T.C.
İSTANBUL YENİ YÜZYIL ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ
SAĞLIK YÖNETİMİ ANABİLİM DALI

SAĞLIK SİGORTACILIĞI ALANINDA KİŞİSEL VERİLERİN KORUNMASI KANUNU HAKKINDA HASTALARIN YAKLAŞIMININ DEĞERLENDİRİLMESİ

YÜKSEK LİSANS TEZİ

AYŞE GİZEM UNUR

DANIŞMAN
Doç. Dr. Itır ERKAN

İSTANBUL, 2021

T.C.
İSTANBUL YENİ YÜZYIL ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ
SAĞLIK YÖNETİMİ ANABİLİM DALI

SAĞLIK SİGORTACILIĞI ALANINDA KİŞİSEL VERİLERİN KORUNMASI KANUNU HAKKINDA HASTALARIN YAKLAŞIMININ DEĞERLENDİRİLMESİ

YÜKSEK LİSANS TEZİ

AYŞE GİZEM UNUR

DANIŞMAN
Doç. Dr. Itır ERKAN

İSTANBUL, 2021

ETİK BEYAN

İstanbul Yeni Yüzyıl Üniversitesi Sağlık Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu projede;

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

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

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

- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,

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

06/08/2021

Ayşe Gizem UNUR

ÖNSÖZ

Kişisel verilerin korunmasının öneminin hem Türkiye'de hem de Dünya'da genelinde işleyişi, hukuksal uygulamaları ve pratik anlamda sahada olan uygulamaların etkililik düzeyinin sağlık sektörüne yansımalarını göstermek için detaylı araştırmalar sonucu ve konuyla ilgili uzman kişilere danışılarak tarafımca hazırlanmıştır.

Hazırladığım tez sürecinin yanı sıra, öğrenim hayatımın başlangıcından sonuna kadar geçen sürede bana olan desteğini esirgemeyen ve her kararımda arkamda duran annem Emsal UNUR ve babam Yalçın UNUR'a, kendimi tanımamı ve yolumu seçmemde bana ışık olan ve desteğini her zaman hissettiğim Zeynep Terzi UZUN'a, lisans hayatımın ilk gününden yüksek lisans tez aşamasına kadar öğrenim hayatıma olan değerli katkısı, akademik alanda her zaman yol gösteren danışmanım Sayın Doç. Dr. Itır ERKAN'a, tezimi hazırlamamda bana hukuki anlamda yol gösteren Av. Ahmet Esad BERKTAŞ'a sonsuz teşekkürler.

İSTANBUL, 2021 Ayşe Gizem UNUR

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
AİHM	: Avrupa İnsan Hakları Mahkemesi
AİHS	: Avrupa İnsan Hakları Sözleşmesi
AK	: Avrupa Komisyonu
BİT	: Bilgi ve İletişim Teknolojisi
BM	: Birleşmiş Milletler
EC	: European Commission
E-PRIVACY	: Privacy and Electronic Communications Directive
ESK	: Elektronik Sağlık Kayıtları
ETK	: Elektronik Tıbbi Kayıt
GDPR	: General Data Protection Regulation
GEBLİZ	: Gebe, Bebek, Lohusa İzleme Sistemi
GVKT	: Genel Verileri Koruma Tüzüğü
HES	: Hayat Eve Sığar
HIEs	: Hiper IgE Sendromu
HSYS	: Halk Sağlığı Yönetim Sistemi
IBAN	: International Bank Account Number
IP	: Internet Protokol
KHK	: Kanun Hükmünde Kararname
KVKK	: Kişisel Verileri Koruma Kanunu
MASAK	: Mali Suçları Araştırma Kurulu
OECD	: Organisation For Economic Co-Operation And Development
ÖSS	: Özel Sağlık Sigortası
PVSK	: Polis Vazife ve Salahiyet Kanunu
SBGM	: Sigorta Bilgi ve Gözetim Merkezi
SGK	: Sosyal Sigortalar Kurumu
SSK	: Sosyal Sigortalar Kurumu

TBK	: Türk Borçlar Kanunu
TBMM	: Türkiye Büyük Millet Meclisi
TC	: Türkiye Cumhuriyeti
TCK	: Türk Ceza Kanunu
TSB	: Türkiye Sigortalar Birliği
URL	: Uniform Resource Locator
USVS	: Ulusal Sağlık Veri Sözlüğü
VERBİS	: Veri Sorumluları Sicil Bilgi Sistemi
WHO	: World Health Organisation

ÖZET

SAĞLIK SİGORTACILIĞI ALANINDA KİŞİSEL VERİLERİN KORUNMASI KANUNU HAKKINDA HASTALARIN YAKLAŞIMININ DEĞERLENDİRİLMESİ

Dünya genelinde veri hacmi ve veri çeşitliliği, insanlık tarihi boyunca hiç görülmediği hızda artmaktadır. Teknolojinin ve sosyal medyanın hayatın her evresine girmesiyle birlikte insanlar günlük faaliyetlerinde bile veri üretir duruma gelmiştir. Kişisel veri kavramı her sektörde yer aldığı gibi sağlık ve sigortacılık alanında ve özellikle özel sağlık sigortacılığında oldukça sık kullanılmaktadır. Öyle ki sağlık alanında ele alınan kişisel veriler aynı zamanda hassas veri olarak nitelendirilmiş ve konunun önemine hukuki olarak da vurgu yapılmıştır. Ele aldığımız çalışmada kişisel sağlık verilerinin işlenmesi sürecinde ulusal ve uluslararası alanda uygulanmakta olan hukuki kurallar ve güncel uygulamalara detaylı olarak yer verilmiştir. Çalışmanın büyük bir kısmı 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve yönetmelikler kapsamında incelenmiştir. Süreç gereği kişisel hem sağlık sektörü hem de sağlık sigortacılığındaki veri işleme süreci ele alınmıştır.

