamak, veriyi bağlamına göre değerlendirmemektir. Bu bağlamda örneğin cinsel hayatla ilgili verilerin bazen hassas olmayabileceği anlamı çıkarılabilmekte, bu da kanun maddesini yoruma açık hale getirmektedir. Bu nedenle maddeye **"ad, soyad, doğum tarihi ve doğum yeri gibi bireyin kimliğini ortaya koyan bilgilerinin yanı sıra telefon numarası, adres, sosyal güvenlik numarası, görüntü, ses kayıtları, DNA, parmak izi, saç, tükürük, tırnak gibi biyolojik örnekleri, e-posta adresi, IP adresi, sosyal medya hesapları"** bilgileri eklenerek kapsamı genişletilmelidir. Yanı sıra 6. maddenin birinci fıkrasında **"Verinin özel nitelikli olup olmadığı ayrıca bağlamına göre de değerlendirilmelidir"** ifadesine yer verilmelidir. Bazı verilerin hassasiyet düzeyi daha yüksektir. Bu nedenle **genetik veriler ve biyometrik verilerin işlenmesi KVK Kanunu kapsamında yasaklanmalı**, bu verilerin hassasiyet düzeyi, KSV Yönetmeliğinde daha ayrıntılı olarak düzenlenerek toplum yararı açısından gerektiği durumlarda toplanacak olan bu verilere nasıl davranılması gerektiği de açıklanmalıdır. Bu konuda **Sağlık Bakanlığı'nın çıkardığı Genetik Veri Paylaşımı isimli genelgede belirtilen "genetik verilerin yurt içinde depolanacağı, uluslararası veri bankalarına eklenmeyeceği ve kontrollü ya da kamusal erişime açılmayacağı" ifadelerine "biyometrik veriler" de dahil edilerek KSV Yönetmeliğine eklenmelidir.** Toplum yararı açısından mutlaka gerekli olan hassas verinin kullanımı konusunda sınırlı yetkiler vermeli, veri sahiplerinin ise hangi bilgilerinin toplanacağı hakkında bilgilendirilmesi ve sürece katılımlarının sağlanması yönündeki yaklaşım düzenlenecek maddelerde mutlaka belirtilmelidir.

Hassas veri ile ilgili düzenlemelerde saptanan bir diğer sorun hassas verinin güvenliğinin sağlanmasına yöneliktir. Bu bağlamda **KSV Yönetmeliği'nin hassas**

verinin güvenliğini düzenleyen 6, 12, 17, 18, 19 ve 20. maddelerinin yeniden düzenlenmesi önerilmektedir. Bu maddelerde hassas verinin korunması için belirtilen yöntemler, yeterli ve somut önlemler ikincil düzenlemelere bırakılmıştır, açık uçlu ve belirsiz ifadelere yer verilmiştir. Dolayısıyla veri güvenliği konusunda risk oluşturmaktadırlar.

Düzenleme maddelerinde saptanan bir diğer sorun, "anonim hale getirme", "imha edilme", "periyodik imha işlemi" ve "veri saklama" kavramlarının ilgili yönetmelik maddelerinde belirsiz ve içerikle uyumlu olmayacak şekilde tanımlanmasıdır. Bu nedenle **KSV Yönetmeliğinin 4. maddesinin verilerin imha edilmesini tanımlayan k fıkrasından "anonim hale getirme"** ifadesi çıkarılmalıdır. **Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik'te imha kavramını tanımlayan 4. maddenin c fıkrasından ve "periyodik imha" yı tanımlayan ğ fıkrasından"… veya anonim hale getirme"** ifadesi çıkarılmalıdır. Böylece anonim hale getirme ve imha etme kavramları daha belirgin hale gelecektir. Bununla birlikte Kişisel Verilerin Silinmesi, Yok Edilmesi Veya Anonim Hale Getirilmesi Hakkında Yönetmelik kapsamında anonim hale getirme yöntemleri (maskeleme, toplulaştırma, veri türetme ve veri karması) belirtilerek, veri güvenliği açısından önceden test edilmiş bir anonimleştirme modelinin kullanılması gerektiği yönünde bir ifadeye yer verilebilir.

Eşitlik ve adalet ilkesi açısından: Toplum yararı açısından gerekli olan kişisel sağlık verisi eşit ve adil bir şekilde toplanmalıdır. Buna göre eşitlik ve adalet ilkesi açısından **dezavantajlı gruplarla ilgili özel bir düzenleme maddesine ihtiyaç bulunmaktadır**. Buna göre kadınlar, LGBTQ+ bireyler, engelli bireyler, yaşlılar ve psikiyatrik desteğe ihtiyaç duyan bireylerin, toplumda şiddet gören, savunmasız, ezilen, ötekileştirilen, damgalanan ve ayrımcılığa uğrayan bir kesimi oluşturmaları nedeniyle bu gruptaki bireylerin kişisel sağlık verileri yasalar tarafından daha hassas düzeyde korunması gerekir. Buna göre **KVK Kanunu'nda ve KSV Yönetmeliği'nde dezavantajlı gruplar görünür olmalı**dır.

Eşitlik ve adalet ilkesi açısından bir diğer önemli sorun veri tabanlarına erişim sorunudur. Bu konuda e-Nabız, ülkemizdeki ulusal kişisel sağlık kaydı uygulaması olarak kullanılan tek uygulama olduğu için uygulamayı kullanmak isteyen her birey,

e-Nabızdan faydalanabilmelidir. Bu bağlamda kişilerin sosyoekonomik durumları ve coğrafi koşullar uygun hale getirilmeli, uygulama internet bağlantısı olmadan da çalışabilmelidir. Ayrıca uygulamaya görme engelli kullanıcılar için sesli yanıt eklenmesi gibi bazı dezavantajlı kullanıcılara yönelik uygulamayı kolaylaştırıcı özellikler geliştirilmelidir. Bununla birlikte e-Nabız uygulamasının okur-yazar olmayanlar, düşük gelirli gruplar ve yaşlılar için yaratabileceği zorluklar araştırılmalı, özellikle sağlık hizmetlerine erişimde yaşanabilecek sorunlara karşı önlemler geliştirilmelidir.

Özerklik ilkesi açısından: Toplum yararı açısından gerekli olan kişisel sağlık verisi aynı zamanda özerkliğe zarar vermeden toplanmalıdır. Karar verme yeterliğine sahip her birey, kişisel verinin işlenmesi, veriye erişim, verinin kullanımı ile veri kayıt sistemlerinde kayıtlı bilgileri silme, düzeltme, erişim ve devre dışı bırakabilme gibi hakları güvence altına alınmalıdır.

Bu ilke ile uyumlu bulunmayan KVK Kanunun 6. maddesi, hassas nitelikli verilerin toplum yararı amacıyla "sır saklama yükümlülüğü altında bulunan kişiler veya yetkili kurum ve kuruluşlar tarafından açık rıza aranmaksızın işlenebileceği" yönündeki ifadede belirtilen "yetkili kurum ve kuruluşların" kimler olduğu açık değildir. Dolayısıyla bu belirsiz ifade yeterli bir bilgilendirme sağlamamaktadır. **Bilgilendirme kapsamında hangi kurum ve kuruluşların bu bilgilere erişim sağlayabileceği açık ve net bir şekilde belirtilmelidir.** Benzer biçimde **Kanunun Md.12, Md.18, Md.19 ve Md.20 maddelerinin gizliliğin nasıl sağlanacağı, hangi koşullarda aktarım yapılacağı, yurt dışına aktarımın koşullarının neler olacağı, verilerin depolanması ve kullanımındaki risklerin neler olabileceği gibi konularda bilgilendirme yapmalıdır.** Bununla birlikte verilerin yurt içi aktarımı ve yurt dışı aktarımı açısından farklı riskler ortaya çıkabilir. Özerklik açısından kişi verilerinin yurt içi aktarıma izin verirken yurt dışına aktarılmasına izin vermek istemeyebilir. Bu durumda **kanun, kişinin bu hakkını kullanabilmesine elverişli olmalıdır. Özerklik ilkesi kapsamında kişinin ret hakkının da bulunduğu göz ardı edilmemelidir.**

Özerklik ilkesinin korunabilmesinin koşullarından biri geçerli bir aydınlatılmış onamdır. Bu konuda çıkarılan **Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliği'nde yapılan**

bilgilendirmenin kapsamı, verinin kullanımındaki riskler ve yükler, gizliliğin nasıl sağlandığı/korunduğu ve verinin varsa ticari kullanımı konularında genişletilmelidir. Bununla birlikte **kişinin "ret" olanağını kullanabilmesine ilişkin olanak bu tebliğde de tanımlanmalıdır.**

Günümüz dijital teknolojisi ile toplanan kişisel veriler ile bireylerin somut olarak takip edilmeleri değil, Büyük Veri analizi ile bireylerin soyutlanmış hakikat parçacıklarının ortaya çıkması gibi çok daha öte bir sorun söz konusudur. Dolayısıyla verinin işlenmesiyle ilgili risklerin boyutu dikkate alındığında, toplumu bilgilendirmek her zamankinden çok daha önemli bir yerdedir. Bu nedenle **hangi veriye niçin ihtiyaç duyulduğu bilgisinden, işlenen veriye ilişkin olası riskler bütün yönleri ile açıklanmalıdır. Sadece bilgi vermek de yeterli değildir, aydınlatılmış onam kişinin anlamasını sağlamayı da içermektedir. Dolayısıyla ilgili düzenleme maddelerinde onamı alacak sağlık çalışanlarına bu yönde bir yükümlülük tanımlanmalıdır.**

Özerklik ilkesi kapsamında sorunlu görülen bir diğer düzenleme, Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik'tir. Yönetmeliğin verilerin silinmesi (Md.8), yok edilmesi (Md.9) ve anonim hale getirilmesini (Md.10) düzenleyen maddelerinde, birey kendi verisinin yönetiminde pasif kalmaktadır. Bu durum özellikle kişisel sağlık kaydı uygulamasının yönetiminde önemli bir sorun oluşturmaktadır. **Özerklik ilkesi açısından kişinin, e-Nabız kaydından veri silebilmek için veri sorumlusu olarak Sağlık Bakanlığı'na başvuru yapılmasına gerek olmamalıdır.** Kişi istediği zaman özellikle silme işlemini yapabilmelidir. Dolayısıyla kişinin kendi verisinin yönetimine aktif olarak katılabilmesi sağlanmalıdır. Bununla birlikte ilgili düzenleme maddelerinde yer alan "açık rıza" ifadesi, doğru terminoloji açısından tüm düzenleme metinlerinde "aydınlatılmış onam" ifadesi biçiminde düzenlenmelidir.

Mahremiyet ve gizlilik ilkesi açısından: Sağlıkta dijitalleşmenin arttığı günümüz dünyasında sağlık verilerinin mahremiyet ve gizliliğini korumak giderek güçleşmektedir. Bu nedenle verinin işlenmesi sürecinin en başından itibaren mahremiyet ve gizliliğin korunmasına yönelik kurallar temel kanun ve yönetmeliklerde açık ve belirli olmalı, uygulama alnında bu kurallar teori düzeyinde

kalmamalıdır. Buna göre, ilgili düzenleme metinlerinde veri güvenliğinin sağlanması için uyulması gereken somut ve uygulanabilir kurallara yer verilmelidir. Diğer ilkeler kapsamında belirtilen sorunlar, mahremiyet ve gizlilik ilkesi açısından da değerlendirmek mümkündür. Bu ilke kapsamında özetle temel düzenlemelerin somut, objektif ve denetlenebilir kurallardan oluşturulması adına düzenlemelerin yeniden düzenlenmesi önerilmektedir. Bu bağlamda Mahremiyet ve Gizlilik ilkesinin gerçekten korunabileceği düzenlemenin Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arşiv Hizmetleri Yönergesinde Değişiklik Yapılmasına Dair Yönerge olduğunu vurgulamak gerekir. Bu yönerge, KSV Yönetmeliği'ne göre daha sistemli ve kuralları daha açık ve nettir. Dolayısıyla mahremiyetin korunabilmesi için bu yönergenin Yönetmelik düzeyinde ele alınması önerilmektedir.

Temel düzenleme maddelerinde mahremiyet ve gizlilik açısından saptanan bir diğer sorun bu düzenlemelerin üçüncü taraflarla veri paylaşımının önünü açabilme potansiyeli taşımasıdır. Buna göre verilerin yurt içi ve yurt dışı paylaşımını düzenleyen KVK Kanunu'nun 9. maddesi ile verilerin yurt dışı paylaşımını düzenleyen KSV Yönetmeliği'nin 15. maddesi mahremiyet ve gizlilik açısından yeterli düzeyde bir güvence sağlamamaktadır. Bu maddelerdeki **"kişinin açık rızası aranmaksızın verilerin yurtdışına aktarılabileceği" ifadesi yerine "kişinin aydınlatılmış onamı alınmadan verilerin yurtdışına aktarılamayacağı" ifadesi getirilmelidir.** Bununla birlikte **kanun maddesinde belirsiz olan "yeterli önlemler" ifadesi daha açık hale getirilmelidir. Kişinin sağlık verilerinin yurt içi aktarımına izin verebileceği, ancak yurtdışı aktarıma izin vermeyeceği seçeneğinin kullanılabilir olması hakkı, kanun kapsamında tanınmalıdır.** Söz konusu yurtiçi paylaşım için de kişilerin ayrıca onamı alınmalıdır. Çünkü veri işleyen kurum açısından potansiyel riskler farklı olabilir. Sosyal Güvenlik Kurumu Kanunu'nun bilgilerin kurumlar arası paylaşılmasını düzenleyen 35. maddesi Aydınlatılmış Onam kapsamında yeniden düzenlenmelidir.

Son olarak mahremiyet ve gizlilikle ilkesi ile ilgili **hekimlere yönelik öneriler geliştirilmiştir.** Mevcut durumda hekimler, meslek ahlakının temelinde bulunan mahremiyeti koruma hakkı ile yasal zorunluluk nedeniyle verileri onam almadan Sağlık Bakanlığına gönderme zorunluluğu çatışmasını yaşamaktadırlar. Bu durumda

hekimler, tıp etiğinin temel değeri olan mesleki gizliliğin ihlaline yönelik Sağlık Bakanlığı uygulamalarını eleştirel değerlendirmeli, Bakanlığın veri toplama gerekçelerini öğrenmeli ve bu gerekçelerin ahlaki açıdan haklı çıkarılıp çıkarılamayacağını sorgulamalıdır.

Hekimler sağlık verisinin nasıl toplandığı, hastaların özerkliğine ve mahremiyetlerine saygı gösterilip gösterilmediği, paylaşımı gerçekleşecek bilgilerin mahremiyetinin ihlal edildiğinde ortaya çıkarabileceği zararların büyüklüğü ve bu zararların telafisinin mümkün olup olmadığı gibi sorgulamalarla bir karar vermelidir. Yapılan değerlendirmelerin ardından yasal gerekliliklere uymaya karar vermişlerse bu kararı uygulamadan önce bunun gereklilikleri konusunda hastalarını aydınlatmalıdır. Kişisel verilerin işlenmesinde hekimlerin aydınlatma yükümlülükleri vardır. Böylece hekimler, kendilerine ve dolayısıyla tıbba olan güveni koruyabilirler. Bununla birlikte özellikle biyometrik veri gibi hassasiyet düzeyi çok yüksek veriler toplanmak istendiğinde ve yasal gereklilikler buna göre oluşturulduğunda da aynı değerlendirmeyi yapmalı, biyometrik verinin toplum yararı açısından seçeneksiz bir biçimde gerekli olup olmadığını sorgulamalıdır. Özellikle **Büyük Veri çağında hekim mahremiyete yönelik risklerin farkında olmalı ve mesleki gizlilik ilkesine biçilen yüksek değeri korumalı**dır.

6.2.2. Mobil uygulamaların geliştirilmesine yönelik öneriler

Olağandışı durumlar açısından incelenen HES ve Korona Önlem mobil uygulamalarının Avrupa Konseyi kılavuzu ile uyumlu hale getirilebilmesi için aşağıdaki şekilde öneriler geliştirilmiştir.

- Temas takip uygulaması olarak kullanılan HES uygulaması, konum verilerini işlememeli, **toplum yararı açısından konum verisi gerekli olduğunda ise aydınlatılmış onam alınarak veri işlenmelidir.**
- **Konum verisi kişisel bilgilerden arındırılarak işlenmeli**, öncelikli olarak hareket verilerinden yararlanılmalıdır.
- Uygulamaya işlenen kimlik verisi, baba adı, doğum tarihi, adres, telefon, konum verisi, sağlık verisi, meslek verisi, Bluetooth verisi, kamera verisi, kişi listesi verisi

ve dosya (video/ses/görüntü) verilerinden **sadece Covid-19 ile ilgili sağlık verisi aydınlatılmış onam alınarak işlenebilir olmalıdır.**

- HES uygulamasının aydınlatma metninde bilgilendirmenin kapsamı genişletilmelidir. Buna göre **bilgilerin salgın süresi boyunca saklanacağı, salgının kontrol altına alınmasıyla işlenen bilgilerin yok edileceği, kullanıcının kendi verilerini silebileceği, verilerin yurt içine ve yurt dışına aktarılmayacağı, kullanıcının dilerse onamını değiştirebileceği ve uygulamanın etkili ve güvenli olduğuna yönelik uzman denetiminin yapıldığı** bilgileri eklenmelidir.
- Temas takip uygulamaları için yapılan tüm değişiklikler veri sorumlusu Sağlık Bakanlığı tarafından sürekli olarak kamuya açıklanmalıdır.
- Uygulamaya **işlenecek olan veriler için ayrı ayrı onam alınmalıdır**. Buna göre konum verisi için ayrı, Bluetooth verisi için ayrı onamlar alınmalıdır. Kullanıcı, uygulamanın bu özelliklerini devre dışı bırakabilmeli ve uygulamanın diğer özelliklerinden faydalanabilmelidir.
- Mahremiyet ve gizlilik açısından **kullanıcı verileri kişinin cihazında kalmalıdır.**
- **Uygulamadan "ihbarda bulun" özelliği kaldırılmalıdır.**
- Korona Önlem uygulamasına, kimlik bilgileri işlenmemelidir.

Sonuç olarak Sağlıkta Büyük Veriyle, sağlık verilerinin mahremiyet ve gizliliğini korumak giderek güçleşmekte, ortaya çıkabilecek etik sorunlar çeşitlenmektedir. Bu tez kapsamında etik kılavuzlar ışığında belirli bir yol izlenerek belirlenen ilkeler, ortaya çıkabilecek sorunların çözümlenmesine ve önlenmesine hitap etmekte ve sağlık veri tabanlarına bağlı olarak pratikte karşılaşılan sorunlarla başa çıkabilme yolları sağlamaktadır. Bu ilkeler geliştirilmeye ve tartışmaya açıktır. Teknolojik gelişmeye bağlı olarak gelişen veri toplama yöntemlerine ayak uydurabilmek için bu ilkeler daha ileri boyutlara taşınmalıdır. Ülkemizde halihazırda veri işleme sürecine dair standart pozisyonun ve kişisel verileri korumayı amaçlayan temel düzenlemelerin bu ilkelerle uyumlu olmadığı bu tez ile gösterilmeye çalışılmıştır. Bu bulgudan hareketle yasal düzenlemelerin ve veri tabanlarının pratikte karşılığı bulunan bu ilkelere uygun hale getirilmesi gerektiği yasa koyucuların bir ödevi olarak savunulmaktadır.

7. KAYNAKLAR

Aile Hekimliği Uygulama Yönetmeliği, (25 Ocak, 2013). *Resmi Gazete* (Sayı: 28539). Erişim adresi:https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=17051&MevzuatTur=7&MevzuatTertip=5

Akgül, A. (2015). Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı. *TTB Dergisi, 118*. http://ab.org.tr/ab09/kitap/samli_yuksel_AB09.

Akkurt, S. S. (2020). Kişisel Veri Kavramının Hukuki Niteliğine İlişkin Yaklaşımlara Mukayeseli Bir Bakış. *Kişisel Verileri Koruma Dergisi, 2*(1). www.kvkk.gov.tr

Alkış, N., & Fındık-Coşkunçay, D. (2021). Covid-19 Salgınında Hayat Eve Sığar (HES) Uygulamasının Kullanıcılar Tarafından Benimsenmesi: Ampirik Bir Çalışma. *Bilişim Teknolojileri Dergisi*, *14*(4), 367–376. https://doi.org/10.17671/gazibtd.883789

Altan, S. (2018). Çin'in Distopik Sosyal Kredi Sistemi, Kısmen Hayata Geçti, (2021, 3 Ağustos).Erişim adresi:https://pazarlamasyon.com/cinin-distopik-sosyal-kredi-sistemi-kismen-hayata-gecti/

Altınbaş, A. (2018). Sağlıkta büyük verinin önemi. *Ortadoğu Tıp Dergisi*, *10*(2), 216–219. https://doi.org/10.21601/ortadogutipdergisi.412200

Altındiş, S., & Kıran Morkoç, İ. (2018). Sağlık Hizmetlerinde Büyük Veri. *Ömer Halisdemir Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *11*(2), 257–271. https://doi.org/10.25287/ohuiibf.366227

Ankaralı, H. (2020). Büyük Verinin Anlamlandırılmasında Kullanılan Metodolojiler. içinde (s.37-62), *Sağlık Alanında Büyük Veri*. İstanbul:İsar Yayınları.

AÖF. (2021). *Bilgi Sistemlerine Giriş: Temel Kavramlar*. Erişim adresi:https://netsorular.com/ataturk-universitesi-yonetim-bilisim-sistemleri-ders-ozeti-konusu-269.html

Arslan Hızal, S. (2018). Türk Ceza Kanunu'ndaki Düzenlemeler Işığında Psikiyatrislerin İhbar Yükümlülüğü ve Hasta Mahremiyetinin Sınırları. içinde (s.563-603) *IV. Uluslararası Sağlık Hukuku Kongresi*. İstanbul:Seçkin Yayıncılık.