Bu çalışmanın amacı hastaların kişisel verilerin korunması hakkındaki farkındalıklarının ne düzeyde olduğunu değerlendirilmiştir. anketimizin son sorusunda ilgili literatürden derlenen 23 madde 5'li likert şeklinde sorulmuştur. Bu maddelerin içsel geçerliliği Cronbach's Alfa testiyle sınanmıştır. Alanda daha önce bu konuda yapılmış bir akademik çalışma bulunmaması sebebiyle bir ilk olma özelliği taşımaktadır.

Çalışma İstanbul ilinde özel bir hastanede hizmet alan 169 hastanın katılımıyla gerçekleştirilmiştir. Elde edilen veriler SPSS 20.0 programı kullanılarak ANOVA, t testi ve ki-kare testleriyle frekans ve yüzde analizleri yapılmıştır. Katılımcıların %62,7'si kadın, %37,3'ü erkektir. Yaş grupları; %28,4'ü 18- 24, %47,9'u 25-34, %13,6'sı 35-44, %7,7'si 45-54, %1,8'i 55-64, %0,6'si 65 yaş ve üzeri şeklindedir. Eğitim düzeyleri; %27,2'si lise, %55'i lisans, %10,7'si yüksek lisans ve %1,2'si doktora olarak ifade edilmiştir. Katılımcıların bazı anket sorularına verdiği yanıtlar cinsiyet, yaş veya eğitim düzeyi ayrımıyla gözlemlenmiştir.

Cinsiyete göre anlamlı farklılıklar gözlemlenen sorular olmuştur. Örneğin; kadın katılımcıların bir sağlık uzmanıyla yapacağı veri paylaşımı için erkek katılımcılara göre daha az endişeli olduğu gözlemlenmiştir(3.42>2.97). Kadınların erkeklere göre poliçe satın aldıktan sonra sigorta tarafından beyan etmedikleri hastalıklarının araştırılması konusunda daha hassas oldukları ve erkeklere göre güvenlerinin daha çok azaldığı gözlemlenmiştir.

Çalışmamızda kişisel sağlık verilerinin Sağlık Sigortacılığı alanında hem uygulama hem de teoride yer alan hukuki süreçler işlenmiştir. Hastaların farkındalığının değerlendirilmesi amacıyla yapılan anket çalışmasının verileri paylaşılmıştır. Hastaların hukuki olarak sahip oldukları hakların teoride olduğu gibi pratikte de da hassasiyetle uygulanmasını sağlamak için devlet ve özel sektör arasında ortak çalışmalar yapılarak süreç zinciri güçlendirilmelidir. Ayrıca yine kamu ve özel sektör çalışanlarının, veri işleme süreciyle ve güncellenen mevzuatlar konusunda kurum içi eğitimler verilerek sürecin önemi belirtilmelidir.

Anahtar Kelimeler: Kişisel Veri, Kişisel Verilerin Korunması, Kişisel Sağlık Verilerinin Korunması, KVKK, Özel Sağlık Sigortacılığı, Sağlık Sektörü

Ayşe Gizem UNUR, 2021

ABSTRACT

EVALUATING PATIENTS' APPROACH ABOUT THE LAW ON THE PROTECTION OF PERSONAL DATA IN THE FIELD OF HEALTH INSURANCE

The volume and variety of data produced day by day continue to increase around the world as it has never happened throughout the human history in such a very quick way. The people have been in a situation in which they produce data even in their daily activities as technology and social media have spread into all phases of our lives. The notion of personal data is frequently used in the fields of health and insurance business as well as in other sectors of the industrialized business world. Thus, personal data used in the field of health has been described as sensitive data and the significance of the notion has been juristically emphasized. In this study, the laws and current applications adopted and used nationally and internationally during the course of process of personal health data have been examined in detail. The large portion of the study has been carried out in accordance with The Law On The Protection Of Personal Data No. 6698 and other regulations. As required in this process, the course of data process of personal health data has been analyzed from the perspective of both the sector of health and health insurance business.

This study aims to measure the awareness level of the patients about the protection of personal data. In the last question of the survey, 23 subjects compiled from the related literature were asked with 5 point likert scale. Internal validity of these subjects was tested with Cronbach's Alpha test. This paper has the feature of being first academic study in this field as there is no any academic study carried out before on this subject.

The study was carried out with the participation of 169 patients who received health service in a private hospital in Istanbul. Anova, T Test, and chi-square tests, frequency and percentile analyses were applied on the obtained data using SPSS 20.0 program. 62.7% of the participants are female and 37.3% are male. Age groups have been categorized as following; 18-24: 28.4%, 25-34: 47.9%, 35-44: 13.6%, 45-54: 7.7%, 55-64: 1.8% and +65: 0.6%.

On the other hand, education levels have been categorized as following. 27.2% of the participants are high school graduate, 55% are have bachelor’s degree, 10.7% have master's degree and 1.2% are have doctorate degree. The responses of the participants given to some of the survey questions were observed in terms of gender, age or education level.