Arslantaş-Toktaş, S., Binark, M., Dikmen, E. Ş., Fidaner, I. B., Küzeci, E., & Özaygen, A. (2012). *Türkiye'de Dijital Gözetim T.C. Kimlik Numarasından E-Kimlik Kartlarına Yurttaşın Sayısal Bedenlenişi*. İstanbul:Alternatif Bilişim Derneği.

Arun, Ö., & Elmas, Ç. (2020). Türkiye'de Dijital Eşitsizliğin Toplumsal Kökenleri. içinde (s.115), *Dijital Kültür, Dijital Eşitsizlikler ve Yaşlanma*. İstanbul:Alternatif Bilişim Derneği.

Aşkin, D. (2021). Covid-19 Pandemisi, Yeni Dışlanma Zeminleri ve Sorumluluk Alanları: Türkiye'de Virüsün Yayılışını Engelleme Politikaları ve Toplumsal

Bağlam. *Bil. Derg*, *5*(1), 145–165. Erişim adresi:https://doi.org/10.31200/makuubd.844035

Avrupa Konseyi. (2017). *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*. Erişim adresi: www.coe.int/data-protection

Bakırel, N. B. (2020). *Veri Sorumlusu ve Veri İşleyen Arasındaki Sorumluluk Paylaşımının Avrupa Birliği Genel Veri Koruma Tüzüğü ve Kişisel Verilerin Korunması Kanunu Çerçevesinde Değerlendirilmesi*.[Yüksek lisans tezi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü] Erişim adresi: http://www.openaccess.hacettepe.edu.tr:8080/xmlui/handle/11655/22193

Balkan, C. (2020). *Ham verinin nitelikli bilgiye dönüştürülme süreci*. Erişim adresi: https://docplayer.biz.tr/48792198-Ham-verinin-nitelikli-bilgiye-donusturulme-sureci.html.

Ballantyne, A. (2020). How should we think about clinical data ownership? *Journal of Medical Ethics*, *46*(5), 289–294. https://doi.org/10.1136/MEDETHICS-2018-105340

Barry, B. (2017). *Sosyal Adalet Neden Önemlidir?* 1. basım (Kılıç E, Çev); İstanbul:Koç Üniversitesi Yayınları.(Orijinal çalışma basım tarihi 2015).

Başer, Y. (2019a). *Hasta kayit kabul modülü eğitim dokümani*. Mia Teknoloji.

Başer, Y. (2019b). *Poliklinik-Klinik-Yoğun Bakım modülü eğitim dokümanı*. Mia Teknoloji.

Başer, Y. (2020). *Gebelik Bildirim-Gebe İzlem-Lohusa İzlem eğitim dokümanı*. Mia Teknoloji.

Bilgi Edinme Hakkı Kanunu, (24 Ekim, 2003). *Resmi Gazete* (Sayı:25269). Erişim adresi: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.4982.pdf

Birdişli, F. (2010). Birleşmiş Milletler (BM)'in Uluslararası Sorunları Önleyebilme Yeteneği. *Uluslararası Sosyal Araştırmalar Dergisi*, *3*(11), 172–182.

Birgün. (2014). *Sağlık Bakanlığı SGK bilgilerini sattığını doğruladı: İsim vermeden sattık*.(2022, 2 Şubat) Erişim adresi:https://www.birgun.net/haber/saglik-bakanligi-sgk-bilgilerini-sattigini-dogruladi-isim-vermeden-sattik-70478

Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Hakları ve İnsan Haysiyetinin Korunması Sözleşmesi: İnsan Hakları ve Biyotıp Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun, (2003, 3 Aralık). *Resmi Gazete* (Sayı: 5013). Erişim adresi: https://www5.tbmm.gov.tr/kanunlar/k5013.html

Boiten, E. (2020). *Our personal health history is too valuable to be harvested by the tech giants*. The Guardian. (2021, 15 Haziran). Erişim adresi: https://www.theguardian.com/commentisfree/2020/feb/16/our-personal-health-history-is-too-valuable-to-be-harvested-by-tech-giants

Boz, A. (2014). *Kişisel Verilerin Korunması: Türkiye, ABD ve AB Örnekleri*. [Yüksek lisans tezi, Polis Akademisi, Güvenlik Bilimleri Enstitüsü].

Bülbül, H. (2019a). *FTR dokümani*. Mia Teknoloji.

Bülbül, H. (2019b). *Hemodiyaliz modülü eğitim dokümani*. Mia Teknoloji.

Bülbül, H. (2019c). *Kan bankasi laboratuvar modül eğitim dokümani*. Mia Teknoloji.

Bülbül, H. (2019d). Kan bankasi modül eğitim dokümani. In *Mia Teknoloji*. Mia Teknoloji.

Bülbül, H. (2019e). *Patoloji modülü eğitim dokümani*. Mia Teknoloji.

Bulut, F., & Civaner, M. M. (2016). Modern tıp insancıl özünü yitiriyor: Artık "Hasta yok, Hastalık var!" *Türkiye Biyoetik Dergisi*, *3*(2), 66–73. Erişim adresi: https://jag.journalagent.com/tjob/pdfs/TJOB-58070-REVIEW-BULUT.pdf.

Bunker, J. P. (2001). The role of medical care in contributing to health improvements within societies. *International Journal of Epidemiology*, *30*, 1260–1263. Erişim adresi: https://academic.oup.com/ije/article/30/6/1260/651763.

Cangil, S. M. (2021). The HES-code and the data protectionduring COVID-19 pandemic in Turkey. *Bioethica, 7*(2). Erişim adresi: https://ejournals.epublishing.ekt.gr/index.php/bioethica/issue/view/1656/501

Cate, F. H., Cullen, P., & Mayer-Schonberger, V. (2013). *Data Protection Principles for the 21st Century*. Erişim adresi:https://www.repository.law.indiana.edu/facbooks

Cavoukian, A. (2011). *Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices*. Erişim adresi: https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf.

Çayır, F. (2020a). *Covid-19 Sürecinde Temas Takip Uygulamaları ve Kişisel Verilerin Korunması*. Ankara:Alternatif Bilişim Derneği.

Çayır, F. (2020b). *Pandemi Takip Uygulamaları ve Kişisel Verilerin İzlenmesi Raporu*. Ankara:Alternatif Bilişim Derneği.

Çayır, F. (2020c). *Pandemi Takip Uygulamaları ve Kişisel Verilerin İzlenmesi Raporu*. Ankara:Alternatif Bilişim Derneği.

Çayır, F. (2020d). Temas Takip Uygulamaları ve "Hayat Eve Sığar" Uygulaması Özelinde Kişisel Verilerin Korunması. içinde (s.108) *Kişisel Sağlık Verileri 4. Ulusal Kongresi 24-25 Ekim Webınar*. TTB Kişisel Sağlık Verileri Çalışma Grubu.

Çimen, M., & Bayraktar, B. (2019a). *Kan alma birimi eğitim dokümani*. Mia Teknoloji.

Çimen, M., & Bayraktar, B. (2019b). *Laboratuvar modülü eğitim dokümani*. Mia Teknoloji.

Ceza Muhakemesi Kanunu, (2004, 17 Aralık) *Resmi Gazete* (Sayı:25673). Erişim adresi: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5271.pdf

Christman, J. (2015). *Autonomy in Moral and Political Philosophy (Stanford Encyclopedia of Philosophy)*. Stanford Encyclopedia of Philosophy. Erişim adresi:https://plato.stanford.edu/entries/autonomy-moral/

Clemens, N. A. (2012). Privacy, consent, and the electronic mental health record: The Person vs. the System. *Journal of Psychiatric Practice*, *18*(1), 46–50. Erişim adresi:https://doi.org/10.1097/01.PRA.0000410987.38723.47

Conseil of Europe. (2017). *Guidelines on the Protection of Individuals With Regard To the Processing of Personal Data in a World of Big Data*. Erişim adresi:https://rm.coe.int/16806ebe7a

Contreras, J. L. (2019). The False Promise of Health Data Ownership. *New York University Law Review*, *94*. Erişim adresi: https://heinonline.org/HOL/Page?handle=hein.journals/nylr94&id=642&div=&collection=

CPME. (2012). *CPME Statement on the Proposal for a Regulation on the General Data Protection Regulation 2012/0011(COD)*. (2020, 27 Şubat) Erişim adresi:www.cpme.eu

CPME. (2013). *Consent in the field of research*. Erişim adresi: https://www.cpme.eu/api/documents/adopted/2013/049_Letter_MEPs_Consent.in_.the_.field_.of_.research_19092013.pdf.

Cumhuriyet. (2021). Moskova metrosunda "yüz tanıma sistemiyle ödeme" dönemi. *Cumhuriyet Gazetesi*. (2021, 16 Ekim). Erişim adresi:https://www.cumhuriyet.com.tr/dunya/moskova-metrosunda-yuz-tanima-sistemiyle-odeme-donemi-1877067

Dalgalıdere, S. (2016). *Epistemolojik Açıdan Büyük Veri ve Gelecek Tahmin Sistemleri*. [Doktora tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü] Erişim adresi: https://acikbilim.yok.gov.tr/handle/20.500.12812/309968.

Davies, C., & Collins, R. (2006). Confidentiality and consent in medical research: Balancing potential risks and benefits of using confidential data. *BMJ : British Medical Journal*, *333*(7563), 349. https://doi.org/10.1136/BMJ.333.7563.349

Davis, K., & Patterson, D. (2012). *Ethics of Big Data*. O'Reilly Media. https://www.oreilly.com/library/view/ethics-of-big/9781449314873/

De Mauro, A., Greco, M., & Grimaldi, M. (2015). What is big data? A consensual definition and a review of key research topics. *AIP Conference Proceedings*, *1644*, 97–104. https://doi.org/10.1063/1.4907823

DeBolt, C., & Harris, D. (2021). The Impact of Social Determinants of Health on Gender Disparities Within Respiratory Medicine. *Clinics in Chest Medicine*, *42*(3), 407–415. https://doi.org/10.1016/J.CCM.2021.04.003

Dinç, E. (2006). *Kişisel Verilerin Korunmasında Uluslararasi Düzenlemeler ve Türkiye'nin Durumu*. [Yüksek lisans tezi, Dicle Üniversitesi Sosyal Bilimler Enstitüsü].

Dinov, I. D. (2016). Volume and value of big healthcare data. *Journal of Medical Statistics and Informatics*, *4*(1), 3. https://doi.org/10.7243/2053-7662-4-3

Doğan, E. (2021). *e-nabız Verileri Çalındı Mı ? Bilgi Güvenliği*. (2022, 20 Şubat) BSHA. https://www.bsha.com.tr/e-nabiz/

Dülger, M. V. (2020). *Kişisel Verilerin Korunması Hukuku* (3. basım). İstanbul:Hukuk Akademisi.

ECHR. (2021). *Guide to the Case-Law of the of the European Court of Human Rights Data protection*. Erişim adresi:https://twitter.com/ECHR_CEDH.

Eke, E., Çelik, R., & Çetin, B. (2018). Mobil Sağlık Uygulamalarının Güvenliğine İlişkin Haberler Aracılığıyla Yaşanan Etik Sorunların Değerlendirilmesi. *AİBÜ Sosyal Bilimler Enstitüsü Dergisi*, *3*(18), 129–145.

Elmas, U., Gürel Gökçay, Ö., & Gül, F. (2020). Sağlıkta Büyük Veri. içinde (s.25-36). *Sağlık Alanında Büyük Veri*. İstanbul:İsar Yayınları.

Erbaş, Ö. (2014). *Kişisel Sağlık Verileri Satılamaz, Ama SGK Sattı*. (2020, 29 Ocak) Bianet. Erişim adresi:https://m.bianet.org/bianet/saglik/159720-kisisel-saglik-verileri-satilamaz-ama-sgk-satti

Erdinç, G. H. (2020). Ölçülülük İlkesi ve Açık Rıza Kapsamında Biyometrik Verilerin İşlenmesi. *Kişisel Verileri Koruma Dergisi*, *2*(1). www.kvkk.gov.tr

Eroğlu, D. (2022). *Belgeleriyle BTK-gate: Türkiye'deki tüm kullanıcıların internet hareketleri, yaklaşık bir buçuk yıldır, kimlikleri ve kişisel verileriyle birlikte BTK'ya akıyor - Medyascope*. (2022, 22 Temmuz). Medyascope. Erişim adresi:https://medyascope.tv/2022/07/21/belgeleriyle-btk-gate-turkiyedeki-tum-kullanicilarin-internet-hareketleri-yaklasik-bir-bucuk-yildir-kimlikleri-ve-kisisel-verileriyle-birlikte-btkya-akiyor/

Ertaşı, H., Eroğlu, E., & Çiftçi Kıraç, F. (2019). E-Nabız Uygulaması Farkındalığının İncelenmesi. içinde (s.94-99) *4. Uluslararası Sağlık Bilimleri ve Yönetimi Kongresi e-Bildiri Kitabı*.

European Commission. (2019). *Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection*. Erişim adresi: https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf.

Fiğan, M., & Dede Özdemir, Y. (2020). Giriş yazısı. içinde, *Dijital Kültür, Dijital Eşitsizlikler ve Yaşlanma*. Ankara: Alternatif Bilişim Derneği.

Garret, P., & Seidman, J. (2011). *EMR vs EHR: What is the Difference?* (2022, 22 Eylül). Health IT Buzz. Erişim adresi:https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference

Gedik, K. Z., & Yalçınkaya, Ö. (2019). Elektronik Sağlık Kayıtlarında Gizlilik ve Mahremiyet Yönetimi. içinde (s.451-464). *Bilgi Yönetimi ve Bilgi Güvenliği eBelge- eArşiv- eDevlet- Bulut Bilişim- Büyük Veri - Yapay Zeka*. Ankara:Bil-Gem Yayınları.

Genel Sağlık Sigortası Verilerinin Güvenliği Ve Paylaşımına İlişkin Yönetmelik.. (11 Temmuz, 2012). *Resmi Gazete* (Sayı: 28350). Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2012/07/20120711-7.htm

Geuss, R. (2007). *Kamusal şeyler, özel şeyler* (Koçak, G., Çev). İstanbul: Yapıkredi Yayınları

Goodin, D. (2011). *Insulin pump hack delivers fatal dosage over the air*. (2021, 31 Aralık) The Register. Erişim adresi:https://www.theregister.com/2011/10/27/fatal_insulin_pump_attack/

Gostin, L. O. (2006). Privacy: rethinking health information technology and informed consent. *Hastings Cent Rep*, 15–17. Erişim adresi:https://pubmed.ncbi.nlm.nih.gov/19891270/

GPA. (2020). *Achieving privacy by design in contact tracing measures.* (2022, 19 Ekim) Global Privacy Assembly. https://globalprivacyassembly.org/contact-tracing-statement/

Gray, J., David Liu, M. T., Maria Nieto-Santisteban, B., Szalay, A. S., DeWitt, D., & Gerd Heber, W. (2005). *Scientific Data Management in the Coming Decade*. (2021, 23 Haziran) Erişim adresi:http://science.hq.nasa.gov/research/earth_

Greenwald, G. (2015). *Saklanacak Yer Yok* (Çolak T, Çev.). İstanbul:Profil Yayıncılık. (Orijinal çalışma basım tarihi 2014).

Gu, Y., & Day, K. (2013). Propensity of people with long-term conditions to use personal health records. *Studies in Health Technology and Informatics*, *188*, 46–51. https://doi.org/10.3233/978-1-61499-266-0-46

Güner, H. (2020). *Kişisel Sağlık Verileri, İşlenmesi ve İhlaller, Seçim Yasasında Son Durum* (H. Oğan (ed.)). Ankara:Türk Tabipleri Birliği Yayınları.

Gürel, B. (2020). E-Nabız Sistemi Değişti Vatandaş Artık Verilerini E-Nabız'dan Silmekte Özgür! (2021, 23 Haziran) *Hukuki Haber*. Erişim adresi:https://www.hukukihaber.net/e-nabiz-sistemi-degisti-vatandas-artik-verilerini-e-nabizdan-silmekte-ozgur-makale,7739.html

Gürsakal, N. (2014). *Büyük veri* (2. basım). Bursa:Dora yayıncılık.

Gürsakal, N. (2019). *Veri Bilim* (1. basım.). Bursa:Dora yayıncılık.

Haberler.com. (2021). TikTok Gizlilik Politikasında Değişikliğe Gitti: Biyometrik Veri Toplayacak! (2021, 17 Ekim). Erişim adresi:https://www.haberler.com/tiktok-gizlilik-politikasinda-degisiklige-gitti-14183015-haberi/

Habl, C., Theresa Renner, A., Bobek, J., & Laschkolnig, A. (2016). *Study on Big Data in Public Health, Telemedine and Healthcare Final Report December 2016*. https://doi.org/10.2875/734795

Hasta Hakları Yönetmeliği.(1 Ağustos, 1998). *Resmi Gazete* (Sayı: 23420). Erişim adresi: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=4847&MevzuatTur=7&MevzuatTertip=5

He, K. Y., Ge, D., & He, M. M. (2017). Big Data Analytics for Genomic Medicine. *International Journal of Molecular Sciences*, *18*(2). https://doi.org/10.3390/IJMS18020412

HealthIT. (2020). *What is an electronic health record (EHR)?* (2020, 22 Eylül) HealthIT.Gov. Erişim adresi:https://www.healthit.gov/faq/what-electronic-health-record-ehr

Helm, T. (2020). *Revealed: how drugs giants can access your health records*. (2022, 18 Ocak) The Guardian. Erişim adresi:https://www.theguardian.com/technology/2020/feb/08/fears-over-sale-anonymous-nhs-patient-data.

Henni, S. H., Maurud, S., Fuglerud, K. S., & Moen, A. (2022). The experiences, needs and barriers of people with impairments related to usability and accessibility of digital health solutions, levels of involvement in the design process and strategies for participatory and universal design: a scoping review. *BMC Public Health*, *22*(1). https://doi.org/10.1186/S12889-021-12393-1

Hoffman, S. (2016). Medical Big Data Research: Privacy and Autonomy Concerns. *Electronic Health Records and Medical Big Data*, 129–151. https://doi.org/10.1017/9781316711149.007

Hoffman, S., & Podgurski, A. (2012). Balancing Privacy, Autonomy, and Scientific Needs in Electronic Health Records Research. *Faculty Publications*, *65*. Erişim adresi:https://scholarlycommons.law.case.edu/faculty_publications/5

Hong, L., Luo, M., Wang, R., Lu, P., Lu, W., Lu, L., & Musterman, M. (2018). *Big Data in Health Care : What Is So Different About Was ist so anders am Neuroenhancement ? 1*(2), 122–135.

Hussoloji. (2018). Sosyal Kredi Sistemi, Çin ve 1984. (2020, 9 Şubat) Erişim adresi:http://www.hussoloji.com/2018/07/sosyal-kredi-sistemi-cin-ve-1984.html

HYP. (2021). *HYP Hastalık Yönetimi Platformu v2.1.17*. Erişim adresi:https://hyp.saglik.gov.tr/

İnal, Y., & Ercil Cağıltay, N. (2019). E-Nabız Mobil Sağlık Uygulamasına Yönelik Kullanıcı Değerlendirmesi. In *Hacettepe Sağlık İdaresi Dergisi* 22(2). https://orcid.org/0000-0003-0875-9276

International Working Group on Data Protection in Telecommunications. (2014a). *Berlin Group Working Paper on Big Data and Privacy*. 1–18.

International Working Group on Data Protection in Telecommunications. (2014b). *International Working Group on Data Protection in Telecommunications*.

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun. (4 Mayıs, 2007). *Resmi Gazete* (Sayı: 26530). Erişim adresi: https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf

İş Kanunu. (22 Mayıs, 2003). *Resmi Gazete* (Sayı: 25134). Erişim adresi: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.4857.pdf

İzgi, C. (2014). *Mahremiyet kavramı bağlamında kişisel sağlık verileri.* Türkiye Biyoetik Dergisi 1(1), 25-37.

Jacquemard, T., Doherty, C. P., & Fitzsimons, M. B. (2021). The anatomy of electronic patient record ethics: a framework to guide design, development, implementation, and use. *BMC Medical Ethics*, *22*(1). https://doi.org/10.1186/S12910-021-00574-X

Jasserand, C. (2017). *Legal Nature of Biometric Data: From 'Generic' Personal Data to Sensitive Data*. European Data Protection Law Review. https://doi.org/10.21552/edpl/2016/3/6

Jilani, M. H., Javed, Z., Yahya, T., Valero-Elizondo, J., Khan, S. U., Kash, B., Blankstein, R., Virani, S. S., Blaha, M. J., Dubey, P., Hyder, A. A., Vahidy, F. S., Cainzos-Achirica, M., & Nasir, K. (2021). Social Determinants of Health and Cardiovascular Disease: Current State and Future Directions Towards Healthcare Equity. *Current Atherosclerosis Reports 2021 23:9*, *23*(9), 1–11. https://doi.org/10.1007/S11883-021-00949-W

Kahn, J. S., Aulakh, V., & Bosworth, A. (2009). What it takes: Characteristics of the ideal personal health record. *Health Affairs*, *28*(2), 369–376. https://doi.org/10.1377/hlthaff.28.2.369

Kan ve Kan Ürünleri Kanunu, (2 Mayıs, 2007). *Resmi Gazete* (Sayı: 26510). Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2007/05/20070502-1.htm

Karakethüdaoğlu, M. (2019). *Sistemlerin Geliştirilmesinde Mobil Uygulamalarda Kullanıcı Geri Bildirimlerinin Önemi: Türkiye E-Nabız Örneği*. [Yüksek lisans tezi, Sakarya Üniversitesi İşletme Enstitüsü]. Erişim adresi: https://acikerisim.sakarya.edu.tr/bitstream/handle/20.500.12619/69163/T07959.pdf?sequence=1&isAllowed=y

Kart, A. (2019). Kişisel veri ve rekabet hukuku kapsamında "Big data." *Kişisel Verileri Koruma Dergisi*, *1*(1). Erişim adresi:www.kvkk.gov.tr

Kasapoğlu, Ç. (2020). *Koronavirüs: Türkiye ve dünyadaki temas takip uygulamaları güvenli mi, hak ve mahremiyet ihlallerine yol açar mı?* (2022, 19 Ekim) BBC Türkçe. https://www.bbc.com/turkce/haberler-dunya-52638919.

Kaya, M. B. (2020). Büyük Veri Analitiği ve Kişisel Verilerin Korunması. içinde (s.63-68), *Sağlık Alanında Büyük Veri*. İstanbul:İsar Yayınları.

Keleş, Ş., Yılmaz Özpolat, A. G., & Yalım, N. Y. (2020). Cinsiyet Kimliği ve Cinsel Yönelim Hakkında Psikiyatristlerin Etik Söylemleri: Nitel Bir Araştırma. *Türk Psikiyatri Dergisi*, *31*(1), 31–40. https://doi.org/10.5080/u23338

Kişisel Nitelikteki Verilerin Otomatik İşleme Tabi Tutulması Karşısında Şahısların Korunmasına Dair Sözleşme. (17 Mart, 2016). *Resmi Gazete* (Sayı: 29656). Erişim adresi: https://insanhaklarimerkezi.bilgi.edu.tr/tr/content/157-kisisel-verilerin-otomatik-isleme-tabi-tutulmas-karssnda-bireylerin-korunmas-sozlesmesi/

Kiraç, R., & Yılmaz, G. (2019). Yetişkinlerde E-Nabız Sistemi Farkındalığının Belirlenmesine Yönelik Bir Araştırma. içinde (s.1658-1668), *3. Uluslararası 13. Ulusal Sağlık ve Hastane İdaresi Kongresi*.

Kişisel Sağlık Verileri Hakkında Yönetmelik. (2019, 21 Haziran). *Resmi Gazete* (Sayı: 30808). Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2019/06/20190621-3.htm

Kişisel Verileri Koruma Kurumu. (2018a). *Kişisel Veri Güvenliği Rehberi*. Ankara:KVKK Yayınları.

Kişisel Verileri Koruma Kurumu. (2018b). *Kişisel Verilerin Korunması Kanununa İlişkin Uygulama Rehberi*. Ankara:KVKK Yayınları.

Kişisel Verileri Koruma Platformu. (2021). *Kişisel Veri Nedir ?* (2021, 29 Haziran) Erişim adresi:http://nitelikliveri.com/kvkk-kavramlar/kisisel-veri-nedir/

Kişisel Verilerin Korunması Kanunu. (2016, 24 Mart). *Resmi Gazete* (Sayı: 29677). Erişim adresi: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf

Kişisel Verilerin Silinmesi, Yok Edilmesi veya Anonim Hale Getirilmesi Hakkında Yönetmelik, (28 Ekim, 2017). *Resmi Gazete* (Sayı: 30224). Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2017/10/20171028-10.htm

Korkmaz, İ. (2016). Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme. *TTB Dergisi*, *124*, 81–152. http://www.resmigazete.gov.tr/

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

KVKK. (2018a). *Aydınlatma Yükümlülüğünün Yerine Getirilmesinde Uyulacak Usul ve Esaslar Hakkında Tebliğ*. https://www.resmigazete.gov.tr/eskiler/2018/03/20180310-5.htm

KVKK. (2019). *Spor salonu hizmeti sunan veri sorumlularının, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma*

Kurulunun 25/03/2019 Tarihli ve 2019/81 Sayılı Karar ve 31/05/201. https://www.kvkk.gov.tr/Icerik/5496/2019-81-165

KVKK. (2020). *"Spor salonu hizmeti sunan veri sorumlusunun, üyelerinin giriş-çıkış kontrolünü biyometrik veri işleyerek yapması ile ilgili Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/167 Sayılı Karar Özeti*. https://www.kvkk.gov.tr/Icerik/6738/2020-167

Layman, E. J. (2020). Ethical Issues and the Electronic Health Record. *Health Care Manager*, *39*(4), 150–161. https://doi.org/10.1097/HCM.0000000000000302

Lee, S., Xu, Y., D'Souza, A. G., Martin, E. A., Doktorchik, C., Zhang, Z., & Quan, H. (2020). Unlocking the potential of electronic health records for health research. *International Journal of Population Data Science*, *5*(1). https://doi.org/10.23889/ijpds.v5i1.1123

Leith, D. J., & Farrell, S. (2020). Contact Tracing App Privacy: What Data Is Shared By Europe's GAEN Contact Tracing Apps. *School of Computer Science & Statistics* https://www.scss.tcd.ie/Doug.Leith/pubs/contact_tracing_app_traffic.pdf

Leonhard, G. (2018). *Teknolojiye Karşı İnsanlık* (C. Akkartal & İ. Akkartal, Çev.). İstanbul:Siyah Kitap. (Orijinal çalışma basım tarihi 2014).

Leprince-Ringue, D. (2021). Contact-tracing apps: Android phones were leaking sensitive data, find researchers. (2022, 4 Eylül) *ZDNET*. Erişim adresi:https://www.zdnet.com/article/contact-tracing-apps-android-phones-were-leaking-sensitive-data-find-researchers/

Lokke, E. (1980). *Mahremiyet Dijital Toplumda Özel Hayat* (D. Başak, Çev.). İstanbul:Koç Üniversitesi Yayınları. (Orijinal çalışma basım tarihi 1980)

Lucivero, F., & Jongsma, K. R. (2018). A mobile revolution for healthcare? Setting the agenda for bioethics. *Journal of Medical Ethics*, *44*(10), 685–689. https://doi.org/10.1136/MEDETHICS-2017-104741

Mahajan, S., Lu, Y., Spatz, E. S., Nasir, K., & Krumholz, H. M. (2022). Inequities still exist in the use of digital health technology across different sociodemographic subgroups. *Evidence-Based Nursing*, *25*(1), 23–23. https://doi.org/10.1136/EBNURS-2020-103355

Mann, S. P., Savulescu, J., & Sahakian, B. J. (2016). Facilitating the ethical use of health data for the benefit of society: electronic health records, consent and the duty of easy rescue. *Philosophical Transactions. Series A, Mathematical, Physical, and Engineering Sciences*, *374*(2083). https://doi.org/10.1098/RSTA.2016.0130

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H. (2011). *Big data: The next frontier for innovation, competition, and productivity*. (2021, 16 Temmuz). Erişim adresi:www.mckinsey.com/mgi.

Martani, A., Geneviève, L. D., Elger, B., & Wangmo, T. (2021). "It's not something you can take in your hands". Swiss experts' perspectives on health data ownership: an interview-based study. *BMJ Open*, *11*(4), e045717. https://doi.org/10.1136/BMJOPEN-2020-045717

Mayer-Schönberger, Cukier, K. (2013). *Büyük Veri Yaşama, Çalışma ve Düşünme Şeklimizi Dönüştürecek Bir Devrim* (B. Erol, Çev.). İstanbul:Paloma.

Mehmet, F. (2022). *Türkiye dünyada 7. ülke: Yerli Biyometrik Veri Sistemi hizmete girdi*. (2022, 1 Şubat). DefenceTurk. https://www.defenceturk.net/turkiye-dunyada-7-ulke-yerli-biyometrik-veri-sistemi-hizmete-girdi

Middleton, A., Milne, R., Almarri, M. A., Anwer, S., Atutornu, J., Baranova, E. E., Bevan, P., Cerezo, M., Cong, Y., Critchley, C., Fernow, J., Goodhand, P., Hasan, Q., Hibino, A., Houeland, G., Howard, H. C., Hussain, S. Z., Malmgren, C. I., Izhevskaya, V. L., … Morley, K. I. (2020). Global Public Perceptions of Genomic Data Sharing: What Shapes the Willingness to Donate DNA and Health Data? *American Journal of Human Genetics*, *107*(4), 743. https://doi.org/10.1016/J.AJHG.2020.08.023

Mikk, K. A., Sleeper, H. A., & Topol, E. J. (2017). The Pathway to Patient Data Ownership and Better Health. *JAMA*, *318*(15), 1433–1434. https://doi.org/10.1001/JAMA.2017.12145

Montgomery, J. (2017). Data Sharing and the Idea of Ownership. *Https://Doi.Org/10.1080/20502877.2017.1314893*, *23*(1), 81–86. https://doi.org/10.1080/20502877.2017.1314893

Mullins, C. (2018). *We Are in Need of Data Ethics Now - Database Trends and Applications*. (2020, 12 Şubat). Database Trends and Applications. Erişim adresi:http://www.dbta.com/Columns/DBA-Corner/We-Are-in-Need-of-Data-Ethics-Now-125891.aspx

National Institutes of Health Office of Science Policy. (2021). *The Framingham Heart Study*. (2021, 18 Ekim). National Institutes of Health Office of Science Policy. Erişim adresi: https://framinghamheartstudy.org/files/2021/07/FHS-Laying-the-Foundation-from-NIH.pdf

Nuffield Council on Bioethics. (2015). *The Collection, Linking and Use of Data in Biomedical Research and Health Care: Ethical Issues*. (2021, 29 Aralık).

OECD. (2013). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Summary in Swedish)*. https://doi.org/10.1787/9789264196391-sum-sv

Öncü, G. A. (2009). *Özel Yaşamın Korunması Hakkı: Avrupa İnsan Hakları Sözleşmesinde*. [Doktora tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü].

Oracle. (2021). *Veritabanı Nedir?* (2021, 22 Haziran). Oracle Türkiye. https://www.oracle.com/tr/database/what-is-database/

Örnek Büken, N., & Zeybek Ünsal, Ç. (2017). Verilerin Korunması Kanununun Biyomedikal Alana Yansımaları Açısından Değerlendirilmesi. *Hacettepe HFD*, *7*(2), 33–54.

Özel Hastaneler Yönetmeliği. (27 Mart, 2002). *Resmi Gazete* (Sayı: 24708). Erişim adresi: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=4854&MevzuatTur=7&MevzuatTertip=5

Öztürk, F. (2019). AKP kısıtlı seçmen bilgilerini nasıl topladı? Muhalefete göre "Yasa dışı yollar kullanıldı", iktidar ise "Çalmadık, ulaşmak zor değil" diyor. (2021, 17 Ekim). *BBC News Türkçe*. https://www.bbc.com/turkce/haberler-turkiye-48311702

Painter Randall, K. (2015). *Health Insurer Anthem Struck By Potential Largest Healthcare Related Data Breach in History*. (2021, 19 Ekim). Connel Foley. Erişim adresi:https://www.connellfoley.com/blog/health-insurer-anthem-struck-by-potential-largest-healthcare-related-data-breach-in-history

Polat, N. (2020). Dijital pandemi gözetimi, beden politikaları ve eşitsizlikler. *Kültür ve Siyasette Feminist Yaklaşımlar*, *41*, 94–107. Erişim adresi:https://www.researchgate.net/publication/347946862

Rawls, J. (1971). *Bir Adalet Teorisi* (V. A. Coşar,Çev). Ankara:Phoenix Yayınevi.(Orijinal çalışma basım tarihi 1971).

Rhodes, C. (2016). Potential International Approaches to Ownership/Control of Human Genetic Resources. *Health Care Analysis*, *24*(3), 260. https://doi.org/10.1007/S10728-015-0300-4

Rosenberg, D. (2013). Data Before the Fact. içinde (s.33), *Raw Data is an Oxymoron*. MIT Press.

Rouse, M. (2017). *Büyük Veri Nedir ve Neden Önemlidir?* (2020, 10 Şubat) Techtarget. https://searchdatamanagement.techtarget.com/definition/big-data

Sağlık Bakanlığı. (2012). *Stratejik plan 2013 - 2017*.

Sağlık Bakanlığı. (2014a). *EHR (Electronic Health Record) - ESK (Elektronik Sağlık Kaydı)*.

Sağlık Bakanlığı. (2014b). *Ulusal Sağlık Veri Sözlüğü* (H. Öztürk, Ü. Hülür, M. Tüleylioğlu, N. Çaylan, & B. Ceyhan). Erişim adresi:http://www.e-saglik.gov.tr/USVS.aspx.

Sağlık Bakanlığı. (2015). *HBYS (Hastane Bilgi Yönetim Sistemi)*. Erişim adresi:https://dijitalhastane.saglik.gov.tr/TR,4881/hbys-hastane-bilgi-yonetim-sistemi.html

Sağlık Bakanlığı. (2018). *e-Nabız'dan Dünya Çapında Başarı*. Erişim adresi: https://sbsgm.saglik.gov.tr/TR,19880/e-nabizdan-dunya-capinda-basari.html

Sağlık Bakanlığı. (2019). *10 Milyon Kişi e-Nabız Kullanıyor*. Erişim adresi:https://sbsgm.saglik.gov.tr/TR-52960/10-milyon-kisi-e-nabiz-kullaniyor.html

Sağlık Bakanlığı. (2020). *e-Nabız nedir?* Erişim adresi:https://enabiz.gov.tr/Yardim/Index

Sağlık Bakanlığı. (2021). *Her 4 Kişiden Biri e-Nabız Kullanıyor*. Erişim adresi:https://sbsgm.saglik.gov.tr/TR,73567/her-4-kisiden-biri-e-nabiz-kullaniyor.html

Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname, (2 Kasım, 2011). *Resmi Gazete* (Sayı: 28103). Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2011/11/20111102M1-3.htm

Sağlık Bilgi Yönetim Sistemleri Hakkında Yönetmelik. (25 Ağustos, 2022), *Resmi Gazete* (Sayı:31934). Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2022/08/20220825-3.htm

Şahin, R. (2020). Bilgi Toplumu ve Mahremiyet. içinde (s.89-104), *Sağlık Alanında Büyük Veri* (1st ed., pp. 89–104). İstanbul:İsar Yayınları.

Şenel Tekin, P., & Köksal, A. (2018). Sağlık Hizmetlerinde Bilgi ve Belge Yönetimi. içinde *Tıbbi Belgeleme*. Eskişehir:Anadolu Üniversitesi.

Sherman, K. (2017). Biometrics: The Future is in Your Hands Biometrics. *Los Angeles Law Review*, *50*(50), 4. Erişim adresi:http://www.planetbiometrics.com/article-details/i/5031/desc/yahoo-adds-

Shi, Y. (2014). Big Data History, Current Status, and Challenges going Forward. *The Bridge, 44*(6), 6–11.

Silahtaroğlu, G. (2018). Veri madenciliği, büyük veri ve sağlıkta kullanımı. *Sağlık Düşüncesi ve Tıp Kültürü*, *46*, 50–51.

Snoad, L. (2011). *Is data safe in brands' hands?* Erişim adresi:https://www.marketingweek.com/is-data-safe-in-brands-hands/

Snowden, E. (2020). *Sistem Hatası* (Arıkan G, Çev.). İstanbul:Epsilon Yayınevi.

SOL. (2019). Doktora gidip antidepresan kullandı, YSK 'kısıtlı seçmen' listesine aldı. (2021, 17 Ekim). Erişim adresi:https://haber.sol.org.tr/toplum/doktora-gidip-antidepresan-kullandi-ysk-kisitli-secmen-listesine-aldi-263929

Sosyal Güvenlik Kurumu Kanunu, (20 Mayıs, 2006). *Resmi Gazete* (Sayı: 26173). Erişim adresi:https://www.mevzuat.gov.tr/MevzuatMetin/1.5.5502-20140910.pdf

T.C. Anayasası, (18 Ekim, 1982) *Resmi Gazete* (Sayı: 17863). Erişim adresi: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.2709.pdf

TDK. (2022a). *Kişisel sözcüğü*. Erişim adresi:https://sozluk.gov.tr/

TDK. (2022b). *Mahremiyet sözcüğü*. Erişim adresi:https://sozluk.gov.tr/

Tene, O., & Polonetsky, J. (2013). Data for All: Privacy and User Control in the Age of Analytics. *Northwestern Journal of Technology and Intellectual Property*, *11*, 239. Erişim adresi:https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1

Tıbbi Deontoloji Nizamnamesi. (19 Şubat, 1960). *Resmi Gazete* (Sayı: 10436). Erişim adresi: https://www.resmigazete.gov.tr/arsiv/10436.pdf

Toplum Sağlığı Merkezi ve Bağlı Birimler Yönetmeliği. (5 Şubat, 2015). *Resmi Gazete* (Sayı: 29258). Erişim adresi: https://www.resmigazete.gov.tr/eskiler/2015/02/20150205-5.htm

Toplum İçin Mühendislik Komisyonu. (2017). Erişim adresi: https://dergi.bmo.org.tr/tekno-politika/ozgurluk-denetim-tartismalari-ikileminde-cipli-kimlik-kartlari. Erişim tarihi:09.12.2022.

TTB. (2012). *Hekimlik Meslek Etiği Kuralları*. Erişim adresi:http://www.ttb.org.tr

TTB. (2013). *TTB: Özel Hastanelerden Sağlık Hizmeti Alırken Avuç İçi, Parmak İzi Vermek Zorunda Değilsiniz!* (2022, 31 Ocak). Erişim adresi:https://www.ttb.org.tr/haberarsiv_goster.php?Guid=67323754-9232-11e7-b66d-1540034f819c

TTB. (2017). *Hekimlik Andı güncellendi*. Erişim adresi:https://www.ttb.org.tr/haber_goster.php?Guid=b6b3bd8a-c9e0-11e7-8a71-159198489f44

TTB. (2020). Tıbbi Genetik Veriler Bildirgesi. içinde *Türk Tabipleri Birliği Etik Bildirgeleri*. Ankara:Türk Tabipleri Birliği Yayınları.

TTB. (2021). *Sağlık kurumlarında avuç içi izi alınarak kimlik tespiti uygulamaları durdurulmalı*. (2021, 17 Haziran). Erişim adresi: https://www.ttb.org.tr/kollar/COVID19/haber_goster.php?Guid=cc46485c-646b-11ea-897f-e0b4e354fcf1

Türk Borçlar Kanunu. (4 Şubat, 2011). *Resmi Gazete* (Sayı: 27836). Erişim adresi: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6098.pdf

Türk Ceza Kanunu. (12 Ekim, 2004). *Resmi Gazete* (Sayı: 25611). Erişim adresi: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf

Türk İnternet. (2019). Avuçiçi Kimlik Tanıma, Balmumu El ile Hacklendi. (2021, 29 Kasım). Erişim adresi:https://turk-internet.com/avucici-kimlik-tanima-balmumu-el-ile-hacklendi/

Türk Tabipleri Birliği Disiplin Yönetmeliği. (28 Nisan, 2004). *Resmi Gazete* (Sayı: 25446). Erişim adresi: https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5500&MevzuatTur=7&MevzuatTertip=5

Uçar, A., & İlkılıç, İ. (2020). Sağlık Sisteminde Büyük Veri ve Etik Sorunlar. içinde (s.69-88), *Sağlık Alanında Büyük Veri*. İStanbul:İsar Yayınları.

WHO. (2005). *Commission on Social Determinants of Health*. World Health Organization. Erişim adresi: https://www.who.int/teams/social-determinants-of-health/equity-and-health/commission-on-social-determinants-of-health

WHO. (2019). Electronic health records. *WHO*. Erişim adresi: http://www.who.int/gho/goe/electronic_health_records/en/

WHO. (2021a). *Coronavirus disease (COVID-19).* Erişim adresi:https://www.who.int/news-room/questions-and-answers/item/coronavirus-disease-covid-19

WHO. (2021b). *Global excess deaths associated with COVID-19, January 2020 - December 2021*. WHO. Erişim adresi:https://www.who.int/data/stories/global-excess-deaths-associated-with-covid-19-january-2020-december-2021

Wilder, M. E., Kulie, P., Jensen, C., Levett, P., Blanchard, J., Dominguez, L. W., Portela, M., Srivastava, A., Li, Y., & McCarthy, M. L. (2021). The Impact of Social Determinants of Health on Medication Adherence: a Systematic Review and Meta-analysis. *Journal of General Internal Medicine*, *36*(5), 1359–1370. https://doi.org/10.1007/S11606-020-06447-0

Winally. (2018). *Veri sızıntılarından en çok sağlık alanı etkileniyor*. (2020, 27 Şubat). Erişim adresi:https://www.winally.com/2018/08/veri-sizintilarindan-en-cok-saglik-alani-etkileniyor/

WMA. (2016). *WMA Declaration of Taipei on ethical considerations regarding health databases and biobanks*. https://doi.org/10.3917/jib.283.0113

Wu, C., Buyya, R., & Ramamohanarao, K. (2016). Big Data Analytics = Machine Learning + Cloud Computing. *Big Data: Principles and Paradigms*, 3–38. https://doi.org/10.1016/B978-0-12-805394-2.00001-5

Yao, R., Zhang, W., Evans, R., Cao, G., Rui, T., & Shen, L. (2022). Inequities in Health Care Services Caused by the Adoption of Digital Health Technologies: Scoping Review. *J Med Internet Res 2022;24(3):E34144 Https://Www.Jmir.Org/2022/3/E34144*, *24*(3), e34144. https://doi.org/10.2196/34144

Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arşiv Hizmetleri Yönergesinde Değişiklik Yapılmasına Dair Yönerge. (2007) https://www.saglik.gov.tr/TR,11242/yatakli-tedavi-kurumlari-tibbi-kayit-ve-arsiv-hizmetleri-yonergesinde-degisiklik-yapilmasina-dair-yonergesi.html.

Yavuz, C. (2019). *Aykırı veri yönelimli fayda temelli büyük veri anonimleştirme modeli*. [Doktora tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü]. Erişim adresi: https://avesis.gazi.edu.tr/yonetilen-tez/8046dec7-2808-4eb2-9799-5efb3c7cb266/aykiri-veri-yonelimli-fayda-temelli-buyuk-veri-anonimlestirme-modeli

Yüksel, M. (2014). Mahremiyet Hakkı ve Sosyo-Tarihsel Gelişimi. *Ankara Üniversitesi SBF Dergisi*, *58*(1), 181–213.