There are some questions via which significant differences have been observed according to gender. For example, it has been observed that female participants are less worried about sharing data with a healthcare professional than male participants (3.42>2.97). It has also been seen that women are more sensitive than men in the investigation of the diseases that they do not declare by the insurance company after purchasing a policy and it is seen that confidence level of women decreases more than men.

In our study, the legal processes in both practice and theory in the field of health insurance of have been examined in terms of personal health data. The data of the survey study conducted to measure the awareness of the patients has been shared.
State and private sector collaborate in this field and process chain should be strengthened in order to make sure that patients’ legal rights are preserved and applied sensitively in both theory and practice. In addition, the importance of the process should be emphasized by providing in-company trainings to with public and private sector employees on the data processing process and the updated legislation.

Keywords: Personal Data, Protection Of Personal Data, Protection Of Personal Health Data, GDPR, Health Legislation

1. GİRİŞ

Kişisel veri, bireyi tanınabilir kılan her türlü bilgiyi kapsayan veriler bütünü için yapılmış tanımlamadır (Resmî Gazete, 2016). Kişisel veri kavramının kapsamı oldukça geniştir ancak kısaca bir bireye erişebilen hemen hemen her türden veriyi içerdiğini belirtebiliriz. Bu sadece isim soyisim, adres veya kimlik numarası gibi bireyin kimliğine atıfta bulunan temel gerçeklere dayanan bilgiyi içermemekte, aynı zamanda alışveriş kayıtları veya online ziyaret ettiği siteler gibi kişinin özel hayatına ait bilgileri de içermektedir (Tekin, 2014).

Veri koruması konusu temelde; kişilerin sahip oldukları verilerin işlenmesiyle oluşacak zararlardan koruma amacıyla somutlaşmış önlemleri ifade etmektedir. Bu durum veri sahiplerinin ilişkili olduğu kişilerin de korunmasını hedef almaktadır. Verilerin korunması adına; depolanması, işlenmesi, silinmesi, saklanması gibi veri işleme sürecinin bütün aşamalarını kapsayacak şekilde bireylere kontrol hakkını kazandırmayı amaçlamaktadır (KVKK Yayınları, 2018).

Son yıllarda dijital platformların ve bilgi teknolojilerinin gelişimi, kişisel verilerin güvenliği konusunda endişeleri artırmıştır. Kişisel verilerin transferi ve depolanmasının geçtiğimiz dönemlere göre daha kolay yapılmaktadır. Bu konuda Dünya'da en çok önem verilen Avrupa'da, çözüm "Veri Koruma Kanununda" bulunmuştur. Bu terim, kişisel verilerin bilgi dâhilinde olmasını ve gizlenmesini düzenlemeyi amaçlayan yasal bir yapıyı ifade etmektedir.

Veri kayıt aşamasında veri güvenliğine yönelik risklerin ortaya çıkmaması adına gerekli kaynak ve zaman ayırılarak teknik ve idari tedbirlerin alınması gerekmektedir. Ülkemizde son yıllarda önem kazanan kişisel verilerin korunması konusunda yasal olarak son yıllarda düzenleme yapılmak istendiği söylenebilir ancak birçok sektörde hala yer edinemediği görülmektedir. Kişisel verilere karşı gelişen tehditler, bilgisayar programlarının gelişmesi ve veri depolama alanlarının oluşturulması ile 1970'li yıllarda Avrupa'da ortaya çıkmış ve zamanla Dünyaya yayılmıştır. Teknolojik olarak savunma mekanizmasının geliştirilmesini ve veri hukuku kavramının gerekliliklerini ortaya çıkarmıştır (Korkmaz, 2016).

Sağlık sigortacılığı hem özel kurumların hem de devletin, kişilere ait sağlık hizmeti almasını sağlayan ve finansal kaynağa ihtiyaç duyan bir kavramdır. Kişilerin prim ödeme yöntemiyle hak sahipliği kazandığı sistemde ihtiyaç duyduğunda kullanabilmesi adına hak sahibi kendine ait bir takım sağlık verilerini paylaşması gerekmektedir. Bu süreçte özel ve tüzel kişilerin hakları üzerinde bilgi sahibi olmaları ve verilerin korunmasının önemini bilerek süreç yönetmeleri olası kötü kullanımların önünü kapatacaktır.

2. GENEL BİLGİLER

2.1. Kişisel Verileri Korumaya İlişkin Kavramsal Çerçeve

Kişisel verilerin korunması mahremiyetin korunmasını da beraberinde getirmektedir. Veri kişiye ait her türlü bilgiyi ifade ederken her ne kadar sosyal boyutta etik ilkesini akla getirse de hukuktan ve yasalardan ayrı değerlendirilemez. Bu konudaki yasaların ülkemize yeni yapılanıyor olması ve birçok sektörde yer edinememiş olmasına rağmen aşağıda açıklanan kavramlar konunun genel sınırını ve özünü ifade etmektedir.

2.1.1. Kişi ve Kişisellik Kavramı

"Kişi" kavramı Türk Dil Kurumu Sözlüğünde "şahıs, zat, nefer", "kişisel" kavramı ise "kişi ile ilgili, kişiye ilişkin, şahsi" anlamlarına gelmektedir (URL-1). Hukuki anlamda ise belirli borçlara ve haklara sahip olabilen, tüzel ve gerçek kişi olarak tanımlanır.

2.1.2. Veri Tarihçesi, Kavramı ve İçeriği

"Veri" kavramı Türk Dil Kurumu sözlüğüne göre "Bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öge, muta, done." anlamına gelmektedir. "Bilgi" ise "Kurallardan yararlanarak kişinin veriye yönelttiği anlam "dır. Birbirinden farklı anlam taşımasına rağmen çoğu zaman birbirinin yerine kullanılmaktadır (URL-1). Bu konuda dikkate alınması gereken, verinin bilginin hammaddesi olmasıdır. Veri işlenerek bilgi haline gelmektedir.

Kimliği belirli veya belirleyebilir gerçek kişiye ilişkin her türlü bilgiye "kişisel veri" denir (T.C. Resmî Gazete, 2016). Kimlik belirleme potansiyeli oluşturabilecek bilgilere; isim, ikamet, kişiyi ilgilendiren her türlü tarih bilgisi, TC kimlik numarası, IBAN, ehliyet numarası, parmak izi kayıtları, fotoğrafları örnek verilebilir (HIPAA, 2018). Ayrıca kişinin; inan değerleri, düşünceleri ve alışveriş alışkanlıklarına ilişkin bilgiler dahil kişisel veri kapsamında yer almaktadır (Aksoy, 2010).

2.1.3. Özel Nitelikli/Hassas Veri Kavramı

Avrupa Birliği'nin GDPR uygulamalarında, bireye ait kişisel veriler "hassas veri", "özel nitelikli veri" şeklinde detaylandırılmıştır. Bu ayrımla kavramlar daha etkin ve özel nitelikte korunmaya alınmıştır (Akgül, 2013). Kişisel veriler çerçevesinde hassas veriler başlığı altında ayrıma gidilmesi, bu veri türlerinin daha katı korunmaya alınması ihtiyacından kaynaklandığı görülmektedir. Bu ihtiyacı doğuran temel sebep ise ele geçebilecek hassas verilerin işlenmesi sonrası telafi edilemeyecek durumların ortaya çıkma riskidir. Bu risk kişilerin karşılaşabileceği ve hayatını etkileyebilecek birçok etkeni barındırmaktadır.

6698 Sayılı KVKK'da özel nitelikli veri olarak tanımlanan bu veriler; "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 biometrik ve genetik verileri özel nitelikli kişisel veri olarak belirtilmektedir" (KVKK Yayınları, 2018). 95/46 sayılı Avrupa Birliği Resmî Gazetesinde yayınlanan Direktifte ise hassas veriler kişinin ırk veya etnik kökeni, siyasi görüşü, dini veya felsefi inançlar ve sendika üyeliği, genetik ve biometrik veriler ve cinsel yaşam veya cinsel yönelimi olarak tanımlanmaktadır (Handbook GDPR, 2018).

2.1.4. Kişisel Verilerin Korunması

Özel kurumlar ve kamu kurumları iş işleyişleri sebebiyle uzun yıllardır uygulanan kanunlarla, kişilerin rızasıyla, yapılan iş sözleşmeleriyle veya yapılan işlerin niteliğine bağlılık gibi çeşitli sebeplerle kişisel verileri toplamaktadır. Her ne kadar kişisel verilerin toplanması ve kötü niyetli olarak kullanılması tehlikeli olsa da sosyal ve ekonomik hayatın sürdürülebilmesi özel ve kamu kurumlarının hizmet sunumu, pazarlama faaliyetlerini sürdürebilmesi, satılan malın veya verilen hizmetin ihtiyaçlar doğrultusunda geliştirilmesi çalışmalarının yapılabilmesi sağlık alanında doğru tanıların konulup uygun tedavi yollarının araştırılabilmesi için kişisel verilerin toplanması kaçınılmazdır. Bu bilgilerin hassas veri kategorisine girmesi sebebiyle ilgili ve yetkili kişi veya kuruluşlarca muhafazası ve amaca uygun kullanımı da mutlak bir sosyal ihtiyaç olmasının yanında Anayasal bir haktır.

Bu alanda çıkarılan Kanunla, kişisel verilen toplanmasının sınırı çizilmiş ve yetkisi olmayan kişilerin eline geçmesinin, ifşa edilmesinin, kötü niyetli kullanılmasının ve kişisel hakların ihlal edilmesinin önüne geçilmesi amaçlanmıştır.
Ulusal düzenlemeye bakılacak olursa ülkemiz; Avrupa Konseyi, OECD, Birleşmiş Milletler gibi örgütlerin de üyesi olmasına rağmen, uluslararası kuruluşlarca benimsenen ilkeleri uzun yıllar boyunca ulusal hukukumuza aktaramamıştır. Uzun yıllar Anayasa maddelerine dolaylı yollardan dahil edilmeye çalışılmasına rağmen bu konuya özgü olarak 24 Mart 2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu çıkarılmıştır.

2010 yılında yapılan referandum sonrası çıkarılan 5982 sayılı Kanunla, Anayasanın özel hayatın gizliliğini düzenleyen 20. Maddesine göre; "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" (T.C. Anayasası, 1982) hükmü eklenerek, kişilerin kişisel verilerinin korunması açıkça Anayasal güvence altına alınmıştır. Ayrıca yurtdışında yerleşik olmakla birlikte Türkiye'de faaliyet gösteren veri sorumluları hakkında da Kanun hükümleri uygulanacaktır (T.C. Resmî Gazete, 2016). Kişisel Verileri Koruma Kanunu'na uyum yasal bir gerekliliktir. Veri koruma yasasına uyum ihlalleri sonrası kişilere veya kurumlara soruşturma, para cezası, olumsuz tanıtım, hukuki veya cezai yaptırım ile sonuçlanabilir (Data Protection & Research, 2018).