Zastrow, M. (2020). Coronavirus contact-tracing apps: can they slow the spread of COVID-19? *Nature*. https://doi.org/10.1038/D41586-020-01514-2

Zorer, U. (2021). Covid-19 Pandemisinde Temas Takip Uygulamaları ve Gözetim Toplumu. içinde *İstanbul Barosu*. Erişim adresi:https://www.istanbulbarosu.org.tr/HaberDetay.aspx?ID=15275&Desc=Yapay-Zeka-

Zuboff, Z. (2021). *Gözetim Kapitalizmi Çağı* (Uzunçelebi T, Çev.). İstanbul:Okuyan Us Yayınları.

8. EKLER

EK-1: Genel Veri Koruma Yönetmeliği'nin (GDPR) ilgili maddeleri[26]

Madde 5 Kişisel verilerin işlenmesine ilişkin ilkeler

1. Kişisel veriler:

(a) veri sahibi ile ilgili olarak hukuka uygun, adil ve şeffaf bir biçimde işlenir ('hukuka uygunluk, adalet ve şeffaflık');

(b) belirtilen, açık ve meşru amaçlara yönelik olarak toplanır ve bu amaçlara uygun olmayan bir şekilde işlenmez; kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçlarıyla veya istatistiki amaçlarla işleme faaliyeti, 89(1) maddesi uyarınca, baştaki amaçlara aykırı şekilde değerlendirilmez ('amacın sınırlandırılması');

(c) işlendikleri amaçlarla ilgili olarak yeterli, yerinde ve gerekli olanla sınırlıdır ('verilerin en az seviyeye indirilmesi');

(d) doğrudur ve, gereken şekilde, güncel tutulur; işlendikleri amaçlar göz önünde tutularak, doğru olmayan kişisel verilerin gecikmeye mahal verilmeksizin silinmesi veya düzeltilmesinin sağlanmasıyla ilgili makul tüm adımlar atılmalıdır ('doğruluk');

(e) veri sahiplerinin yalnızca kişisel verilerin işlenme amaçlarının gerektirdiği sürece teşhis edilmesini sağlayan bir şekilde tutulur; 89(1) maddesi uyarınca yalnızca kamu yararına arşivleme amaçlarıyla, bilimsel veya tarihi araştırma amaçlarıyla ya da istatistiki amaçlarla işlendikleri sürece ve veri sahibinin hakları ve özgürlüklerinin güvence altına alınmasına için bu Tüzük uyarınca gereken uygun teknik ve düzenlemeye ilişkin tedbirlerin uygulanmasına tabi olarak, kişisel veriler daha uzun süreler boyunca saklanabilir ('saklama süresinin sınırlandırılması');

(f) yetkisiz veya yasa dışı işlemeye karşı ve kazara kayba, imhaya veya tahribe karşı koruma da dahil olmak üzere teknik veya düzenlemeye ilişkin uygun tedbirlerin kullanılması suretiyle kişisel verilerin güvenliğini sağlayan bir şekilde işlenir ('bütünlük ve gizlilik').

2. Kontrolör 1. paragrafa uygun davranmaktan sorumludur ve buna uygun davrandığını gösterebilmelidir ('hesap verebilirlik').

Madde 6 İşleme faaliyetinin hukuka uygunluğu

1. İşleme faaliyeti, ancak aşağıdaki hususlardan en az biri geçerli olduğunda ve olduğu ölçüde, hukuka uygundur:

(a) veri sahibinin bir ya da daha fazla sayıda spesifik amaca yönelik olarak kişisel verilerinin işlenmesine onay vermesi;

(b) veri sahibinin taraf olduğu bir sözleşmenin uygulanması veya bir sözleşme yapılmadan önce veri sahibinin talebiyle adımlar atılması için, işleme faaliyetinin gerekli olması;

(c) kontrolörün tabi olduğu bir yasal yükümlülüğe uygunluk sağlanması amacı ile işleme faaliyetinin gerekli olması;

(d) veri sahibinin veya başka bir gerçek kişinin hayati menfaatlerinin korunması amacı ile işleme faaliyetinin gerekli olması;

(e) kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya kontrolöre verilen resmi bir yetkinin uygulanması hususunda işleme faaliyetinin gerekli olması;

(f) özellikle veri sahibinin çocuk olması halinde veri sahibinin kişisel verilerin korunmasını gerektiren menfaatleri veya temel hakları ve özgürlüklerinin bir kontrolör veya üçüncü bir kişi tarafından gözetilen meşru menfaatlere ağır basması haricinde, söz konusu menfaatler doğrultusunda işleme faaliyetinin gerekli olması.

İlk alt paragrafın (f) bendi kamu kuruluşları tarafından görevlerinin yerine getirilmesi hususunda gerçekleştirilen işleme faaliyetine uygulanmaz.

2. Üye devletler, Bölüm IX'te belirtilen diğer spesifik işleme durumları da dahil olmak üzere işleme faaliyetine ilişkin daha kati gereklilikler ve hukuka uygun ve adil işlemenin sağlanmasına yönelik diğer tedbirler belirlenmesi suretiyle, bu Tüzük'ün işleme faaliyetine ilişkin kurallarının uygulamasını 1. paragrafın (c) ve (e) bentlerine uygun olacak şekilde uyarlamak üzere daha spesifik hükümler uygulamaya devam edebilir veya uygulamaya koyabilir.

3. 1. paragrafın (c) ve (e) bentlerinde belirtilen işleme dayanağı

(a) Birlik hukuku veya

[26] ***Kaynak:*** *Kişisel Verilerin Korunması Platformu (KVKP), Erişim adresi:https://www.kisiselverilerinkorunmasi.org/mevzuat/avrupa-birligi-genel-veri-koruma-tuzugu-gdpr-turkce-ceviri/.*

(b) kontrolörün tabi olduğu üye devlet hukuku ile ortaya konur.

İşleme amacı söz konusu yasal dayanakta belirlenir veya, 1. paragrafın (e) bendinde atıfta bulunulan işleme faaliyeti ile ilgili olarak, kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya kontrolöre verilen resmi bir yetkinin uygulanması hususunda gereklidir. Söz konusu yasal dayanak bu Tüzük kurallarının uygulamasının uyarlanmasına yönelik spesifik hükümler ihtiva edebilir: bunun yanı sıra, kontrolör tarafından gerçekleştirilen işleme faaliyetinin hukuka uygunluğunu düzenleyen genel koşullar; işleme faaliyetine tabi veri türleri; ilgili veri sahipleri; kişisel verilerin açıklanabileceği kuruluşlar ve açıklanma amaçları; amacın sınırlandırılması; saklama süreleri ve Bölüm IX'te belirtilen diğer spesifik işleme durumlarına yönelik tedbirler gibi hukuka uygun ve adil işlemenin sağlanmasına yönelik tedbirler de dahil olmak üzere işleme faaliyetleri ve işleme usulleri. Birlik veya üye devlet hukuku kamu yararı hedefini karşılar ve gözetilen meşru amaçla orantılıdır.

4. Kişisel verilerin toplanma amacı dışında bir amaca yönelik olarak yapılan işleme faaliyetinin veri sahibinin rızasına veya 23(1) maddesinde atıfta bulunulan hedeflerin güvence altına alınmasına yönelik olarak demokratik bir toplumda gerekli ve ölçülü bir tedbir teşkil eden bir Birlik veya üye devlet kanununa dayanmaması durumunda, kontrolör, başka bir amaca yönelik işleme faaliyetinin kişisel verilerin asıl toplanma amacına uygun olup olmadığını değerlendirmek üzere, bunun yanı sıra aşağıdaki hususları dikkate alır:

(a) kişisel verilerin toplanma amaçları ile planlanan diğer işleme amaçları arasındaki herhangi bir bağlantı;
(b) veri sahipleri ve kontrolör arasındaki ilişki başta olmak üzere kişisel verilerin toplandığı bağlam;
(c) 9. madde uyarınca özel kategorilerdeki kişisel verilerin işlenip işlenmediği veya 10. madde uyarınca mahkumiyet kararları ve ceza gerektiren suçlara ilişkin kişisel verilerin işlenip işlenmediği başta olmak üzere kişisel verilerin mahiyeti;
(d) planlanan diğer işleme faaliyetlerinin veri sahiplerine olası yansımaları;
(e) şifreleme veya takma ad kullanımı da dahil olmak üzere uygun güvencelerin bulunması.

Madde 7 Rıza koşulları

1. İşleme faaliyetinin rızaya dayandığı hallerde, kontrolör veri sahibinin kişisel verilerinin işlenmesine rıza göstermiş olduğunu gösterebilir.
2. Veri sahibinin rızasının diğer hususlarla da ilgili olan yazılı bir beyan bağlamında verilmesi durumunda, rıza talebi diğer hususlardan açık bir şekilde ayırt edilebilecek bir şekilde, anlaşılır ve kolayca erişilebilir bir biçimde, açık ve sade bir dil kullanılarak sunulur. Söz konusu beyanın bu Tüzük açısından ihlal teşkil eden hiçbir kısmı bağlayıcı değildir.
3. Veri sahibinin istediği zaman rızasını geri çekme hakkı vardır. Rızanın geri çekilmesi, geri çekim işleminden önce rızaya dayalı olarak yapılan işleme faaliyetinin hukuka uygunluğunu etkilemez. Veri sahibi, rıza vermeden önce, bu hususta bilgilendirilir. Rızanın geri çekilmesi rıza vermek kadar kolaydır.
4. Rızanın özgür bir şekilde verilip verilmediği değerlendirilirken, her şeyden önce, bir hizmetin sağlanması da dahil olmak üzere bir sözleşmenin ifasının söz konusu sözleşmenin ifası için gerekmeyen kişisel verilerin işlenmesine yönelik bir rızaya bağlı olup olmadığına azami özen gösterilir.

Madde 8 Çocuğun bilgi toplumu hizmetlerine ilişkin rızası açısından geçerli koşullar

1. 6(1) maddesinin (a) bendinin uygulandığı hallerde, doğrudan bir çocuğa bilgi toplumu hizmetleri sağlanması ile ilgili olarak, çocuğun en az 16 yaşında olması halinde, ilgili çocuğun kişisel verilerin işlenmesi hukuka uygundur. Çocuğun 16 yaşından küçük olması halinde, söz konusu işleme faaliyeti, ancak rızanın çocuk üzerinde velayet hakkı bulunan kişi tarafından verilmesi veya onaylanması halinde ve verildiği veya onaylandığı ölçüde hukuka uygundur.

Üye devletler, 13 yaştan küçük olmamak kaydıyla, bu amaçlara yönelik olarak kanunla daha küçük bir yaş belirleyebilir.

2. Bu durumlarda, kontrolör mevcut teknolojiyi dikkate alarak rızanın çocuk üzerinde velayet hakkı bulunan kişi tarafından verildiğini veya onaylandığını doğrulamak adına makul çaba sarf eder.
3. 1. paragraf bir çocuğa ilişkin bir sözleşmenin geçerliliği, oluşturulması veya etkisi ilgili kurallar gibi üye devletlerin genel sözleşme hukukunu etkilemez.

Madde 9 Özel nitelikli kişisel verilerin işlenmesi

1. Irk veya etnik köken, siyasi görüşler, dini veya felsefi inançlar ya da sendika üyeliğinin ifşa edildiği kişisel verilerin işlenmesi ve bir gerçek kişinin kimlik teşhisinin yapılması amacıyla genetik veriler ile biyometrik

verilerin, sağlık ile ilgili verilerin veya bir gerçek kişinin cinsel yaşamı veya cinsel eğilimine ilişkin verilerin işlenmesi yasaktır.

2. 1. paragraf aşağıdakilerden birinin geçerli olması halinde uygulanmaz:
   (a) Birlik veya üye devlet hukuku çerçevesinde 1. paragrafta belirtilen yasağın veri sahibi tarafından kaldırılamayacağına ilişkin bir hüküm sağlanması haricinde, veri sahibinin belirtilen bir veya daha fazla sayıda amaca yönelik olarak söz konusu kişisel verilerin işlenmesine açık bir şekilde rıza göstermesi;
   (b) Birlik veya üye devlet hukuku çerçevesinde ya da üye devlet hukuku uyarınca yapılan ve veri sahibinin temel hakları ve menfaatlerine yönelik uygun güvencelerin sağlandığı bir toplu sözleşme çerçevesinde izin verildiği sürece, kontrolörün veya veri sahibinin istihdam ve sosyal güvenlik ve sosyal hukuku koruma alanındaki yükümlülüklerinin gerçekleştirilmesi ve spesifik haklarının kullanılması amacıyla işleme faaliyetinin gerekmesi;
   (c) veri sahibinin fiziksel veya hukuki olarak rıza veremeyecek durumda olması halinde, veri sahibi veya başka bir gerçek kişinin hayati menfaatlerinin korunması açısından işleme faaliyetinin gerekli olması;
   (d) işleme faaliyetinin bir vakıf, birlik veya kar amacı gütmeyen başka bir organ tarafından siyasi, felsefi, dini veya sendika amacıyla uygun güvencelerle birlikte yürütülen meşru faaliyetleri esnasında işlemenin ve yalnızca organın üyeleri veya eski üyeleri ya da amaçlarıyla bağlantılı olarak kendisi ile düzenli olarak temas halinde bulunan kişilerle ilgili olması ve kişisel verilerin veri sahiplerinin rızası olmaksızın söz konusu organ dışında açıklanmaması koşuluyla gerçekleştirilmesi;
   (e) işleme faaliyetinin veri sahibi tarafından açık bir biçimde kamuya açıklanan kişisel verilerle ilgili olması;
   (f) yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından veya mahkemeler kendi yargı yetkisi çerçevesinde hareket ettiğinde, işleme faaliyetinin gerekmesi;
   (g) gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve veri sahibinin temel hakları ve menfaatlerinin güvence altına alınması adına uygun ve spesifik tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak kayda değer ölçüde kamu yararı adına nedenlerden ötürü işleme faaliyetinin gerekmesi;3e
   (h) koruyucu hekimlik veya meslek hekimliği amaçları doğrultusunda, Birlik ya da üye devlet hukukuna dayalı olarak veya bir sağlık profesyoneli ile yapılan sözleşme uyarınca ve 3. paragrafta atıfta bulunulan koşullar ve güvencelere tabi olarak çalışanın çalışma kapasitesinin değerlendirilmesi, tıbbi tanı, sağlık veya sosyal bakım hizmetlerinin veya tedavinin sağlanması ya da sağlık veya sosyal bakım sistemleri ve hizmetlerinin yönetilmesi açısından işleme faaliyetinin gerekli olması;
   (i) özellikle mesleki gizlilik olmak üzere veri sahibinin hakları ve özgürlüklerine ilişkin güvence sağlanmasına uygun ve spesifik tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak, sağlığa yönelik ciddi sınır ötesi tehditlere karşı koruma sağlanması veya sağlık hizmetleri ve tıbbi ürünler ya da tıbbi cihazlara ilişkin yüksek kalite ve emniyet standartları sağlanması gibi halk sağlığı alanında kamu yararına yönelik olarak işleme faaliyetinin gerekmesi;
   (j) gözetilen amaçla orantılı olan, veri koruma hakkının özüne saygı gösteren ve veri sahibinin temel hakları ve menfaatlerinin güvence altına alınmasına uygun ve spesifik tedbirler sağlayan Birlik veya üye devlet hukukuna dayalı olarak, 89(1) maddesi uyarınca kamu yararına yönelik arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işleme faaliyetinin gerekmesi.
3. 1. paragrafta atıfta bulunulan kişisel veriler Birlik ya da üye devlet hukuku kapsamındaki mesleki gizlilik yükümlülüğü veya ulusal yetkin organlar tarafından konan kurallara tabi olarak bir profesyonel tarafından veya söz konusu profesyonelin sorumluluğu altında ya da Birlik ya da üye devlet hukuku kapsamındaki mesleki gizlilik yükümlülüğü veya ulusal yetkin organlar tarafından konan kurallara tabi olarak başka bir kişi tarafından işlendiğinde, söz konusu veriler 2. paragrafın (h) bendinde atıfta bulunulan amaçlara yönelik olarak işlenebilir.
4. Üye Devletler genetik veriler, biyometrik veriler veya sağlık ile ilgili veriler ile alakalı olarak sınırlamalar da dahil olmak üzere ek koşullar uygulamaya devam edebilir ya da ek koşullar getirebilir.

Madde 13 Veri sahibinden kişisel verilerin toplandığı hallerde sağlanacak bilgiler

1. Bir veri sahibine ilişkin kişisel verilerin veri sahibinden toplanması durumunda, kontrolör kişisel verilerin elde edildiği anda aşağıdaki bilgilerin tamamını veri sahibine sağlar:
   (a) kontrolörün ve, uygun olduğu hallerde, kontrolörün temsilcisinin kimlik ve irtibat bilgileri;
   (b) uygun olduğu hallerde, veri koruma görevlisinin irtibat bilgileri;
   (c) kişisel verilerin planlanan işlenme amaçlarının yanı sıra işleme faaliyetinin yasal dayanağı;
   (d) işleme faaliyetinin 6(1) maddesinin (f) bendine dayanması durumunda, kontrolör veya üçüncü bir kişi tarafından gözetilen meşru menfaatler;
   (e) varsa, kişisel verilerin alıcıları veya alıcı kategorileri;
   (f) uygun olduğu hallerde, kontrolörün kişisel verileri üçüncü bir ülke veya uluslararası kuruluşa aktarmayı amaçladığı ve Komisyon tarafından bir yeterlilik kararı verilip verilmediği ya da, 46 veya

47. maddelerde veya 49(1) maddesinin ikinci alt paragrafında atıfta bulunulan aktarımlar olması halinde, uygun veya münasip güvencelere ilişkin atıf ve bunların bir nüshasının elde edilme yolları veya bunların nerede sağlandığı.

2. 1. paragrafta atıfta bulunulan bilgilere ek olarak, kontrolör kişisel verilerin elde edildiği anda adil ve şeffaf bir işleme sağlanması için gereken aşağıdaki ek bilgileri veri sahibine sağlar:
   (a) kişisel verilerin saklanacağı süre veya, bunun mümkün olmaması halinde, bu sürenin belirlenmesi amacı ile kullanılan kriterler;
   (b) kontrolörden kişisel verilere erişim ve kişisel verilerin düzeltilmesi ya da silinmesini veya veri sahibi ile ilgili işleme faaliyetinin kısıtlanmasını talep etme ya da işleme faaliyetine itiraz etme hakkının yanı sıra verilerin taşınabilirliği hakkının varlığı;
   (c) işleme faaliyetinin 6(1) maddesinin (a) bendine veya 9(2) maddesinin (a) bendine dayandığı hallerde, rızanın geri çekilmesinden önce rızaya dayalı olarak gerçekleştirilen işleme faaliyetinin hukuka uygunluğu etkilenmeden, herhangi bir zamanda rızayı geri çekme hakkının varlığı;
   (d) bir denetim makamına şikayette bulunma hakkı;
   (e) kişisel verilerin sağlanmasının yasal ya da sözleşmeye bağlı bir gereklilik mi yoksa bir sözleşme yapılması için gereken bir gereklilik mi olduğu ve ayrıca, veri sahibinin kişisel verileri sağlamak zorunda olup olmadığı ve söz konusu verilerin sağlanmamasının muhtemel sonuçları;
   (f) profil çıkarma da dahil olmak üzere 22(1) ve (4) maddelerinde atıfta bulunulan otomatik karar vermenin varlığı ve, en azından bu hallerde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işleme faaliyetinin veri sahibi açısından önemi ve öngörülen sonuçları.
3. Kontrolörün kişisel verileri bu verilerin toplanma amacı dışında bir amaçla işleme faaliyetine niyet ettiği hallerde, kontrolör söz konusu işleme faaliyetinden önce diğer amaca ilişkin bilgileri ve 2. paragrafta atıfta bulunulan diğer ilgili bilgileri veri sahibine sağlar.
4. Veri sahibinin halihazırda bu bilgilere sahip olduğu hallerde ve ölçüde, 1, 2 ve 3. paragraflar uygulanmaz.

Madde 15. Veri sahibinin erişim hakkı

1. Veri sahibinin kendisi ile ilgili kişisel verilerin işlenip işlenmediğini kontrolörden teyit etme ve, işleme faaliyeti olması halinde, kişisel verilere erişim ile aşağıdaki bilgileri talep etme hakkı bulunur:
   (a) işleme amaçları;
   (b) ilgili kişisel veri kategorileri;
   (c) üçüncü ülkeler veya uluslararası kuruluşlardaki alıcılar başta olmak üzere, kişisel verilerin açıklandığı veya açıklanacağı alıcılar veya alıcı kategorileri;
   (d) mümkün olması halinde, kişisel verilerin saklanması açısından öngörülen süre veya, bunun mümkün olmaması halinde, bu sürenin belirlenmesi amacı ile kullanılan kriterler;
   (e) kontrolörden veri sahibine ilişkin kişisel verilerin düzeltilmesi veya silinmesini veya söz konusu verilerin işlenmesinin kısıtlanmasını talep etme veya söz konusu işleme faaliyetine itiraz etme hakkının varlığı;
   (f) bir denetim makamına şikayette bulunma hakkı;
   (g) kişisel verilerin veri sahibinden elde edilmemesi halinde, bu verilerin kaynaklarına ilişkin mevcut bilgiler;
   (h) profil çıkarma da dahil olmak üzere 22(1) ve (4) maddelerinde atıfta bulunulan otomatik karar vermenin varlığı ve, en azından bu hallerde, yürütülen mantığa ilişkin anlamlı bilgilerin yanı sıra söz konusu işleme faaliyetinin veri sahibi açısından önemi ve öngörülen sonuçları.

2. Kişisel verilerin üçüncü bir ülke ya da uluslararası bir kuruluşa aktarılması durumunda, veri sahibinin aktarımla ilgili olarak 46. madde uyarınca uygun güvenceler hususunda bilgilendirilme hakkı bulunur.
3. Kontrolör işleme faaliyetinden geçen kişisel verilerin bir nüshasını sağlar. Veri sahibi tarafından talep edilen diğer nüshalar açısında, kontrolör idari masraflara dayalı olarak makul bir ücret talep edebilir. Veri sahibinin talebi elektronik yollarla yapması halinde ve veri sahibi tarafından aksi talep edilmedikçe, bilgiler yaygın kullanılan bir elektronik yolla sağlanır.
4. 3. paragrafta atıfta bulunulan bir nüsha elde etme hakkı başkalarının hakları ve özgürlüklerini olumsuz yönde etkilemez.