Uluslararası düzenlemelerde ise yapılan çalışmaların ülkemize nazaran daha önceki yıllarda çalışmalara başlanmış ve uygulamaya koyulduğu görülmektedir. "108 sayılı Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" Avrupa Konseyi bünyesinde hazırlanarak 28 Ocak 1981 tarihinde Strazburg'ta imzaya açılıp ve 1 Ekim 1985 tarihinde yürürlüğe girmiştir (Korkmaz, 2016).

Avrupa Birliği tarafından çıkarılan resmî gazetede; Avrupa Parlamentosu ve Konsey'in 95/46 / EC sayılı Direktifi, veri işleme faaliyetleri bakımından gerçek kişilerin temel hak ve özgürlüklerinin korunmasını uyumlaştırmayı ve kişisel verilerin Üye Devletler arasında serbest akışını sağlamayı amaçladığı belirtilmiştir (URL- 2).

Temel sebebi inceleyecek olursak, hukuk sistemleri, korunmaya değer gördükleri maddi ve manevi her şeyi yazılı düzenlemeler yaparak koruma altına almayı amaçlamaktadır. Teknolojik gelişmelerin yaşanmasıyla birlikte internet başta olmak üzere birçok mecrada verilerin toplanması, kayıt altına alınması, kişilerin mahremiyet gerektiren bilgilerinin paylaşılması veya işlenmesinin daha kolay bir hal aldığını görmekteyiz. Yapılan bu yanlış ve zarar verici uygulamaların başlanmasıyla dünya genelinde kişiler, sivil toplum kuruluşları, resmi ve özel kurumlar harekete geçmiş ve bireyi korumayı esas alan yasal düzenlemeler yapılmıştır. Özellikle kişisel sağlık verileri özel nitelikli veri olması sebebiyle mevzuatta ayrıca korunmaktadır. Bunun sebebi ise verilerin başkalarının eline geçmesi durumunda telafi edilemeyecek risklerin ortaya çıkmasına sebep olabilmekte ihtimali bulunmaktadır. Bu sebepten dolayı kurumlar için kişisel sağlık verilerinin korunması oldukça önemlidir.

2.1.5. Kişisel Verilerin İşlenmesi

İşleme, kişisel verilerin toplanmasından silinmesine kadar olan uzun ve birçok işlemi kapsayan bir süreçtir. Avrupa Birliği Direktifi bu terimi "Silme veya tahrip etme, engelleme, birleştirme veya sıralama, sağlama ya da dağıtma, iletmeyle açıklama, toplama, kaydetme, organizasyon, depolama, adaptasyon veya değiştirme, kurtarma, danışma gibi otomatik ya da otomatik olmayan araçlarla kişisel veriler üzerinde yapılan herhangi bir faaliyet veya faaliyet dizisi" olarak tanımlamaktadır (Avrupa Parlamentosu Yönetmeliği, 2016). Veri işleme konusunda mevzuatta yer alan ve bilinmesi gereken ifadeler aşağıdaki gibidir;

İlgili kişi: Kişisel verisi işlenen gerçek kişiyi,
Veri kayıt sistemi: Kişisel verilerin belirli kriterlere göre yapılandırılarak işlendiği kayıt sistemini,
Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak onun adına kişisel verileri işleyen gerçek veya tüzel kişiyi,

Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade etmektedir (Resmî Gazete, 2016).

Direktifin 2 (e) maddesi uyarınca; "veri işleyici veri sorumlusu adına kişisel verileri işleyen gerçek veya tüzel kişidir ancak veri işleyicisi, çalışması sırasında bu tür verileri işleyen bir veri sorumlusunun çalışanını kapsamamaktadır. Uygulamada, veri sorumluları, zaman ve maliyet tasarrufu sağlamak için verilerini işlemek üzere sıklıkla üçüncü taraf yani harici kişi ya da şirketleri kullanmaktadırlar. Üçüncü taraf, yalnızca veri kontrolörünün emri üzerine hareket ettiği ve işlenecek verinin amacını kendisi belirlemediği için, bu kişi veri işleyici olarak tanımlanmaktadır" (Tekin, 2014). Bu bağlamda veri işleyicilerine örnek olarak; başkası adına kişisel işleyebilen veya saklayabilen; "sigorta şirketleri, muhasebeciler veya pazar araştırma şirketleri" gösterilebilir. Ayrıca bir şirket veya birey hem veri kontrolörü hem de veri işleyicisi olması mümkündür. Örneğin, bir sigorta şirketi kendi çalışanı hakkındaki veriler açısından "veri kontrolörü" olacaktır; ancak müvekkil şirketler için işlediği çalışan bordrosuna ilişkin olarak "veri işleyicisi" olarak tanımlanır (Tekin, 2014). Ayrıca bir hastane eğer kendi yazılım sistemini üretim sahada da bu yazılım sistemini kullanarak veri işliyor ise bu gruba örnek vermek mümkündür.

2.1.5.1. Envanter

Günümüzde birçok yerli, yabancı, devlet veya özel kurum şirket faaliyetleri kapsamında çok sayıda kişisel veri elde etmekte, işlemekte ve daha iyi hizmet sunmak veya ticaret hacmini artırarak ekonominin gelişmesini sağlamak amacıyla daha fazla kişisel veriye ulaşmayı ve üçüncü kişilerle paylaşmayı hedeflemektedir. Ancak daha fazla veriye ulaşmaya ve işlemeye yönelmek; işlenen kişisel verilerin sağladığı kolaylık ve avantajlar sebebiyle ülke ekonomisine katkı yapılmasıyla birlikte veri güvenliğine dair çeşitli risk ve ihlal ihtimallerini de gündeme getirmektedir.

Bu riskler nedeniyle kişisel verilerin korunması ve buna yönelik hukuki bir altyapının oluşturulmasına ihtiyaç duyulmuş olup öncelikle Türkiye Cumhuriyeti Anayasasında

2010 yılında yapılan değişiklikle, kişisel verilerin korunması hakkı Anayasal güvenceye kavuşturularak buna yönelik Kanunla düzenleme yapılması gerektiği hükme bağlanmıştır (T.C. Anayasası Madde 20).

Çıkarılan bu kanunla temel hak, özgürlük ve mahremiyetin korunması, gerçek ve tüzel kişilerin uyacakları usul ve esasların belirlenmesi ve gelişi güzel ve Kanuna aykırı olarak veri işlemesinin, yetkisiz kişilerin eline geçmesinin ve hukuka aykırı olarak paylaşım yapılarak kişilik haklarının ihlal edilmesinin engellenmesi amaçlanmıştır.

Kanunun koruma altına aldığı haklara ek getirilmiş olup bunlardan birisi; Kişisel Veri İşleme Envanteri hazırlanmasıdır. Envanter, "30.12.2017 tarihli Resmî Gazete 'de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmeliğin 4. Maddesi 1. fıkrası (h) bendinde" tanımlanmıştır (28.04.2019 tarihli Resmî Gazete 'de yayımlanan Veri Sorumluları Sicili Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmeliğin 1. maddesi ile bentte değişiklik yapılmıştır). Veri Sorumluları Sicili Hakkında Yönetmelik Madde 4 – (1) Bu Yönetmelikte geçen;

h) "Kişisel veri işleme envanteri: Veri sorumlularının iş süreçlerine bağlı olarak gerçekleştirmekte oldukları kişisel veri işleme faaliyetlerini; kişisel veri işleme amaçları ve hukuki sebebi, veri kategorisi, aktarılan alıcı grubu ve veri konusu kişi grubuyla ilişkilendirerek oluşturdukları ve kişisel verilerin işlendikleri amaçlar için gerekli olan azami muhafaza edilme süresini, yabancı ülkelere aktarımı öngörülen kişisel verileri ve veri güvenliğine ilişkin alınan tedbirleri açıklayarak detaylandırdıkları envanteri," ifade eder (T.C. Anayasası, 1982).

Bu duruma göre Envanter, yapılan faaliyetler ve iş işleyişi kapsamında işlenmekte olan kişisel verilerin değerlendirilmesi, yapılan tüm faaliyetlerin detaylı incelenebilmesi ve işleme amacının vaka bazlı belirlenebilmesi, veri sorumlusunca belirlenen saklama süresi ve yurt içi ve yurt dışına aktarım yapılıp yapılmağı görüntülenebilecek bir rapordur. Ayrıca bu rapor hazırlanırken veri sorumlusu kanuna uyumunu kendisi de takip edebilir.

2.1.5.2. Verbis

Yıllık olarak personel sayısı 50'den fazla veya mali bilançosunun toplamı 25 milyon TL'den fazla olan gerçek ve tüzel kişi veri sorumluları ile yurtdışında yerleşik gerçek ve tüzel kişi veri sorumlularını kapsayan Kişisel verileri Koruma Kanunu'nun 16. maddesinde; "Veri Sorumluları Sicilinin kamuya açık olarak tutulması gerektiği ve kişisel verileri işleyen gerçek ve tüzel kişilerin veri işlemeye başlamadan önce Veri Sorumluları Siciline kaydolmak zorunda olduğu belirtilmektedir" (Resmî Gazete, 2016). Buna göre, Sicile kayıt sırasında veri sorumlusunun "kimlik ve adres bilgileri, kişisel verilerin hangi amaçla işleneceği, veri konusu kişi grubu ve grupları ile bu kişilere ait veri kategorileri hakkındaki açıklamalar, kişisel verilerin aktarılabileceği alıcı veya alıcı grupları, yabancı ülkelere aktarımı öngörülen kişisel veriler, kişisel veri güvenliğine ilişkin alınan tedbirler ve kişisel verilerin işlendikleri amaç için gerekli olan azami süre" gibi bilgilere ilişkin giriş yapılması gerekmektedir. Bu kapsamda Kişisel Verileri Koruma Kurumu tarafından sorumluları tarafından Sicile bilgi girişi yapılmasına imkân sağlayan sistem hazırlanmış ve Veri Sorumluları Sicil Bilgi Sistemi (Verbis) adı ile hizmete açılmıştır (Kişisel veri işleme envanteri, 2019).

2.1.5.3. Envanter ve Verbis'in Farkları

Envanter ve Verbis, veri işleme sistemi olarak benzer gözükseler de 3 konuda birbirinden ayrılmaktadır.