Madde 16. Düzeltme hakkı

1. Veri sahibinin kendileri ile ilgili doğru olmayan kişisel verilerin gereksiz gecikmeye mahal verilmeksizin düzeltilmesini kontrolörden talep etme hakkı bulunur. İşleme amaçları dikkate alınarak, veri sahibinin, bir ek beyan yoluyla da dahil olmak üzere, eksik kişisel verileri tamamlatma hakkı bulunur.

Madde 17. Silme hakkı ('unutulma hakkı')

1. Veri sahibinin kendisi ile ilgili kişisel verilerin herhangi bir gecikmeye mahal verilmeksizin silinmesini kontrolörden talep etme hakkı bulunur ve, aşağıdaki hallerden birinin geçerli olması durumunda, kontrolörün kişisel verileri herhangi bir gecikmeye mahal vermeksizin silme yükümlülüğübulunur:
   (a) kişisel verilerin toplanma veya işlenme amaçlarıyla ilişkili olarak artık gerekli olmaması;
   (b) veri sahibinin 6(1) maddesinin (a) bendi veya 9(2) maddesinin (a) bendine göre işleme faaliyetinin dayandığı izni geri çekmesi ve işleme faaliyetiyle ilgili başka bir yasal gerekçe bulunmaması;
   (c) veri sahibinin 21(1) maddesi uyarınca işleme faaliyetine itirazda bulunması ve işleme faaliyetine yönelik ağır basan meşru bir gerekçe bulunmaması ya da veri sahibinin 21(2) maddesi uyarınca işleme faaliyetine itirazda bulunması;
   (d) kişisel verilerin yasa dışı biçimde işlenmiş olması;
   (e) kontrolörün tabi olduğu Birlik veya üye devlet hukukundaki bir yasal yükümlülüğe uygunluk sağlanması amacı ile kişisel verilerin silinmesinin zorunlu olması;
   (f) kişisel verilerin 8(1) maddesinde atıfta bulunulan bilgi toplumu hizmetlerinin sağlanması ile ilgili toplanmış olması.
2. Kontrolörün kişisel verileri kamuya açıklamış olduğu ve 1. paragraf uyarınca kişisel verileri silmek zorunda olduğu hallerde, kontrolör, mevcut teknoloji ve uygulama maliyetini göz önünde bulundurarak, veri sahibinin talep etmiş olduğu kişisel verileri işleyen kontrolörleri söz konusu kişisel verilere yönelik her türlü bağlantı veya bu verilerin her türlü nüshası ya da çoğaltmasının söz konusu kontrolörlerce silinmesi hususunda bilgilendirmek üzere teknik tedbirler de dahil olmak üzere makul adımları atar.
3. 1 ve 2. paragraflar işleme faaliyeti aşağıdaki amaçlar doğrultusunda gerekli olduğu ölçüde uygulanmaz:
   (a) ifade ve bilgi edinme hakkının kullanılması;
   (b) kontrolörün tabi olduğu Birlik veya üye devlet hukuku çerçevesinde işleme faaliyeti gerektiren bir yasal yükümlülüğe uygunluk açısından veya kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya kontrolöre verilen resmi bir yetkinin uygulanması açısından;
   (c) 9(2) maddesinin (h) ve (i) bentlerinin yanı sıra 9(3) maddesi uyarınca halk sağlığı alanındaki kamu yararı sebeplerinden dolayı;
   (d) 1. paragrafta atıfta bulunulan hakkın ilgili işleme hedeflerinin yakalanmasını imkansız hale getirmesi veya yakalanmasına ciddi şekilde zarar vermesinin muhtemel olduğu ölçüde, 89(1) maddesi uyarınca kamu yararına arşivleme amaçları, bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda veya
   (e) yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından.

Madde 18 İşleme faaliyetini kısıtlama hakkı

1. Aşağıdaki durumlardan birinin geçerli olması halinde, veri sahibinin kontrolörden işleme faaliyetinin kısıtlanmasını talep etme hakkı bulunur:
   (a) kişisel verilerin doğruluğuna veri sahibi tarafından itiraz edilmesi halinde, kontrolörün kişisel verilerin doğruluğunu teyit etmesini sağlayan bir süre boyunca;
   (b) işleme faaliyetinin yasa dışı olması ve veri sahibinin kişisel verilerin silinmesine itiraz etmesi ve bunun yerine verilerin kullanımının kısıtlanmasını talep etmesi;
   (c) kontrolörün işleme amaçlarına yönelik olarak artık kişisel verilere ihtiyaç duymaması, ancak veri sahibinin yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması amacıyla söz konusu verilere ihtiyaç duyması;
   (d) kontrolörün meşru gerekçelerinin veri sahibinin meşru gerekçelerine ağır basıp basmadığı doğrulanana kadar, veri sahibinin 21(1) maddesi uyarınca işleme faaliyetine itiraz etmesi.
2. İşleme faaliyetinin 1. paragraf kapsamında kısıtlanmış olduğu hallerde, söz konusu kişisel veriler, saklama haricinde, yalnızca veri sahibinin rızasıyla veya yasal iddialarda bulunulması, bu iddiaların uygulanması ya da savunulmasına yönelik olarak ya da başka bir gerçek veya tüzel kişinin haklarının korunmasına yönelik olarak ya da Birlik veya bir üye devletin önemli kamu yararı adına önemli sebeplerinden dolayı işlenir.
3. 1. paragraf uyarınca işleme faaliyetinin kısıtlanmasını sağlayan bir veri sahibi, işleme faaliyetine ilişkin kısıtlama kaldırılmadan önce, kontrolör tarafından bilgilendirilir.

Madde 19 Kişisel verilerin düzeltilmesine ya da silinmesine veya işleme faaliyetinin kısıtlanmasına ilişkin bildirim yükümlülüğü

1. Kontrolör, imkansız olmaması veya ölçüsüz bir çabayı gerektirmemesi halinde, 16. madde, 17(1) maddesi ve 18. madde uyarınca gerçekleştirilen her türlü kişisel veri düzeltme veya silme işlemi ya da işleme faaliyetini kısıtlama işlemini kişisel verilerin açıklandığı her alıcıya bildirir. Veri sahibinin bu yönde bir talebinin bulunması halinde, kontrolör veri sahibini bu alıcılar hakkında bilgilendirir.

Madde 20 Veri taşınabilirliği hakkı

1. Aşağıdaki hallerde, veri sahibinin kendisi ile ilgili olarak bir kontrolöre sağlamış olduğu kişisel verileri yapılandırılmış, yaygın olarak kullanılan ve makine tarafından okunabilecek bir formatta alma hakkı bulunur ve kişisel verilerin sağlandığı kontrolörün herhangi bir engellemesi olmaksızın bu verileri başka bir kontrolöre iletme hakkı bulunur:
   (a) işleme faaliyetinin 6(1) maddesinin (a) bendi veya 9(2) maddesinin (a) bendi uyarınca bir rızaya veya 6(1) maddesinin (b) bendi uyarınca bir sözleşmeye dayanması ve
   (b) işleme faaliyetinin otomatik yollarla gerçekleştirilmesi.
2. 1. paragraf uyarınca veri taşınabilirliği hakkını kullanırken, veri sahibinin, teknik açıdan uygulanabilir olması halinde, kişisel verilerin doğrudan bir kontrolörden diğerine ilettirme hakkı bulunur.
3. Bu maddenin 1. paragrafında atıfta bulunulan hakkın kullanımı ile 17. maddeye halel gelmez. Söz konusu hak kamu yararına gerçekleştirilen bir görevin yerine getirilmesi veya kontrolöre verilen resmi bir yetkinin uygulanması için gereken işleme faaliyetlerine uygulanmaz.
4. 1. paragrafta atıfta bulunulan hak başkalarının hakları ve özgürlüklerini olumsuz yönde etkilemez.

Madde 21 İtiraz hakkı

1. Veri sahibinin, kendi özel durumu ile ilgili gerekçelere dayalı olarak, (6)1 maddesinin (e) veya (f) bentlerindeki hükümlere dayalı olarak profil çıkarma da dahil olmak üzere bu bentlere dayalı olarak kendisi ile ilgili kişisel verilerin işlenmesine herhangi bir zamanda itiraz etme hakkı bulunur. Kontrolör veri sahibinin menfaatleri, hakları ve özgürlüklerinden ağır basan işleme faaliyetlerine yönelik olarak veya yasal iddialarda bulunulması, bu iddiaların uygulanması veya savunulması açısından zorlayıcı meşru gerekçeler göstermediği sürece, kontrolör artık kişisel verileri işleyemez.
2. Kişisel verilerin doğrudan pazarlama amaçları doğrultusunda işlenmesi durumunda, veri sahibinin doğrudan pazarlama ile alakalı olduğu ölçüde profil çıkarma da dahil olmak üzere kendisi ile ilgili kişisel verilerin söz konusu doğrudan pazarlama amacı ile işlenmesine herhangi bir zamanda itiraz etme hakkı bulunur.
3. Veri sahibinin doğrudan pazarlama amaçlarına yönelik olarak işleme faaliyetine itiraz etmesi halinde, kişisel veriler artık bu amaçlarla işlenemez.
4. En geç veri sahibi ile ilk kez iletişime geçildiği zaman, 1 ve 2. paragraflarda atıfta bulunulan hak açık bir şekilde veri sahibinin dikkatine sunulur ve diğer bilgilerden açık ve ayrı bir şekilde sunulur.
5. Bilgi toplumu hizmetlerinin kullanımı bağlamında ve 2002/58/AT sayılı Direktif'e bakılmaksızın, veri sahibi teknik açıklamaları kullanmak suretiyle otomatik yollarla itiraz hakkını kullanabilir.
6. Kişisel verilerin 89(1) maddesi uyarınca bilimsel veya tarihi araştırma amaçları ya da istatistiki amaçlar doğrultusunda işlenmesi durumunda, işleme faaliyeti kamu yararı sebeplerinden dolayı gerçekleştirilen bir görevin yürütülmesi için gerekli olmadığı sürece, veri sahibinin, kendi özel durumu ile ilgili gerekçelere dayalı olarak, kendisi ile ilgili kişisel verilerin işlenmesine itiraz hakkı bulunur.

Madde 22 Profil çıkarma da dahil olmak üzere otomatik münferit karar verme

1. Veri sahibinin kendisi ile ilgili hukuki sonuçlar doğuran veya benzer biçimde kendisini kayda değer şekilde etkileyen profil çıkarma da dahil olmak üzere yalnızca otomatik işleme faaliyetine dayalı bir karara tabi olmama hakkı bulunur.
2. Kararın aşağıdaki özellikleri taşıması halinde, 1. paragraf uygulanmaz:
   (a) veri sahibi ve bir veri kontrolörü arasında bir sözleşme yapılması veya uygulanması için gerekli olması;
   (b) kontrolörün tabi olduğu ve veri sahibinin hakları ile özgürlükleri ve meşru menfaatlerinin güvence
   (c) altına alınması amacıyla uygun tedbirlerin de belirtildiği Birlik veya üye devlet hukukun çerçevesinde izin verilmesi veya
   (d) veri sahibinin açık rızasına dayanması.
3. 2. paragrafın (a) ve (c) bentlerinde atıfta bulunulan hallerde, veri kontrolörü en azından kontrolör açısından insan müdahalesinin sağlanması hakkı başta olmak üzere veri sahibinin kendi görüşünü ifade etme ve karara karşı çıkma yönündeki hakları ile özgürlükleri ve meşru menfaatlerinin güvence altına alınması amacı ile uygun tedbirler uygular.
4. 9(2) maddesinin (a) veya (g) bendinin geçerli olmaması ve veri sahibinin hakları ile özgürlükleri ve meşru menfaatlerinin güvence altına alınması amacı ile uygun tedbirlerin alınmamış olması durumunda, 2. paragrafta atıfta bulunulan kararlar 9(1) maddesinde atıfta bulunulan özel kategorilerdeki kişisel verilere dayanamaz.

Madde 32 İşleme güvenliği

1. Kontrolör ve işleyici, son teknoloji, uygulama maliyetleri ve işleme faaliyetinin mahiyeti, kapsamı, bağlamı ve amaçlarının yanı sıra gerçek kişilerin hakları ve özgürlükleri açısından çeşitli olasılıklar ve ciddiyetlere sahip riskleri dikkate alarak, risk açısından uygun bir güvenlik seviyesi sağlamak üzere, uygun olduğu hallerde, aşağıdakiler de dahil olmak üzere uygun teknik ve düzenlemeye ilişkin tedbirler uygular:
   (a) kişisel verilerde takma ad kullanımı ve şifreleme;
   (b) işleme sistemleri ve hizmetlerinin gizliliği, bütünlüğü, elverişliliği ve esnekliğinin sürekli olarak sağlanabilmesi;
   (c) fiziksel veya teknik bir olay halinde, kişisel verilerin elverişliliği ve kişisel verilere erişimin vakitlice eski haline getirilebilmesi;

(d) işleme faaliyetinin güvenliliğinin sağlanmasına yönelik olarak teknik ve düzenlemeye ilişkin tedbirlerin etkililiğinin düzenli olarak sınanması, ölçülmesi ve değerlendirilmesine ilişkin süreç.

2. Uygun güvenlik seviyesi değerlendirilirken, iletilen, saklanan veya işlenen kişisel verilerin kazara veya yasa dışı olarak imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişim başta olmak üzere özellikle işleme faaliyetinin yol açtığı riskler göz önündebulundurulur.
3. 40. maddede atıfta bulunulan onaylı davranış kuralları veya 42. maddede atıfta bulunulan onaylı belgelendirme mekanizmasına uygun hareket edilmesi bu maddenin 1. paragrafında ortaya konan gerekliliklere uygunluğun gösterilmesine ilişkin bir unsur olarak kullanılabilir.
4. Kontrolör ve işleyici kontrolör ya da işleyicinin yetkisi ile hareket eden ve kişisel verilere erişimi bulunan herhangi bir gerçek kişinin, Birlik ya da üye devlet hukuku çerçevesinde bu yönde hareket etmesinin gerekmemesi durumunda, kontrolörden aldığı talimatlar haricinde bu verileri işlememesini sağlamak üzere adımlar atar.

Madde 33 Bir kişisel veri ihlalinin denetim makamına bildirilmesi

1. Bir kişisel veri ihlali olması durumunda, kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından bir riske sebebiyet vermesinin muhtemel olmaması haricinde, kontrolör, gereksiz gecikmeye mahal vermeden ve, uygun olması halinde, ihlalden haberdar olduktan itibaren en geç 72 saat içerisinde, kişisel veri ihlalini 55. madde uyarınca yetkin denetim makamına bildirir.

Denetim makamına yönelik bildirimin 72 saat içerisinde yapılmadığı hallerde, bu bildirimle birlikte gecikme sebeplerine de yer verilir.

2. İşleyici, bir kişisel veri ihlalinden haberdar olduktan sonra, herhangi bir gecikmeye mahal vermeden, kontrolöre bildirimde bulunur.
3. 1. paragrafta atıfta bulunulan bildirimde en azından:
(a) uygun olduğu hallerde, ilgili veri sahibi kategorileri ve yaklaşık sayısı ile ilgili kişisel veri kaydı kategorileri ve yaklaşık sayısı da dahil olmak üzere kişisel veri ihlalinin mahiyetiaçıklanır;
(b) veri koruma görevlisi veya daha fazla bilginin elde edilebileceği başka bir temas noktasının isim ve irtibat bilgileri iletilir;
(c) kişisel veri ihlalinin olası sonuçları açıklanır;
(d) uygun olduğu hallerde, kişisel veri ihlalinin olası olumsuz etkilerinin azaltılmasına yönelik tedbirler de dahil olmak üzere kişisel veri ihlalinin ele alınması için kontrolör tarafından alınan veya alınması önerilen tedbirler açıklanır.
4. Bilgilerin aynı zamanda sağlanmasının mümkün olmadığı hallerde ve ölçüde, bilgiler gereksiz herhangi bir ek gecikmeye mahal verilmeksizin aşamalı olarak sağlanabilir.
5. Kontrolör kişisel veri ihlallerini kişisel veri ihlaline ilişkin bilgiler, etkileri ve gerçekleştirilen düzeltici işlemi de kapsayacak şekilde belgelendirir. Bu belgelendirme denetim makamının bu maddeye uyumluluğu doğrulamasını sağlar.

Madde 34 Bir kişisel veri ihlalinin veri sahibine iletilmesi

1. Kişisel veri ihlalinin gerçek kişilerin hakları ve özgürlükleri açısından yüksek bir riske sebebiyet vermesinin muhtemel olduğu hallerde, kontrolör kişisel veri ihlalini gereksiz bir gecikmeye mahal vermeden veri sahibine iletir.
2. Bu maddenin 1. paragrafında atıfta bulunulan veri sahibine ilişkin bildirimde kişisel veri ihlalinin mahiyeti açık ve sade bir dille açıklanır ve en azından 33(3) maddesinin (b), (c) ve (d) bentlerinde atıfta bulunulan bilgiler ve tedbirlere yer verilir.
3. Aşağıdaki koşulların herhangi birinin yerine getirilmesi durumunda, 1. paragrafta atıfta bulunulan veri sahibine ilişkin bildirim gerekmez:
(a) kontrolörün uygun teknik ve düzenlemeye ilişkin koruma tedbirleri uygulaması ve kişisel verileri bu verilere erişim yetkisi bulunmayan herkese okunamaz hale getiren şifreleme gibi tedbirler başta olmak üzere bu tedbirlerin kişisel veri ihlalinden etkilenen kişisel verilere uygulanmışolması;
(b) kontrolörün 1. paragrafta atıfta bulunulan veri sahiplerinin hakları ve özgürlüklerine ilişkin yüksek riskin ortaya çıkmasının artık mümkün olmamasını sağlayan ek tedbirler alması;
(c) bildirimin ölçüsüz bir çaba gerektirecek olması. Bu durumda, bunun yerine, veri sahiplerinin aynı etkililikle bilgilendirildiği kamuya yönelik bir bildirim veya benzeri bir tedbir uygulanır.
4. Kontrolörün halihazırda kişisel veri ihlalini veri sahibine iletmemiş olması durumunda, denetim makamı, kişisel veri ihlalinin yüksek bir riske sebebiyet verme olasılığını değerlendirdikten sonra, kontrolörün bu bildirimi yapmasını şart koşabilir veya 3. paragrafta atıfta bulunulan koşullardan herhangi birinin yerine getirilmesine karar verebilir.

Madde 44 Genel aktarım ilkesi

Üçüncü bir ülkeye veya uluslararası bir kuruluşa aktarılmasının ardından işlenen veya işlenmesi amaçlanan kişisel verilerin aktarılması, üçüncü ülkeden veya uluslararası bir kuruluştan başka bir üçüncü ülke veya başka bir uluslararası kuruluşa yönelik transit aktarımlar da dahil olmak üzere, ancak, bu Tüzük'ün diğer hükümlerine tabi olarak, bu Bölüm'de

belirtilen koşullara kontrolör ve işleyici tarafından uyulması halinde gerçekleşir. Bu Tüzük ile temin edilen gerçek kişilere yönelik koruma düzeyine zarar verilmemesinin sağlanması amacı ile bu bölümdeki tüm hükümler uygulanır.

EK-2: Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arşiv Hizmetleri Yönergesinde Değişiklik Yapılmasına Dair Yönerge

06.06.2007 tarihli ve **5228** sayılı makam onayı ile yürürlüğe girmiştir.

MADDE 1- Bakanlık Makamının 06.11.2001 tarih ve 10588 sayılı olurlarıyla yürürlüğe giren Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arşiv Hizmetleri Yönergesinin Ek 1 inci maddesinin birinci fıkrası aşağıdaki şekilde değiştirilmiş, birinci fıkradan sonra gelmek üzere aşağıdaki fıkralar eklenmiştir.

"Kurumlarda kağıt üzerinde tutulan, kurum dışına çıkmayan ve hukuken ıslak imza gerektirmeyen poliklinik defterleri, laboratuar defterleri, yatan hasta takip kartları, anamnez formları, tedavi takip kartları gibi sağlık kayıtları ve belgeleri, lüzumu halinde istenilen içerik ve formatta çıktıları alınacak şekilde olmak şartıyla, elektronik imza uygulamaları yaygınlaşana kadar, Ek-5 de belirlenen standart ve kurallar çerçevesinde gerekli yedekleme ve güvenlik önlemleri alınarak yapılandırılan kurumlar sadece elektronik ortamda tutabilir, iş ve işlemler bu ortamda gerçekleştirilebilir."

"Sağlık kurumlarımızda kullanılmakta olan tüm bilgi sistemlerinde gerek veritabanından gerekse kullanılan uygulama yazılımları arayüzlerinden (Hastane Bilgi Sistemleri, Aile Hekimliği Bilgi sistemleri, Birinci Basamak Sağlık Kurumları Bilgi sistemleri vb.) geçmiş kayıtlardaki kapanmış, onaylanmış ve sonuçlandırılmış işlemlere ait verilerde değiştirme, silme ve ekleme yapılamaz. Son kullanıcılara sadece okuma ve raporlama yetkisi verilir."

"Herhangi bir nedenden (teknik, programatik, mevzuat vb.) kaynaklanan zorunlu haller söz konusu olduğu takdirde bunun için gerekli değiştirme, silme ve ekleme yapma yetkisi, ilgili sağlık kurumunun en üst amirine aittir. Bu değişikliklere ait detaylı loglar mutlaka tutulmalıdır."

MADDE 2- Aynı Yönerge'ye ek'teki Ek-5 eklenmiştir.

MADDE 3- Bu Yönerge Bakan onayını müteakiben yürürlüğe girer.

MADDE 4- Bu Yönerge hükümlerini Sağlık Bakanı yürütür.