1) Verbis' te; veri işleyen sorumlu tarafından kişisel verilerin işlenme süreci, işlenip işlenmediği, işlenmiş olması durumunda hangi amaçlarla işlendiği, veri aktarımı olup olmadığı, aktarım yapıldıysa; alıcı grupları, varsa saklama süresi, ilgili kişiler ve alınan güvenlik tedbirleri konusunda bilgi girişi yapılması gerekir. Envanterde ise veri sorumlusunun iş süreçlerinin tamamında kişisel veri gerçekleştirdiği "faaliyetleri, belge, doküman ve kayıtlar gibi kişisel veri içeren tüm fiziksel veya elektronik ortamlarda işlenen kişisel verilerin her biri için ayrı ayrı olmak üzere hangi amaç ve hukuki gerekçelerle işlendiği, aktarım olup olmadığı, aktarım yapılan üçüncü taraflar, saklama süreleri, veri konusu kişi grupları ve alınan güvenlik tedbirleri" bilgisini içeren ve çok daha detaylı olarak hazırlanan bir rapor olması gerekir.

Kısaca Verbis' te sadece başlıklar halinde kategorik bazda bilgi girişi yapılırken, Envanterde bu verilerin, alt kırılımlarıyla birlikte detaylı şekilde yer alması gerekmektedir (Kişisel veri işleme envanteri, 2019).

2) Kanunun 16. maddesi gereği kamunun erişimine açık tutulan Verbis' e girilmiş olan bilgiler isteyen kişiler tarafından görüntülenebilmekte iken, Envanter 'de ise sadece veri sorumlusunun kendi bünyesinde kalacak ve kamuya açık değildir. Yalnızca Kurul tarafından talep edilmesi durumunda Envanterin Kurula ibraz edilmesi zorunludur (Kişisel veri işleme envanteri, 2019).

3) Verbis için bir sistem hazırlanmış ve belirlenen sistemden giriş yapılması zorunlu tutulurken Envanterin için belirli bir biçimsel yönlendirme yapılmamıştır. Envanter, örneğin Microsoft Office (Excel, Word) dosyası şeklinde veya veri tabanında ilgili dosyalarda tutulabilecektir (Kişisel veri işleme envanteri, 2019).

2.2. Veri Sahibinin Haklarına İlişkin Kavramlar

2.2.1. Bilgi Edinme Hakkı

Kişinin, kişisel verilerin işlenme sürecine dair birtakım bilgileri talep etme hakkına sahip olması, verilerin korunmasına dair diğer haklara kaynaklık eden ve ilgili kişinin menfaatlerini koruyan ana ilkedir (Şimşek, 2008). Genel anlamda, kişilerin devlet müdahalesi olmaksızın kendi seçimleriyle ve haberleşme imkânları ile her türlü bilgiyi elde edebilmesini, devlet müdahalesi olmadan tüm özel kaynaklardaki bilgiye ulaşabilmesini ve devletin elinde tuttuğu kamuyu ilgilendiren tüm verilere erişebilmesini ifade etmektedir. Dar anlamda ise bilgi edinme hakkı, devletin elinde bulunan her türlü resmi veriye erişim hakkı olarak tanımlanabilir (Soykan, 2006).

4982 sayılı Bilgi Edinme Hakkı Kanunu, kişilerin bilgi edinme hakkını kullanmalarına ilişkin esas ve usulleri düzenlemektir. İlgili Kanun, bilgi edinme hakkının sınırsız olmadığını belirtmiş ve bu hak kapsamında değerlendirilemeyecek bilgi türleri olduğunu belirtmiştir. Bu bilgi türlerinden biri de özel hayatın gizliliğine ilişkin bilgilerdir. Bu doğrultuda, Bilgi Edinme Kanunu'nun 21. maddesi aşağıdaki hükmü getirmektedir.

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 (Bilgi Edinme Hakkı Kanunu, 2003).

Bu kanun hükmü ile kişisel sağlık verileri bilgi edinme hakkı kapsamı dışında tutulmuştur. Kişisel kendilerine ait sağlık verileri hakkında bilgi edinebilir ancak başka kişilere ait kişisel sağlık verileri konusunda bilgi edinme hakları yoktur. Hukuki anlamda hasta mahremiyetini destekleyici bir maddedir. Kişilerin özellikle sağlık verileri edinme sürecinde kendi adına yapılan tüm işleyişleri bilme hakkına sahip olduğu gibi, yapılacak tüm işlemlerden öncesinde de bilgi alma hakkına sahiptir. Yapılacak işlemler için kişilerin anlayacağı biçimde medikal terimleri açıklayarak, süreçlerle ve risklerle ilgili bilgi verilip Aydınlatılmış Onam Forumu'na kişinin imzası eğer reşit değil veya engeli olması sebebiyle imzalayamıyor ise birinci derece yakınının imzası alınmalıdır.

2.2.2. Erişim Hakkı

Kişinin, kişisel verilerinin ne zaman, kim tarafından, nereye, hangi amaçla ve hangi yöntemle işlendiğini bilebilme imkanının yaratılmasıdır. Hukuka uygunluk ve mahremiyet konusu çerçevesinde şeffaflığın amaç edinilerek yapılan düzenlemelerin önemli bir sonucudur. 2020 yılı itibariyle yapılan düzenleme ve uygulamalarla da faal olarak kişilerin "Erişim Hakkı" aktif olarak sağlanacaktır.

"Envanter ve Verbis'in farkı" konusunda anlatıldığı üzere yapılan bu uygulamalar kişilerin "Erişim Hakkı" nı uygulamaya yönelik hukuk, dürüstlük ve mahremiyet anlamında amaca uygun ve şeffaflık ilkesine dayanan bir uygulama olduğunu söyleyebiliriz.