EK-5

5.1. KRİZ / ACİL DURUM YÖNETİMİ

Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınmalıdır. Örneğin, uygulama veya veri tabanı sunucularında donanım ve yazılıma ait problemler oluştuğunda, yerel veya uzak sistemden yeniden kesintisiz (veya makul kesinti süresi içerisinde) çalışma sağlanabilmelidir. Kümeleme (cluster) veya uzaktan kopyalama (remote replication) çözümleri hayata geçirilmelidir. Hastaneler, sistemlerini tasarlarken ne kadar süre ile ve ne kadar performans kaybını tolere edeceklerini göz önüne almalıdırlar. Kurum çalışanlarının, bilgi güvenliği ile ilgili acil bir durum oluştuğunda sorumlulukları dahilinde gerekli müdahaleyi yapabilmelerine yönelik standartlar şunlardır.

5.1.1. Acil durum sorumluları atanmalı ve yetki ve sorumlulukları belirlenmeli ve dokümante edilmelidir.
5.1.2. Acil durumlarda kurum içi işbirliği gereksinimleri tanımlanmalıdır.
5.1.3. Acil durumlarda sistem log'ları incelenmek üzere saklanmalıdır.
5.1.4. Güvenlik açıkları ve ihlallerinin rapor edilmesi için kurumsal bir mekanizma oluşturulmalıdır.
5.1.5. Yaşanan acil durumlar sonrası politikalar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmelidir.
5.1.6. Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulmalı ve bu bildirim süreçleri tanımlanmış olmalıdır.
5.1.7. Acil Durum kapsamında değerlendirilen olaylar aşağıda farklı seviyelerde tanımlanmıştır:
- **Seviye A:** Bilgi kaybı. Kurumsal değerli bilgilerin yetkisiz kişilerin eline geçmesi, bozulması, silinmesi.
- **Seviye B:** Servis kesintisi. Kurumsal servislerin kesintisi veya kesintisine yol açabilecek durumlar.
- **Seviye C:** Şüpheli durumlar. Yukarıda tanımlı ilk iki seviyedeki duruma sebebiyet verebileceğinden şüphe duyulan ancak gerçekliği ispatlanmamış durumlar.

5.1.8. Herbir seviyede tanımlı acil durumlarda karşılaşılabilecek riskler, bu riskin kuruma getireceği kayıplar ve bu riskler oluşmadan önce ve oluştuktan sonra hareket planları tanımlanmalı ve dokümante edilmelidir.
5.1.9. Acil durumlarda bilgi güvenliği yöneticisine erişilmeli, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere önceden tanımlanmış ilgili yöneticiye bilgi verilmeli ve zararın tespit edilerek süratle daha önceden tanımlanmış felaket kurtarma faaliyetleri yürütülmelidir.
5.1.10. Bilgi güvenliği yöneticisi tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgili makamlara iletilmelidir.
5.1.11. Olayın türü ve boyutuna göre emniyet veya diğer kurumlara başvurmak gerekebilir. Bu özel olaylar (hırsızlık vb), başvurulacak kurumlar, başvuru şekli (telefon, dilekçe vb), başvuruyu yapacak kurum yetkilisi önceden belirlenmiş ve dokümante edilmiş olmalıdır.

5.2. BİLGİ SİSTEMLERİNDE YEDEKLEME

Bilgi sistemlerinde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigurasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesi gerekir. Sunucular ve veri depolama üniteleri yedekli olarak aynı veya uzak ortamlarda çalışmalıdır. Verinin de operasyonel ortamda online olarak aynı disk sisteminde farklı disk volümlerde ve offline olarak Manyetik kartuş, DVD veya CD ortamında yedekleri alınmalıdır. Taşınabilir ortamlar (Manyetik kartuş, DVD veya CD) fiziksel olarak bilgi işlem odalarından faklı odalarda veya binalarda güvenli bir şekilde saklanmalıdır. Veriler offline ortamlarda süresiz olarak saklanmalıdır. Buna yönelik standartlar şunlardır.

5.2.1. Kurumsal kritik verilerin saklandığı sistemler ile sistem kesintisinin kritik olduğu sistemlerin bir varlık envanteri çıkartılmalı ve yedekleme ihtiyacı bakımından sınıflandırılarak dokümante edilmelidir.

5.2.2. Düzenli yedeklemesi yapılacak varlık envanteri üzerinde hangi sistemlerde ne tür uygulamaların çalıştığı ve yedeği alınacak dizin, dosya Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümante edilmelidir.
5.2.3. Yedekleme konusu bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır. Bu konuyla ilgili sorumluluklar tanımlanmalı ve atamalar yapılmalıdır.
5.2.4. Yedekleri alınacak sistem, dosya ve veriler dikkatle belirlenmeli ve yedeği alınacak sistemleri belirleyen bir yedekleme listesi oluşturulmalıdır.
5.2.5. Yedek ünite üzerinde gereksiz yer tutmamak üzere, kritiklik düzeyi düşük olan veya sürekli büyüyen izleme dosyaları yedekleme listesine dahil edilmemelidir.
5.2.6. Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilmeli ve güncellenmelidir.
5.2.7. Yeni sistem ve uygulamalar devreye alındığında, yedekleme listeleri güncellenmelidir.
5.2.8. Yedekleme işlemi için yeterli sayı ve kapasitede yedek üniteler seçilmeli ve temin edilmelidir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilmelidir.
5.2.9. Yedekleme ortamlarının mümkünse düzenli olarak test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmalıdır.
5.2.10. Geri yükleme prosedürlerinin düzenli olarak kontrol ve test edilerek etkinliklerinin doğrulanması ve operasyonel prosedürlerin öngördüğü süreler dahilinde tamamlanabileceğinden emin olunması gerekir.
5.2.11. Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanmalıdır.
5.2.12. Yedekleme Standardı ile doğru ve eksiksiz yedek kayıt kopyalarının bir felaket anında etkilenmeyecek bir ortamda bulundurulması ve kritik bilgiler için en az üç nesil yedekleme bilgisinin tutulması gerekir.
5.2.13. Veri Yedekleme Standardı; yedekleme sıklığı, kapsamı, gün içinde ne zaman yapılacağı, ne koşullarda ve hangi aşamalarla yedeklerin yükleneceği ve yükleme sırasında sorunlar çıkarsa nasıl geri dönüleceği, yedekleme ortamlarının ne şekilde işaretleneceği, yedekleme testlerinin ne şekilde yapılacağı ve bunun gibi konulara açıklık getirecek şekilde hazırlanmalı ve işlerliği periyodik olarak gözden geçirilmelidir.

5.3. VERİ TABANI GÜVENLİĞİ

Kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) loglanmalıdır. Log kayıtlarına idarenin izni olmadan kesinlikle hiçbir şekilde erişim yapılamamalıdır. Manyetik kartuş, DVD veya CD ortamlarında tutulan log kayıtları en az 5 (beş) yıl süre ile güvenli ortamlarda saklanmalıdır. Veritabanı sunucularının güvenliği hakkında daha detaylı bilgi ve uyulması gereken kurallar şunlardır.

5.3.1. Veritabanı sistemleri envanteri ve bu envanterden sorumlu personel tanımlanmalı ve dokümante edilmelidir.
5.3.2. Veritabanı işletim kuralları belirlenmeli ve dokümante edilmelidir.
5.3.3. Veritabanı sistem logları tutulmalı ve izlenmelidir.
5.3.4. Veritabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli alınması kontrol altında tutulmalıdır.
5.3.5. Yedekleme planları dokümante edilmelidir.
5.3.6. Veritabanı erişim politikaları "Kimlik doğrulama ve Yetkilendirme" politikaları çerçevesinde oluşturulmalıdır.
5.3.7. Hatadan arındırma, bilgileri yedekten dönme kuralları "Acil Durum Yönetimi" politikalarına uygun olarak oluşturulmalı ve dokümante edilmelidir.
5.3.8. Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.
5.3.9. Veritabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmaları yetkili bir personel gözetiminde yapılmalıdır.
5.3.10. Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulmalı ve sonrasında ilgili uygulama kontrolleri gerçekleştirilmelidir.
5.3.11. Bilgi saklama ortamlarının kurum dışına çıkarılması için yetkilendirme yapılması ve bu durumun izleme takip amacıyla kaydedilmesi gerekir.
5.3.12. Sistem dokümantasyonu güvenli şekilde saklanmalıdır.
5.3.13. İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için kurulacak temaslar belirlenmelidir.
5.3.14. Veritabanı serverda sadece ssh açık olmalı ftp, telnet, remote vb. bağlantılara kapalı olmalıdır.
5.3.15. Veritabanı servera veritabanı yöneticisi dışında hiçbir kullanıcı ssh bağlantı yapma yetkisi olmamalıdır.
5.3.16. Application serverlardan veritabanına rlogin vb. şekilde erişememelidir.
5.3.17. Veritabanı serverların şifresi sorumlu kişiler dışında bir zarfa yazılıp bantlanıp imzalanıp üst düzey yöneticisinin kasasında saklanmalıdır. Çok kritik bilgilere erişim için çift şifreleme mekanizması olmalıdır. Bu durumda en az iki kullanıcı bir şifreyi tamamlayacak olup birbirlerinin şifrelerini bilmeyeceklerdir.
5.3.18. Arayüzden gelen kullanıcılar bir tabloda saklanmalı bu tablodaki kullanıcı adı ve şifreleri şifrelenmiş olmadır.
5.3.19. Veritabanında güvenliği önemli veriler mutlaka şifrelenmelidir. Bu sayede verileri taşınsa bile orjinallerine erişilmemesi sağlanır.
5.3.20. Veritabanı servera root olarak hiçbir kullanıcı bağlanmamalı. Bağlanması gereken kişilere kendi adında belli yetkilerle kullanıcı oluşturulmalıdır. Bu kullanıcıların yaptıkları işlemler loglanmalıdır. Root şifresi sadece sistem yöneticisinde olmalıdır.
5.3.21. Veritabanında Veritabanı yöneticisi dışında SYSDBA,DBA yetkili kullanıcı olmamalıdır.
5.3.22. Veritabanında bulunan farklı Schemaların kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenmelidir.
5.3.23. Veritabanına internetten direkt bağlantı kesinlikle engellenmelidir.
5.3.24. Veritabanı server a Sistem yöneticisi, Veritabanı Yöneticisi ve application server dışında hiçbir kullanıcı erişememelidir, ip bazında kısıtlana yapılmalıdır.
5.3.25. Veritabanı servera kod geliştiren kullanıcı dışında hiçbir kullanıcı bağlanıp sorgu yapamamalıdır. İstekler arayüzden sağlanmalıdır.(Kullanıcılara tablolardan select yapamamalılar)
5.3.26. Veritabanına giden veri trafiği şifrelenmelidir. (Networku dinleyen verilere ulaşamamalıdır.)
5.3.27. Bütün şifreler düzenli aralıklarla değiştirilmelidir. Detaylı bilgi için şifreleme politikasına bakılmalıdır.

5.4. ŞİFRELEME

Şifreleme, bilgisayar güvenliği için önemli bir özelliktir. Kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir şifre, ağ güvenliğini tümüyle riske atabilir. Güçlü bir şifreleme oluşturulması, oluşturulan şifrenin korunması ve bu şifrenin değiştirilme sıklığı hakkındaki standartlar ve uyulması gereken kurallar şunlardır.

5.4.1. Genel Bilgiler
5.4.1.1. Bütün sistem seviyeli şifreler (örnek, root, administrator, enable, vs) en az üç ayda bir değiştirilmelidir.

5.4.1.2. Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web, masaüstü bilgisayar vs.) en az altı ayda bir değiştirilmelidir. Tavsiye edilen değiştirme süresi her dört ayda birdir.
5.4.1.3. Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.
5.4.1.4. Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
5.4.1.5. SNMP kullanıldığı durumlarda varsayılan olarak gelen "public", "system" ve "private" gibi community string'lere farklı değerler atanmalıdır.
5.4.1.6. Kullanıcı, şifresini başkası ile paylaşmaması, kağıtlara yada elektronik ortamlara yazmaması konusunda eğitilmelidir.
5.4.1.7. Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.
Bütün kullanıcı ve sistem seviyeli şifrelemeler aşağıdaki ana noktalara uymalıdır.

5.4.2. Genel Şifre Oluşturma Kuralları
Şifreler değişik amaçlar için kullanılmaktadır. Bunlardan bazıları: Kullanıcı şifreleri, web erişim şifreleri, e-posta erişim şifreleri, ekran koruma şifreleri, yönlendirici erişim şifreleri vs.). Bütün kullanıcılar güçlü bir şifre seçimi hakkında özen göstermelidir.

Zayıf şifreler aşağıda belirtilen karakteristiklere sahiptir.

- Şifreler sekizden daha az karaktere sahiptirler.
- Şifreler sözlükte bulunan bir kelimeye sahiptir.
- Şifreler aşağıdaki gibi ortak değere sahiptir.
  - Ailesinin, arkadaşının, sahip olduğu bir hayvanın veya bir sanatçının ismine sahiptir.
  - Bilgisayar terminolojisi ve isimleri, komutlar, siteler, şirketler, donanım veya yazılım gibi.
  - "Sağlık", "istanbul", "ankara" gibi isimler.
  - Doğum tarihi veya adres ve telefon numaraları gibi kişisel bilgiler.
  - Aaabbb, qwerty,zyxwuts, 123321 vs. Gibi sıralı harf veya rakamlar.
  - Yukardaki herhangi bir kelimenin geri yazılış şekli.
  - Yukarıdaki herhangi bir kelimenin rakamla takip edilmesi (örnek ,gizli1, gizli2).

Güçlü şifreler aşağıdaki karakteristiklere sahiptir.

- Küçük ve büyük karakterlere sahiptir (örnek, a-z, A-Z)
- Hem dijit hemde noktalama karakterleri ve ayrıca harflere sahiptir. (0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- En az sekiz adet alfanümerik karakttere sahiptir.
- Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.
- Aile isimleri gibi kişisel bilgilere ait olmamalıdır.
- Şifreler herhangi bir yere yazılmamalıdır veya elektronik ortamda tutulmamalıdır. Kolayca hatırlanabilen şifreler oluşturulmalıdır. Örnek olarak; "olmaya devlet cihanda bir nefes sıhhat gibi" cümlesi "OdC1nSg!" veya türevleri şeklinde olabilir. Not: Yukarıdaki herhangi bir örneği şifre olarak kullanmayınız.

5.4.3. Şifre Koruma Standartları
Sağlık Bakanlığı bünyesinde kullanılan şifreleri kurum dışında herhangi bir şekilde kullanmayınız. (örnek, internet erişim şifreleri, bankacılık işlemlerinde veya diğer yerlerde). Değişik sistemler için farklı şifreleme kullanın. Örnek, Unix sistemler için farklı şifre, Windows sistemler için farklı şifre kullanınız.

Bakanlık bünyesinde kullanılan şifreleri herhangi bir kimseyle paylaşmayınız. Bütün şifreler Bakanlığa ait gizli bilgiler olarak düşünülmelidir.

Aşağıdakiler yapılmayacakların listesidir:

- Herhangi bir kişiye telefonda şifre vermek.
- e-posta mesajlarında şifre belirtmek.
- Üst yöneticinize şifreleri söylemek.
- Başkaları önünde şifreler hakkında konuşmak.
- Aile isimlerini şifre olarak kullanmak.
- Herhangi form üzerinde şifre belirtmek.
- Şifreleri aile bireyleri ile paylaşmak.
- Şifreleri işten uzakta olduğunuz zamanlarda iş arkadaşlarınıza bildirmek.

Herhangi bir kimse şifre isteğinde bulunursa bu dökümanı referans göstererek Bilgi İşlem birimi yetkilisini aramasını söyleyiniz.

Uygulamalardaki "şifre hatırlama" özelliklerini seçmeyiniz. (örnek, Outlook, Internet Explorer vs.)

Tekrar etmek gerekirse, şifreleri herhangi bir yere yazmayınız ve herhangi bir ortamda elektronik olarak saklamayınız.

Şifreler an az altı ayda bir değiştirilmelidir (sistemlerin şifreleri ise en az üç ayda bir değiştirilmelidir). Tavsiye edilen aralık ise 3 ayda birdir.

Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıya şifresini değiştirmesi talep edilecektir.

5.4.4. Uygulama Geliştirme Standartları
5.4.4.1. Uygulama geliştiricileri programlarında aşağıdaki güvenlik özelliklerinin sağlandığından emin olmalıdırlar.
5.4.4.2. Bireylerin (grupların değil) kimlik doğrulaması (authentication) işlemini destekleyebilmelidir.
5.4.4.3. Şifreleri text olarak veya kolay anlaşılabilir formda saklamamalıdır.
5.4.4.4. Kural yönetim sistemini desteklemelidir. (Örnek; bir kullanıcı diğer bir kimsesin şifresini bilmeden fonksiyonlarına devam edebilmesi.)
5.4.4.5. Mümkün olduğu kadar TACACS+ , RADIUS ve/veya X.509/LDAP güvenlik protokollerini desteklemelidir.

5.4.5. Uzaktan Erişen Kullanıcılar için Şifre Kullanımı
Kurumun bilgisayar ağına uzaktan erişim tek yönlü şifreleme algoritması veya güçlü bir passphrase ile yapılacaktır.

5.4.6. Passphrase
Bir passphrase standart şifrelerden daha uzun karakter dizisine sahiptir (genellikle 4'ten 16'ya kadar karaktere sahiptir), dijital imzaların (bir mesajı gönderen kişinin gerçekten o kişi olduğunu kanıtlayan kodlanmış bir imza), mesajların kodlanması veya çözülmesinde kullanılır.
Passphrase'ler şifreler gibi değildir. Passphrase şifrelerden daha uzundur, dolayısı ile daha güvenlidir.
Passphrase'ler tipik olarak birçok kelimeden ibarettir. Bundan dolayı passphrase'ler "sözlük" saldırılarına karşı daha güvenlidir.
İyi bir passphrase büyük ve küçük harf ve rakamlardan oluşan kombinasyona sahiptir.
Örnek bir passphrase:
"*?#>*@1012inciCaddekiTrafik*&#!#BuSabah"
Şifreleme için geçerli olan bütün kurallar passphrase'ler için de geçerlidir.

5.5. SUNUCU GÜVENLİĞİ

Sunucuların güvenliğinin sağlanması için uyulması gereken kurallar ve standartlar şunlardır.

5.5.1 Genel Bilgiler
5.5.1.1 Sahip Olma ve Sorumluluklar
Kurum bünyesindeki bütün dahili sunucuların yönetiminden sistem yöneticileri sorumludur.
Sunucu konfigurasyonları sadece bu grup tarafından yapılacaktır.
5.1.1.1. Bütün sunucular ilgili kurumun yönetim sistemine kayıt olmalıdır. En az aşağıdaki bilgileri içermelidir:
- Sunucuların yeri ve sorumlu kişi.
- Donanım ve İşletim Sistemi.
- Ana görevi ve üzerinde çalışan uygulamalar.
- İşletim Sistemi versiyonları ve yamalar.

5.1.1.2. Bütün bilgiler tek bir merkezde güncel olarak tutulmalıdır.
Genel Konfigurasyon Kuralları
5.1.2.1. İşletim sistemi konfigurasyonları Bilgi İşlem Biriminin talimatlarına göre yapılacaktır.
5.1.2.2. Kullanılmayan servisler ve uygulamalar kapatılacaktır.
5.1.2.3. Eğer mümkünse servislere erişimler için log tutulacak (örnek; TCP Wrapper) ve erişim kontrol metotlarıyle koruma sağlanacaktır.
5.1.2.4. Sunucu üzerinde çalışan işletim sistemlerinin, hizmet sunucu yazılımlarının ve anti-virüs vb. koruma amaçlı yazılımların sürekli güncellenmesi sağlanmalıdır. Mümkünse, yama ve anti virüs güncellemeleri otomatik olarak yazılımlar tarafından yapılmalı, ancak değişiklik yönetimi kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanmalıdır.
5.1.2.5. Uygulama erişimleri için standart güvenlik prensiplerini çalıştırın, gereksiz servisleri açmayın.
5.1.2.6. Sistem yöneticileri gerekli olmadığı durumlar dışında "Administrator" ve "root" gibi genel kullanıcı hesapları kullanmamalı, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmalıdır. Genel yönetici hesapları yeniden adlandırılmalıdır. Gerekli olduğunda önce kendi hesapları ile log-on olup, daha sonra genel yönetici hesaplarına geçiş yapmalıdırlar.
5.1.2.7. Ayrıcalıklı bağlantılar teknik olarak mümkünse güvenli kanal (SSH veya IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
5.1.2.8. Sunucular fiziksel olarak erişim kontrollü sistem odalarında bulunmalıdırlar.

5.5.2. Gözlemleme
5.5.2.1. Kritik sistemlerde oluşan bütün güvenlikle ilgili olaylar loglanmalıdır ve aşağıdaki şekilde saklanmalıdır:
- Bütün güvenlikle ilgili loglar minimum 1 hafta saklanmalıdır ve online olarak erişilmelidir.
- Günlük tape backupları en az 1 ay saklanmalıdır.
- Logların haftalık tape backupı en az 1 ay tutulmalıdır.
- Aylık full backuplar en az 6 ay tutulmalıdır.

5.5.2.2. Güvenlikle ilgili loglar sorumlu kişi tarafından değerlendirilecek ve gerekli tedbirleri alacaktır. Güvenlikli ilgili olaylar aşağıdaki gibi olabilir fakat bunlarla sınırlı değildir.
- Port tarama atakları.
- Yetkisiz kişilerin ayrıcalıklı hesaplara erişmeye çalışması.
- Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar.

5.5.3. Uygunluk
5.5.3.1. Denetimler yetkili organizasyonlar tarafından Bakanlık bünyesinde belli aralıklarda yapılacaktır.
5.5.3.2. Denetimler Bilgi İşlem grubu tarafından yönetilecektir.
5.5.3.3. Denetimler organizasyonun işleyişine zarar vermemesi için maksimum gayret gösterilecektir.
5.5.4. İşletim
5.5.4.1. Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir.
5.5.4.2. Sunucuların yazılım ve donanım bakımları üretici tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılmalıdır.
5.5.4.3. Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve kayıt edilmelidir.

5.6. KİMLİK DOĞRULAMA VE YETKİLENDİRME

Bilgi sistemlerinde Kimlik Doğrulama ve Yetkilendirme, konusunda alınması gereken önlemler, uyulması gereken kurallar ve standartlar şunlardır.

5.6.1. Kurum sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecek ve dokümante edilecektir.
5.6.2. Kurum sistemlerine erişmesi gereken kurum dışı ve extranet kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanacak ve dokümante edilecektir.
5.6.3. Bakanlık bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veritabanları, işletim sistemleri, ve log-on olarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkiler belirlenmeli, dokümante edilmeli ve denetim altında tutulmalıdır.

5.6.4. Tüm kurumsal sistemler üzerindeki kullanım hakları (kullanıcıların kendi sistemlerine yönelik olarak birbirlerine verdikleri haklar dahil) periyodik olarak gözden geçirilmeli ve gereksinimler ve gerekli minimum yetkinin verilmesi prensibi doğrultusunda revize edilmelidir.
5.6.5. Erişim ve yetki seviyelerinin sürekli güncelliği temin edilmelidir.
5.6.6. Kullanıcılar kurum adına kullanımları için tahsis edilmiş sistemlerin güvenliğinden sorumludurlar.
5.6.7. Sistemlere başarılı ve başarısız erişim logları düzenli olarak tutulmalı, tekrarlanan başarısız log-on girişimleri incelenmelidir.
5.6.8. Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.
5.6.9. Sistemlere log-on olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve yetki ihlalleri kontrol edilmelidir.
5.6.10. Kullanıcılara erişim haklarını yazılı olarak beyan edilmeli ve erişim haklarını ihlal eden kullanıcılar için ilgili politika maddesi uygulanmalıdır.
5.6.11. Kullanıcı hareketlerini izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.
5.6.12. Sistemler üzerindeki tüm roller, rollere sahip kullanıcılar, ve rollerin sistem kaynakları üzerindeki yetkileri, uygun araçlar kullanılarak belirli aralıklarla listelenmelidir. Bu listeler yetki matrisleri ile karşılaştırılmalıdır. Eğer uyumsuzluk var ise nedenleri araştırılmalı, ve dokümanlar veya yetkiler düzeltilerek uyumlu hale getirilmelidir.

5.7. KİŞİSEL SAĞLIK KAYITLARININ GÜVENLİĞİ

Kişisel sağlık kaydı kapsamına, hasta ile ilgili sözlü bilgi, yazılı bilgi, tıbbı müdahaleler, ön tanı, teşhisler, grafik imajları, fatura gibi konular girmektedir.

Kişisel sağlık kayıtlarının güvenliğinin sağlanması amacıyla; Bakanlığımıza bağlı bütün kurum ve kuruluşlarda (merkez ve taşra teşkilatları, hastaneler, sağlık ocakları, aile hekimleri vs.) hasta sağlık bilgisinin mahremiyeti hususunda uyulması gereken temel kurallar şunlardır.

5.7.1. Genel Kurallar
Bütün kişisel ve kurumsal bilgilerin (klinik, idari, mâli vb.) güvenliğinin sağlanması için aşağıda belirtilen hususlara dikkat edilmelidir.

5.7.1.1. Veri güvenliği konusunda üç temel prensibin göz önüne alınması gerekmektedir. Bunlar; gizlik, bütünlük ve erişilebilirliktir.
5.7.1.2. Kurumda kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi tanımlanmalıdır. Rol bazlı yetkilendirme yapılmalıdır ve yetkisiz kişilerin hastanın sağlık kayıtlarına erişmesi mümkün olmamalıdır.
5.7.1.3. Sağlık kayıt bilgileri hastaya aittir. Yetkilendirilmiş çalışanlar ancak kendisine kayıtlı olan hastaların sağlık kayıtlarına erişebilmelidirler. Ancak hastanın yazılı onayı ile diğer sağlık çalışanları bu veriye erişebilirler.
5.7.1.4. Hasta taburcu olmuş ise hiçbir kurum çalışanı hastanın sağlık kayıtlarına erişemez.
5.7.1.5. Hastanın rızası olmadan hiçbir çalışan sözle de olsa hasta sağlık bilgilerini hastanın yakınları dışında üçüncü şahıslara ve kurumlara iletemez.
5.7.1.6. Hasta sağlık bilgileri ticari amaçlı olarak da üçüncü şahıslara iletilemez. Hastanın kullandığı ilaçlar, diyet programları vs. buna dahildir.
5.7.1.7. Hasta dosyasının bir kopyası hastaya teslim edilmelidir. İlgili mevzuat hükümleri saklı kalmak kaydıyla hiç bir hasta kaydı, elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilmemelidir.
5.7.1.8. Hastanın dosyasının izlenmemesi için gerekli tedbirler alınmalıdır. [Hasta dosyalarının gelişigüzel ortada bırakılmaması, bilgisayar ekranının başkalarınca okunabilecek şekilde bırakılmaması gibi]
5.7.1.9. Telefon ile konuşurken hasta ile ilgili mahrem bilgilerin üçüncü şahısların eline geçmemesine azami özen göstermelidir.
5.7.1.10. Bütün hasta sağlık kayıtları fiziksel olarak korunmuş mekanlarda saklanmalıdır.
5.7.1.11. Elektronik hasta kayıtlarına internet ortamından erişim mümkün olmamalıdır.
5.7.1.12. Hasta sağlık bilgileri bilginin üretildiği kurum tarafından veya Bakanlığımızın Bilgi Yönetim sistemleri tarafından araştırma, istatistik ve Karar Destek Sistemleri için kullanılabilir. Bu durumda hasta sağlık bilgisi hasta tanımlayıcısı ile ilişkilendirilemez.

5.7.2. Sistem Güvenliği
5.7.2.1. Veriye erişirken dört temel prensibin gerçekleştirilmesi gerekmektedir. Bunlar; İzlenebilirlik, kimlik sınama, güvenirlik ve inkar edilememedir.
5.7.2.2. Sağlık kurumları bünyesinde hasta tanımlayıcı olarak TC Kimlik numarası baz alınacaktır. Veri tabanlarında hiçbir zaman hastalık tanısı ile TC kimlik numarası eşleşmeyecek, TC kimlik numarasından tek yönlü algoritma ile türetilmiş özel bir tanımlayıcı numara kullanılacaktır.
5.7.2.3. Bilgi sistemlerinde güvenlik veriye erişim bazında olacaktır. Bunun için bu sistemin özellikle yazılım ve veritabanı erişim katmanlarında özel uygulamalar oluşturulacaktır. **Veriye erişecek kişiler aşağıdaki şekilde tanımlanmıştır:**

- Hasta kendi verisine online olarak hiçbir zaman erişmemelidir.
- Bir Aile hekimi ancak kendisine kayıtlı olan hastaların elektronik sağlık kayıtlarına erişebilmelidir.
- Hastanedeki yetkilendirilmiş sağlık çalışanları ise, ancak hastanın giriş tarihinden, taburcu olana kadar geçen zaman içerisinde ve ancak hasta kendisi ile ilgili sağlık kayıtlarının erişimine yazılı olarak onay vermiş ise hastanın elektronik sağlık kayıtlarına erişebilirler. Ve bu da "geçici bir süreliğine" olacaktır.

5.7.2.4. Sistem yöneticilerine de bir güvenlik katmanı konulacaktır. Bunun için veritabanı yazılımının gelişmiş güvenlik yönetimi özellikleri kullanılacaktır.
5.7.2.5. Gerektiğinde saat ve/veya gün bazında belirlenen bir sure için bazı kullanıcı ve istemci makinelerin sisteme oturum açmalarına kısıtlama getirilebilmelidir.
5.7.2.6. Aynı kullanıcı kodu ile aynı anda birden fazla oturum açılmasına izin verilmemelidir.
5.7.2.7. Eğer hasta, herhangi bir sağlık çalışanının elektronik sağlık kayıtlarına erişmesini istemiyorsa, sağlık çalışanı ilgili dosyayı okuma hakkına kavuşamamalıdır. Fakat sağlık çalışanı muayene sonuçlarını hastanın veri tabanına aktarabilmelidir. Bu diğer doktorlar tarafından yazılan kayıtlara erişilmemesi için kullanılan metottur.
5.7.2.8. Sadece yetkisi olan kullanıcılar için veri girişi ve/veya verinin elde edilmesi için erişim izni verilmelidir. Birçok kullanıcının veri tabanında sadece belirli bir veri setine erişim yetkisinin denetlenebilmesini sağlamak için çok katmanlı denetim mekanizmaları olmalıdır.
5.7.2.9. Veri tabanında tutulacak verilerin tutarlılığı tam ve kesin bir şekilde sağlanmalıdır. Bunu sağlamak için en azından, veri onay (validation), çapraz sorgulama (cross-checking) ve mükerrer kayıt önleme gibi ölçütler uygulanmalıdır.
5.7.2.10. Yönetimsel analizler yapmak için veri tabanındaki veriler bir yerden başka bir yere aktarılırken, kayıtlarda bulunan kişisel kimlik tanımlayıcıları kayıtlardan çıkartılmalı ve analizler hasta ile hastalık bilgilerini eşleştirmeden yapılmalıdır.
5.7.2.11. Kullanıcı aktiviteleri (yapılan tüm işlemler ve erişimler) izlenebilmelidir. Veri tabanı üzerinde yapılan şüpheli işler denetlenebilmelidir. Sistemin hem etkin bir şekilde yönetilmesi, hem de yetkisiz erişimlerin engellenmesi ve izlenmesi anlamında gelişmiş bir kontrol mekanizması olmalıdır. Sistem, hangi kullanıcının sistemin hangi kısmına ne zaman ve nereden eriştiğine dair (zaman damgası-date stamp, işlem, kullanılan istemci bilgisayar tanımı gibi bilgileri de içeren) kayıt tutmalıdır.

5.7.2.12. Sistem yöneticilerinin kimlik tanımlama ve doğrulaması için X.509v3 uyumlu sayısal sertifikalar kullanılmalıdır. Sayısal sertifikaların güvenli depolaması için akıllı kartlar veya usb token cihazları kullanılmalıdır.

5.7.2.13. Sertifika tabanlı kimlik doğrulama yapılmadığı halde password ve hash tabanlı kimlik doğrulama yapılacaktır. Sistemlere erişim için tek yönlü şifreleme algoritmaları kullanılacaktır.

Kurum içerisinde veya Kurum ile başka ağlar arasındaki tüm haberleşme şifreli yapılmalıdır. Bütün iletişim VPN ve Açık Anahtar Alt Yapısı (PKI) teknolojilerini kullanmalıdır.

EK-3: HES Uygulamasının Son Güncel Aydınlatma Metni

TÜRKİYE CUMHURİYETİ
SAĞLIK BAKANLIĞI
HAYAT EVE SIĞAR (HES) UYGULAMASI

Aydınlatma Metni

Bu Aydınlatma Metni, 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun ("KVK Kanunu") "Veri Sorumlusunun Aydınlatma Yükümlülüğü" kenar başlıklı 10 uncu maddesi uyarınca ve KVK Kanunu kapsamında veri sorumlusu olan T.C. Sağlık Bakanlığı (Bakanlık) tarafından, COVID-19'la mücadele etmek veya hastalığın yayılmasını azaltmak için temaslı ya da enfekte olmuş kişileri takip eden veya izleyen, kişilerin seyahat etmeye veya kamusal alanlara girmeye uygun olup olmadığını belirlemek amacıyla güncel enfeksiyon durumunu veya enfeksiyon geçmişini doğrulayan bir uygulama olan Hayat Eve Sığar Uygulaması (HES Uygulaması) kullanıcılarına, kullanıcılara ait kişisel veriler hususunda bilgilendirme yapmak amacıyla hazırlanmıştır. KVK Kanunu uyarınca veri sorumlusu sıfatını haiz Bakanlığın merkez adresi "Bilkent Yerleşkesi, Üniversiteler Mah. Dumlupınar Bulvarı 6001. Cad. No:9 Çankaya/Ankara 06800"dir.

Veri Sorumlusunun Kimliği

Bu uygulamada işlenen kişisel verileriniz bakımından veri sorumlusu T.C. Sağlık Bakanlığı'dır.

Kişisel Verilerin İşlenme Amaçları

Bu uygulamada aşağıda yer alan kişisel verileriniz şu amaçlarla işlenebilmektedir:

- **Kimlik verisi:** T.C. kimlik numarası, baba adı ve doğum tarihi bilgileriniz kimliğinizin doğrulanması ve sağlık hizmeti süreçlerinin yürütülmesi amacıyla işlenebilmektedir. Bu verilerinizi beyan etmeksizin de uygulamayı bazı kısıtlamalarla kullanabilmektesiniz. T.C. kimlik numaranızı HES Uygulaması aracılığıyla beyan etmeyi tercih etmemeniz halinde, COVID-19 riskinizin hesaplanabilmesi için yaş bilginizi paylaşmanız gerekmektedir.
- **İletişim verisi:** Cep telefonu numarası bilginiz HES Uygulamasını ilk yüklediğinizde, SMS ile gönderilecek olan kodu girmek, telefon numarası bilginizi doğrulayarak bilgi güvenliğini sağlamak ve sağlık hizmeti süreçlerinin yürütülmesi amacıyla işlenebilmektedir. Her cep telefonu numarası ile HES Uygulamasına yalnızca bir kez kayıt olunabilmekte; aynı cep telefonu numarası ile birden fazla kişinin HES Uygulamasını kullanma imkânı bulunmamaktadır. Ayrıca HES Uygulamasının "Aile" sekmesinde takip etmek istediğiniz sevdiklerinize davetiye göndermek için onların cep telefon numaralarını girmeniz veya kişi listesinden seçmeniz gerekmektedir.
- **Konum verisi:** Konum bilginiz harita üzerinde konumuzun gösterilmesi, bulunduğunuz bölgede COVID-19 pozitif ve risk yoğunluğunun harita üzerinden gösterilmesi, izolasyon altında bulunduğunuz lokasyonun belirlenmesi, bu lokasyonu terk etmeniz durumunda tarafınıza bildirim gönderilmesi ve ilgili makamlara bilgi verilmesi amaçlarıyla işlenebilmektedir.
- **Sağlık verisi:** Sağlık bilgileriniz, COVID-19 riskinizin belirlenmesi ve sağlık hizmeti süreçlerinin yürütülmesi amacıyla işlenebilmektedir. Yöneltilen sorulara vereceğiniz yanıtlara göre en yakın sağlık tesisini ziyaret etmeniz istenebilecek veya periyodik aralıklarla hastalık belirtileriniz hakkında tarafınıza sorular yöneltilebilecektir. Risk durumu bilginiz HES Kodlarınızda riskli/risksiz durum bilginizin görüntülenebilmesi ile sağlık hizmeti faaliyetinin yürütülmesi amacıyla işlenecektir.
- HES Kodunuz aracılığıyla ayrıca COVID-19 aşı durumunuz, son 6 ay içerisinde COVID-19 hastalığını geçirip geçirmediğiniz, son 72 saat içerisinde sonucu negatif çıkmış bir PCR testinizin olup olmadığı bilgileriniz de paylaşılabilecektir. Sayılan bu bilgileri HES Kodu aracılığıyla paylaşmak istememeniz halinde;
    - HES Uygulamasını indirebilir, HES Uygulaması üzerinde yer alan "HES Kodu Ayarlarım" sekmesi üzerinden HES Kodu ayarlarınızı değiştirebilirsiniz. Sayılan bu bilgileri HES Kodu aracılığıyla paylaşıma dilediğiniz zaman açabilir veya kapatabilirsiniz.
    - Ayrıca 2023 kısa numarasına göndereceğiniz SMS ile HES IZIN yazıp aralarında boşluk bırakarak sırasıyla, T.C. Kimlik Numarası, T.C. Kimlik Seri Numarasının son 4 hanesi ve RET" yazabilir, sayılan bu bilgilerin HES Kodu aracılığıyla paylaşımını kapatabilirsiniz.
    - Mavi Kart sahibiyseniz veya T.C. Kimlik Numaranız 97, 98, 99 ile başlıyor ise HES IZIN yazıp aralarına boşluk bırakarak sırasıyla, T.C. Kimlik Numarası, doğum yılı ve RET" yazabilir, 2023 kısa numarasına SMS gönderebilirsiniz.
    - T.C. Kimlik Numaranız veya 99, 98, 97 ile başlayan Yabancı Kimlik Numaranız bulunmuyor ise, Pasaport bilgileriniz ile "HES IZIN yazıp aralarında boşluk bırakarak sırasıyla, Uyruk, Pasaport Seri Numarası, Doğum yılı, Soyadı, RET" yazabilir 2023'e SMS gönderebilirsiniz.
    - HES Kodu ayarlarınızı dilediğiniz zaman yukarıda tanımlanan usul ile ve "RET" yerine "KABUL" yazarak değiştirebilir; HES Kodunuz aracılığıyla ayrıca COVID-19 aşı durumunuz, son 6 ay içerisinde COVID-19 hastalığını geçirip geçirmediğiniz, son 72 saat içerisinde sonucu negatif çıkmış bir PCR testinizin olup olmadığı bilgilerinizi yeniden paylaşıma açabilirsiniz.
- **Meslek verisi:** Sağlık çalışanı olup olmadığınız ve eğer sağlık çalışanıysanız hastalarla temasınızın olup olmadığı bilgisi, hastalık riski seviyesini belirlemek amacıyla işlenebilmektedir.
- **Bluetooth verisi:** HES Uygulaması üzerinden izin vermeniz dahilinde kullanıcıların sosyal mesafeyi koruyarak sağlıklı kalmasına yardımcı olunması adına bluetooth bilginiz işlenebilmektedir. Bu izin uygulama içerisinde gelecek olan uyarı penceresi sayesinde verilebilecektir.
- **Kamera verisi:** HES Uygulaması üzerinden izin vermeniz dahilinde HES Kodu QR Kod fotoğrafını çekmek için kamera bilginiz işlenebilmekte ve arka planda işlem güvenliği süreçlerinin yürütülebilmesi amacıyla kaydedilebilmektedir. Bu izin uygulama içerisinde gelecek olan uyarı penceresi sayesinde verilebilecektir.
- **Kişi listesi verisi:** HES Uygulaması üzerinden izin vermeniz dahilinde kullanıcıların kişi listesinden sevdiklerini ekleyerek takip edebilmesi için kişiler (telefon rehberi) bilginiz işlenebilmektedir. Bu izin uygulama içerisinde gelecek olan uyarı penceresi sayesinde verilebilecektir.

- **Dosya (Video/Ses/Görüntü) verisi:** HES Uygulaması üzerinden izin vermeniz dahilinde kural ihlal bildiriminde bulunurken beyanlarınızı destekleyecek video, ses ve görüntü bilginiz virüsün kontrol altına alınması ve işlem güvenliği süreçlerinin yürütülebilmesi amacıyla işlenebilmekte ve kaydedilebilmektedir. İlgili video, ses ve görüntü telefon hafızasından dosya yüklemek suretiyle veya uygulama üzerinden kamera ile sağlanmaktadır. Bu izin uygulama içerisinde gelecek olan uyarı penceresi sayesinde verilebilecektir. Uygulamada "Covid-19 Aşı Bilgilerim" menüsünden aşı kartı oluşturulabilmekte ve telefon hafızasına pdf dosya türünde kaydedilebilmektedir.

Kullanım ve Telif Hakları Bakanlığımıza Ait Olan Diğer Uygulamalar

Uygulama içerisinde bulunan aşağıdaki tüm uygulamaların kullanım, yayım, telif vb. tüm hakları tamamen Bakanlığımıza aittir.

- **Sağlık Bakanlığı:** Bakanlığımızın resmî web sitesidir.
- **Merkezi Hekim Randevu Sistemi (MHRS):** Vatandaşların Sağlık Bakanlığına bağlı hastaneler ile ağız ve diş sağlığı merkezleri ve aile hekimlerine Alo182 arayarak canlı operatörlerden, web üzerinden ya da MHRS mobil uygulamasından kendilerine istedikleri hastane ve hekimden randevu alabilecekleri bir sistemdir.
- **e-Nabız:** e-Nabız sağlık kuruluşlarından toplanan sağlık verilerine vatandaşların ve sağlık profesyonellerinin internet ve mobil cihazlar üzerinden erişebilecekleri bir uygulamadır.
- **HealthPass:** Vatandaşların aşı, test ve bağışıklık sertifikalarını uluslararası standartlarda saklayabileceği ve seyahat esnasında kolaylıkla kullanabileceği bir uygulamadır.
- **Korona Önlem:** Vatandaşların yeni koronavirüs (COVID-19) semptomlarına göre ön değerlendirme yapması ve yapılan ön değerlendirmenin olumlu çıkması durumunda bir sağlık tesisini ziyaret etmesi tavsiyesinde bulunmak amacıyla geliştirilen bir uygulamadır.
- **Türkiye'ye Giriş Formu:** Kişilerin Türkiye'de kalacağı süre boyunca Covid-19 pandemisi ile ilgili kişilere sağlıklı bilgi aktarabilmek, kişilerin ve sevdiklerinin sağlığını koruyabilmek adına geliştirilmiş bir web sitesidir.
- **İlacımı Kontrol Et (İTS Mobil):** Türkiye'de kullanıma sunulan ilaçların, ambalaj üzerindeki karekodunu okutarak sisteme kayıtlı olup olmadığını sorgulayıp ilaç hakkında detaylı bilgilere erişebileceğiniz bir uygulamadır.
- **Maskemi Kontrol Et (ÜTS Mobil):** İster Türkiye'de üretilsin ister ithal edilsin tıbbi cihazların ve kozmetik ürünlerin kullanıcılar tarafından takibinin gerçekleştirilmesini sağlayan bir sistemdir..

Kişisel Verilerin Aktarımı

HES Uygulamasındaki kişisel verileriniz KVK Kanunu'nun 28 inci maddesinin ilk fıkrasında yer alan muafiyet halleri saklı kalmak üzere, hiçbir şekilde üçüncü taraflarla paylaşılmamaktadır.

Kişisel Veri Toplamanın Yöntemi ve Hukuki Sebebi

Kişisel verileriniz tamamen otomatik yollarla HES Uygulaması aracılığıyla elde edilmektedir. Kişisel verileriniz;

- KVK Kanunu'nun 5 inci maddesinin ikinci fıkrasının (a) bendi uyarınca kanunlarda açıkça öngörülmesi ve (ç) bendi uyarınca veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması ve
- KVK Kanunu'nun 6 ncı maddesinin üçüncü fıkrası uyarınca; 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 kişiler veya yetkili kurum ve kuruluşlar tarafından işlenmesi

hukuki sebeplerine dayanılarak işlenebilmektedir.

İlgili Kişilerin Hakları ve Veri Sorumlusuna Başvuru

HES Uygulaması Kullanıcıları KVK Kanunu'nun 11 inci maddesinde düzenlenen haklarını, KVK Kanunu'nun 13 üncü maddesi ve Veri Sorumlusuna Başvuru Usul ve Esasları Hakkında Tebliğ hükümleri çerçevesinde Bakanlığa başvurmak suretiyle kullanabilir.

KVK Kanunu'nun 13 üncü maddesi uyarınca yapılacak yazılı başvurular "T.C. Sağlık Bakanlığı, Üniversiteler Mahallesi, 6001. Cadde, No:9, Çankaya, Ankara" adresine; Kayıtlı Elektronik Posta (KEP) ile yapılacak başvurular ise "sb@hs01.kep.tr" adresine iletilmelidir.

EK-4: Uludağ Üniversitesi Tıp Fakültesi Klinik Araştırmalar Etik Kurulu İzin Yazısı

T.C.
ULUDAĞ ÜNİVERSİTESİ
Tıp Fakültesi Klinik Araştırmalar Etik Kurulu

Sayı : 2011-KAEK-26/489 13/08/2021
Konu : Etik Kurul kararı

Sayın Prof.Dr.M.Murat CİVANER
Bursa Uludağ Üniversitesi Tıp Fakültesi
Tıp Tarihi ve Etik Anabilim Dalı Öğretim Üyesi

Kurulumuza başvurusunu yaptığınız ve sorumlu araştırıcısı olduğunuz *"Sağlıkta büyük veri: Etik değerleri gözeten bir model önerisi"* başlıklı araştırmanız ile ilgili kurulumuzun 11 Ağustos 2021 tarih, 2021-11/1 nolu kararı ekte gönderilmektedir.

Araştırmanın tamamlanma bildiriminin ve özet sonuç raporunun kurulumuza iletilmesi için bilgilerinize sunulur.

Prof.Dr.Mustafa HACIMUSTAFAOĞLU
Kurul Başkanı

EK:
-Karar (1 adet)

EK-4: Uludağ Üniversitesi Tıp Fakültesi Klinik Araştırmalar Etik Kurulu İzin Yazısı (Devamı)

ULUDAĞ ÜNİVERSİTESİ TIP FAKÜLTESİ KLİNİK ARAŞTIRMALAR ETİK KURULU KARAR FORMU

ARAŞTIRMANIN AÇIK ADI	**Sağlıkta Büyük Veri: Etik Değerleri Gözeten Bir Model Önerisi**

ETİK KURUL BİLGİLERİ	ETİK KURULUN ADI	Uludağ Üniversitesi Tıp Fakültesi Klinik Araştırmalar Etik Kurulu 2011-KAEK-26
	AÇIK ADRESİ	
	TELEFON	
	FAKS	
	E-POSTA	

BAŞVURU BİLGİLERİ	SORUMLU ARAŞTIRMACI UNVANI/ADI/SOYADI	Prof.Dr.M.Murat Civaner			
	SORUMLU ARAŞTIRMACININ BULUNDUĞU MERKEZ	Bursa Uludağ Üniversitesi Tıp Fakültesi Tıp Tarihi ve Etik Anabilim Dalı			
	YARDIMCI ARAŞTIRMACININ UNVANI/ADI/SOYADI	MSc.Filiz Bulut			
	YARDIMCI ARAŞTIRMACININ BULUNDUĞU MERKEZ	Bursa Uludağ Üniversitesi Tıp Fakültesi Tıp Tarihi ve Etik Anabilim Dalı			
	DESTEKLEYİCİ	-			
	ARAŞTIRMANIN TÜRÜ	Boş veritabanı incelemesi			
	ARAŞTIRMANIN YAPILIŞ AMACI	Doktora tez çalışması			
	ARAŞTIRMANIN BAŞLAMA TARİHİ/ SÜRESİ	15.08.2021/ 1 yıl			
	GÖNÜLLÜ/DOSYA SAYISI	0			
	ARAŞTIRMAYA KATILAN MERKEZLER	TEK MERKEZ ☒	ÇOK MERKEZLİ ☐	ULUSAL ☒	ULUSLARARASI ☐

	Belge Adı	**Tarihi**	**Dili**
DEĞERLENDİRİLEN İLGİLİ BELGELER	GİRİŞİMSEL OLMAYAN ARAŞTIRMALAR İÇİN BAŞVURU FORMU	28.07.2021	Türkçe

	Belge Adı		**Açıklama**
DEĞERLENDİRİLEN DİĞER BELGELER	ARAŞTIRMA BÜTÇE FORMU	☒	Tarih: 28.07.2021
	ARAŞTIRICILAR İÇİN TAAHHÜTNAME FORMU	☒	Tarih: 28.07.2021
	PROSPEKTİF ÖZELLİKLİ GİRİŞİMSEL OLMAYAN KLİNİK ARAŞTIRMA TAAHHÜTNAMESİ	☐	
	İKU klavuzunun okunduğuna dair taahhütname	☒	Tarih: 28.07.2021
	SONUÇ ÖZET RAPORU	☐	
	DİĞER:	☒	Araştırma ilk başvuru ön yazısı (Tarih: 28.07.2021), ilgili kurum izin yazısı, sorumlu araştırmacı özgeçmişi, araştırıcılar tarafından imzalanmış Dünya Tıp Birliği Helsinki Bildirgesi, literatür

EK-4: Uludağ Üniversitesi Tıp Fakültesi Klinik Araştırmalar Etik Kurulu İzin Yazısı (Devamı)

ULUDAĞ ÜNİVERSİTESİ TIP FAKÜLTESİ KLİNİK ARAŞTIRMALAR ETİK KURULU KARAR FORMU

ARAŞTIRMANIN AÇIK ADI	**Sağlıkta Büyük Veri: Etik Değerleri Gözeten Bir Model Önerisi**

KARAR BİLGİLERİ	**Karar No: 2021-11/1** **Tarih: 11 Ağustos 2021** Yukarıda başvuru bilgileri verilen araştırma başvuru dosyası ve ilgili belgeler araştırmanın gerekçe, amaç, yaklaşım ve yöntemleri dikkate alınarak incelendi. 1-Araştırmanın başvurusu dosyasında belirtilen merkezde gerçekleştirilmesinin uygun olduğuna, 2-Araştırmanın başlama tarihinin bildirilmesi ve araştırma tamamlandığında özet bir sonuç raporunun hazırlanarak kurulumuza iletilmesine, 3-Araştırma protokolünde ve başvuru formunda yapılacak tüm değişiklikler için Etik Kuruldan izin alınması gerektiğinin sorumlu araştırıcılara iletilmesine toplantıya katılan etik kurul üye tam sayısının salt çoğunluğu ile karar verilmiştir.

ULUDAĞ ÜNİVERSİTESİ TIP FAKÜLTESİ KLİNİK ARAŞTIRMALAR ETİK KURULU

ÇALIŞMA ESASI	İlaç ve Biyolojik Ürünlerin Klinik Araştırmaları Hakkında Yönetmelik, İyi Klinik Uygulamalar Kılavuzu
BAŞKANIN UNVANI/ADI SOYADI	Prof.Dr.Mustafa HACIMUSTAFAOĞLU

ÜYELER

Unvanı/Adı/Soyadı	Uzmanlık Alanı	Kurumu	Cinsiyet		Araştırma ile ilişki		Katılım *		İmza
Prof.Dr.Mustafa HACIMUSTAFAOĞLU Başkan	Çocuk Sağlığı ve Hastalıkları	Bursa UÜ.Tıp Fakültesi Çocuk Sağlığı ve Hastalıkları AD	E ☒	K ☐	E ☐	H ☒	E ☒	H ☐	
Prof.Dr.Elif BAŞAĞAN MOĞOL Başkan Yardımcısı	Anesteziyoloji	Bursa UÜ.Tıp Fakültesi Anesteziyoloji ve Reanimasyon AD	E ☐	K ☒	E ☐	H ☒	E ☒	H ☐	
Prof.Dr.M.Sertaç YILMAZ Üye	Farmakoloji	Bursa UÜ.Tıp Fakultesi Tıbbi Farmakoloji AD	E ☒	K ☐	E ☐	H ☒	E ☒	H ☐	
Prof.Dr.Hilal ÖZKAN Üye	Çocuk Sağlığı ve Hastalıkları	Bursa UÜ.Tıp Fakültesi Çocuk Sağlığı ve Hastalıkları AD Yenidoğan BD	E ☐	K ☒	E ☐	H ☒	E ☒	H ☐	
Prof.Dr.Hasan ARI Üye	Kardiyoloji	Bursa Yüksek İhtisas EAH Kardiyoloji Kliniği	E ☒	K ☐	E ☐	H ☒	E ☐	H ☒	İzinli
Doç.Dr.Alpaslan TÜRKKAN Üye	Halk Sağlığı	Bursa UÜ. Tıp Fakültesi Halk Sağlığı AD	E ☒	K ☐	E ☐	H ☒	E ☐	H ☒	İzinli
Doç.Dr.Kağan HUYSAL Üye	Biyokimya	Bursa Yüksek İhtisas EAH Biyokimya	E ☒	K ☐	E ☐	H ☒	E ☒	H ☐	
Doç.Dr.Özen ÖZ GÜL Üye	İç Hastalıkları Endokr.ve Metab.	BUÜ.Tıp Fakültesi İç Hastalıkları AD Endokrinoloji ve Metabolizma BD	E ☐	K ☒	E ☐	H ☒	E ☒	H ☐	
Doktor Öğretim Üyesi Engin SAĞDİLEK Üye	Biyofizik	Bursa UÜ.Tıp Fakültesi Biyofizik AD	E ☒	K ☐	E ☐	H ☒	E ☐	H ☒	
Doktor Öğretim Üyesi Sezer ERER KAFA Üye	Tıp Tarihi ve Etik	Bursa UÜ.Tıp Fakültesi. Tıp Tarihi ve Etik AD.	E ☐	K ☒	E ☐	H ☒	E ☒	H ☐	
Av. Ahmet BAYRAM	Hukuk	Bursa UÜ.Rektörlüğü Hukuk Bürosu	E ☒	K ☐	E ☐	H ☒	E ☒	H ☐	
Tolga MUHTAR Üye	Sağlık mesleği mensubu olmayan üye	Serbest Meslek	E ☒	K ☐	E ☐	H ☒	E ☒	H ☐	

*:Toplantıda Bulunma

EK-5: Bursa Uludağ Üniversitesi Sağlık Uygulama ve Araştırma Merkezi Müdürlüğü-MİA MED İzin Yazısı

T.C.
BURSA ULUDAĞ ÜNİVERSİTESİ
Sağlık Uygulama ve Araştırma Merkezi Müdürlüğü

Sayı: E-73115338-000-17561 21.06.2021
Konu: Doktora Öğrencisi Filiz BULUT' un Veritabanlarını İnceleme Talebi

İlgi : a) 27.02.2020 tarihli ve B.30.2.ULU.0.H1.10.06-000/7290 sayılı yazımız.
b) 14.06.2021 tarihli ve B.30.2.ULU.0.H1.10.06-000-16917 sayılı yazımız.

Anabilim Dalınızın Doktora programı öğrencisi Filiz BULUT' un, ""Sağlıkta büyük veri: Etik değerleri gözeten bir model önerisi" isimli tez çalışması kapsamında MİA-MED Hastane Bilgi Yönetim Sisteminden veri tabanlarının incelenmesine ilişkin talebi uygun bulunmuştur.

Bilgilerinize rica ederim.

Prof. Dr. Bedrettin AKOVA
Başhekim a.
Başhekim Yardımcısı

Dağıtım :
Gereği :
Tıp Tarihi ve Etik AD. Başk.na

Bilgi :
SUAM Bilgi İşlem Merkezine

Bu Belge, 5070 sayılı Kanun hükümlerine uygun olarak elektronik imza ile imzalanmıştır.

Bilgi İçin: Özlem M.ÖKSÜZ
Memur

EK-6: Bursa Sağlık Müdürlüğü Halk Sağlığı Hizmetleri Başkanlığı - Hızır AHBS İzin Yazısı

BURSA İL SAĞLIK MÜDÜRLÜĞÜ - BURSA TOPLUM SAĞLIĞI BİRİMİ
06/09/2021 17:02 / 72873149 / 604.02 / 02-839
00147243393

T.C.
BURSA VALİLİĞİ
İl Sağlık Müdürlüğü

Sayı : E-72873149-604.02
Konu : Araştırma İzin Talebi (Filiz BULUT) Hk.

BURSA SAĞLIK MÜDÜRLÜĞÜ
HALK SAĞLIĞI HİZMETLERİ BAŞKANLIĞI
ARAŞTIRMA TALEPLERİNİ DEĞERLENDİRME KOMİSYONU
TOPLANTI TUTANAĞI

Başkanlığımız Araştırma Taleplerini Değerlendirme Komisyonuna sunulan dosyanın Halk Sağlığı Genel Müdürlüğünün ***"Birinci Basamak Sağlık Hizmetleri Alanında Yapılacak Olan Araştırma İzin / Onay Taleplerine İlişkin Değerlendirmeye Esas Teşkil Eden Kriterler"***e uygunluğunu değerlendirmek üzere 06.09.2021 tarihinde saat 14.00'da toplanmıştır.

Başvuru evrakları incelendiğinde, Ege Üniversitesi Sağlık Bilimleri Enstitüsü Tıp Tarihi Ve Etik Anabilim Dalı Öğretim Üyesi Prof.Dr.Murat CİVANER'in danışmalığında bulunan doktora öğrencisi Filiz BULUT'un Bursa Nilüfer 36 nolu Ertuğrul Eğitim Aile Sağlığı Merkezi'de yapmak istediği **"Sağlıkta Büyük Veri: Etik Değerleri Gözeten Bir Model Önerisi"** konulu tez çalışması kapsamında, Aile hekimliği bilgi sistemi içinde kullanılan yazılım programlarının hangi tür bilgileri topladığını incelemek istediği bildirilmiş olup çalışmanın başlatılabilmesi için söz konusu inceleme için Müdürlüğümüzün onayını istediği anlaşılmaktadır.

Komisyon tarafından yapılan değerlendirme sonucunda:

1. Yapılması planlanan çalışmanın Hasta Hakları Yönetmeliğine uygun bir şekilde yürütülmesi ve özellikle bu yönetmelikte bahsi geçen "Mahremiyete Saygı Gösterilmesi" ile "Bilgilerin Gizli Tutulması" hususlarına azami dikkat gösterilmesi kaydıyla yapılmasının komisyonumuzca kabul edilmesine,
2. Aile hekimleri ile aile sağlığı elemanlarının onayı çerçevesinde, ASM'nin işleyişi ve güvenilirliğine zarar verilmeksizin ve mesai saatleri içerisinde, sunulan hizmetlerin aksatılmasına sebep olmaksızın bizzat araştırma ekibi tarafından yürütülmesine,
3. Komisyonun çalışmanın yapılmasına ilişkin onayının, yapılan çalışmanın sonuç raporunun bir nüshasının Halk Sağlığı Genel Müdürlüğü'ne iletilmek üzere iki nüsha olarak Başkanlığımıza gönderilmesi hususunda çalışmacıya bilgi verilerek tebliğine;

Oy birliği ile karar verilmiştir

KOMİSYON BAŞKANI

Dr. İrfan OĞUZ
Halk Sağ. Hizm. Başk. Yardımcısı.

Bilgi için: Zeynep KUŞAT

EK-6: Bursa Sağlık Müdürlüğü Halk Sağlığı Hizmetleri Başkanlığı - Hızır AHBS İzin Yazısı (Devamı)

ÜYE
Dr. Betül Fatma AKAÇ
Uzman

ÜYE
Dr. Raif ÖZDEMİR
Uzman

ÜYE
Dr. Gaye CANTEKİN AKPINAR
Uzman

ÜYE
Dr. Tülay KÖSE
Uzman

ÜYE
İbrahim ALPTEKİN
Uzman

Ek: Araştırma İzin Talebi (Filiz BULUT) Evrakları.

Bilgi için: Zeynep KUŞAT

9. TEŞEKKÜR

Yüksek lisans tezimin teşekkür bölümüne, tez yazmanın zorluklarından bahsederek başlamıştım. Yine aynı düşünce ile ve bu defa daha farklı zorlukları deneyimleyerek bu tezi yazmış bulunmaktayım. Pandemi koşulları başta olmak üzere, yaşanılan diğer birçok kişisel sorunlarıma rağmen, her şeyi bir kenara bırakıp bu tezi zamanında ve hakkını verdiğimi düşünerek bitirmiş olmanın gururunu yaşıyorum. Bu tez ile, yazar Murat Menteş'in deyimiyle kaosa mütevazi bir katkıda bulunmaya çalıştım (Büyük veri dünyasının yaratmış olduğu kaosa). Umarım başarabilmişimdir.

Bana bu gururu yaşatan kişilere teşekkür etmeye gelince, tabi ki ilk olarak 2012 yılında kaybettiğim güzel insan dedem Mehmet Bulut'a teşekkür edeceğim. Her şeyden önce beni bu kadar güçlü bir insan olarak yetiştirdiği için. Ve ikinci teşekkürüm benim bu dünyadaki eşsiz destekçim olan, duaları ile huzur bulduğum babaannem Müzeyyen Bulut'a sonsuz teşekkür ediyorum. Beni motive etmeyi çok iyi bilen kız kardeşim Emine Deniz Bulut'a da en içten teşekkürlerimi sunuyorum. Ailemden bir farkı olmadığını düşündüğüm, bu dünyada bana çok iyi bir abla olan ve var olduğu için kendimi çok şanslı hissettiğim Nefise Sever'e çok ama çok teşekkür ediyorum.

Tez için yaptığım araştırmada görüşleri ile bana katkıda bulunan Aile Hekimliği Anabilim Dalı asistanlarından Dr. Zeynep Avcu, Dr. Erdinç Sevinç, Dr. Canan Tuz Yılmaz ve Dr. Sergen Aygüneş'e çok teşekkür ediyorum.

Tezimin biçimsel düzeltmesi için bana yardımcı olan ve tüm ricalarımı gerçekleştiren sevgili Barış Yüksel'e çok teşekkür ediyorum.

Tez izleme komitemde yer alan Doç. Dr. Elif Atıcı'ya teşekkür ediyorum.

Bu zorlu süreçte benim ikinci danışmanım gibi olan, sözleri, güler yüzü ve enerjisiyle bana destek veren, tez izleme kurulumda da bulunarak görüşleri ile katkıda bulunan Prof. Dr. Yeşim Uncu'ya çok teşekkür ediyorum.

Türkiye Biyoetik Dergisi sekreterliği görevim sırasında birlikte çalışma fırsatı bulduğum ve iyi ki tanıdım dediğim hocam Prof. Dr. Gürkan Sert'e çok teşekkür ediyorum.

Bana bir öğretmenden çok beni bir kardeşi gibi gören, bana sözleri ile cesaret veren, yanımda olduğunu, içtenliğini derinden hissettiğim abim güzel insan Murat Aksu'ya çok teşekkür ediyorum.

Son olarak danışman hocam Prof. Dr. M. Murat Civaner'e teşekkür etmeliyim. Bazı emekler sözlerle ifade edilemez. Çok kutsal bir meslek olduğuna inandığım öğretmenlik mesleği de böyledir. Bu mesleği üstlenen ve mesleğin gereğini fazlasıyla yerine getiren danışmanıma, üzerimdeki tüm emekleri için sonsuz teşekkürü bir borç bilirim.

Tez yazmanın zorluğunu bir kez daha anlamış bulunmaktayım. Bu süreçte insanın desteğe, cesarete, ilhama, güce, yapıcı eleştiriye ve motive edici sözlere gerçekten çok ihtiyacı oluyor. Bu nedenle yukarıda ismi geçen her bir kişinin bu tezin ortaya çıkmasında büyük payı olduğunu düşünüyorum. Tekrar sonsuz teşekkürlerimle…

10. ÖZGEÇMİŞ

2011-2015 yılları arasında Uludağ Üniversitesi Fen Edebiyat Fakültesi'nde Felsefe lisansımı aldım. Lisansım devam ederken Türk Dili ve Edebiyatı Bölümü'nde yan dal öğrenimi gördüm.

2015-2016 eğitim-öğretim yılında Uludağ Üniversitesi Tıp Fakültesi Tıp Tarihi ve Etik Anabilim Dalı'nda başladığım Yüksek Lisans programını "Hizmet Sunma Yükümlüğünün Sınırlarının Tıp Etiği Açısından Analizi" başlıklı tez ile başarı ile tamamladım. 2017-2018 eğitim-öğretim yılında aynı bölümde doktora programına başladım.

Uludağ Üniversitesi'nin veteriner hekim olan Güler-Osman Köseoğlu'nu anma adına düzenlediği "İçinden Fıkra Geçen Öykü Yarışması" nda, 2017 yılı birincilik ödülünü kazandım. 22-24 Mart 2018 Su ve Çevre Fuarı kapsamında düzenlenen Uluslararası Su ve Çevre Kongresi'nde Şiir dalında ikincilik ödülü kazandım.

Mart 2020 tarihinden itibaren Türkiye Biyoetik Dergisi'nin (TJOB) Genel Sekreterliğini yapmaktayım. Türkiye Biyoetik Derneği ve Bursa Tabip Odası Parantez Sahnesi tiyatro topluğuna üyeyim.