2.2.3. Düzeltme Hakkı

Kişilerin veri hakkında bilgi edinme hakkının yanı sıra eriştiği verinin doğru olmadığı durumlarda bunu düzelttirme hakkına sahiptir. AB koruma Direktifi Madde 26'da "İşlemin amaçları göz önüne alındığında, veri sahibi ek bir beyanda bulunmak da dahil olmak üzere, hatalı veya eksik olan kişisel verilerin düzeltme hakkına sahip olacaktır" olarak ifade edilmiştir (Avrupa Parlamentosu Yönetmeliği, 2016).

Talep edilmesi durumunda veri sorumlusu en kısa sürede gerekli düzenlemelerin yapılması gerekmektedir. Ayrıca yapılan bu düzeltmelerin veri paylaşılan kurumlara da güncel bilgi olarak bildirilmesi zorunludur (Sarıusta, 2018).

2.2.4. Unutulma Hakkı

Unutulma hakkının bireye ait ana haklardan biri olarak tanınması konusunda Avrupa Komisyonu'nun da görüşülmesi ve önerilmesi oldukça etkileyici olmuştur. Komisyonun önerisine göre; eğer geçerli bir sebep söz konusu değilse kişisel verilerin saklanmaması ve silinmesi gerekmektedir (Gülener, 2012). Unutulma hakkın uygulanabilmesini sağlayacak yöntem; manuel gerçekleştirilen işlemelerde fiziki evrakın yok edilmesi, otomatik yöntemlerde ise verilerin kayıtlı olduğu taşıyıcılarından veya ortamlardan çıkartılması, ilişkisini koparacak şekilde ayrıştırılarak yok edilmesidir (Başalp, 2004). 6698 sayılı kişisel verileri koruma kanunu madde 7 de bu durum aşağıdaki gibi ifade edilmiştir.

Madde 7- (1) "Bu Kanun ve ilgili diğer kanun hükümlerine uygun olarak işlenmiş olmasına rağmen, işlenmesini gerektiren sebeplerin ortadan kalkması hâlinde kişisel veriler resen veya ilgili kişinin talebi üzerine veri sorumlusu tarafından silinir, yok edilir veya anonim hâle getirilir" (Resmî Gazete, 2016).

Uluslararası ve ulusal hukukta kanunlar ile güvence altına alınan unutulma hakkının amacına uygun kullanımı oldukça önemlidir. Öte yandan kurumların özellikle sağlık kuruluşlarının ve sigorta şirketlerinin silmemesi gereken veriler ve kayıtlar bulunmaktadır. Kişiye ve kuruma göre vaka bazlı değerlendirmek gerekmektedir. Kişisel bilgilerinin silinmesini isteyen kişiler tarafından unutulma hakkının kullanılması verilerin yedekleme ve arşivleme politikalarının uygulanması da gerektiği için dikenli bir konu haline gelmiştir (T.C. Resmî Gazete, 2020).

GDPR'da bu konunun netliği tam olarak belirtilmemiş olsa da 6698 sayılı KVKK'nın 3. maddesinde kişisel verilerin işlenmesi kavramı tanımlanmış, 4. Maddesinde; "İşlenen kişisel verinin işlendikleri amaçla bağlantılı, sınırlı ve ölçülü olması ve ilgili mevzuatta öngörülen veya işlendikleri amaç için gerekli süre kadar muhafaza edilmesi gerektiği" belirtilmiştir. Kişisel veriler, ilgili mevzuatta öngörülen veya işleme amaçlarına uygun süre kadar saklanır (HES, 02.08.2020). Kişiler unutulma hakkını kullanmak ve kişisel verilerinin imha edilmesi/yok edilmesini talep etse dahi muhafaza edilmesi gereken süre tamamlanmadan bu talep gerçekleştirilememektedir.

2.3. Kişisel Sağlık Verisi Kavramı

Sağlık sistemlerinin bir taraftan güvenilir, ihtiyaca uygun ve tanıya yönelik sağlık hizmeti üretirken diğer taraftan geleceğe planlama yapmak ve sonuç üretmek hedefiyle sürekli ve güvenilir kayıt tutma zorunluluğu vardır. Sağlık sistemlerinde tutulan tüm kayıtlar geçtiğimiz dönemlerde uzun yıllar manuel işlemlerle yapılsa da günümüzde teknolojinin de hayatımıza yerleşmesiyle elektronik ortama taşınmıştır.

Örneğin 2005'te ABD'de yapılan bir araştırmada; hastanelerin ve hekimlerin %30'u hastalara ait tıbbi kayıtları elektronik olarak kullanırken, 2011 yılının sonu itibarıyla bu oranda artış görülmüş ve yaklaşık olarak hastanelerin %75'i ve hekimlerin %45'i tıbbi kayıtları elektronik olarak kullanır hâle gelmiştir. Ayrıca ABD'deki hastanelerin yaklaşık %45'i 2013 yılından beri bölgesel ve yerel sağlık verilerinin paylaşıldığı HIEs (Health Information Exchanges) elektronik platformlarında yer almış ve önümüzdeki yıllarda da bu platforma veri kaynağı aktararak devamlılığını sürdüreceği düşünülmektedir (Groves, Kayyali, Knott & Kuiken, 2013). Ancak erişimi kolaylaştırmasına rağmen elektronik ortama aktarılan sağlık verilerinin kişi mahremiyetinin maddi ve manevi yönden korunması için gerekli önlemlerin alınması gerekmektedir.

Şekil 2.1: Elektronik Sağlık Kayıtlarının Üç Temel Paydaşı (Kohli ve Tan, 2016)

Kişisel sağlık verileri hassas veri grubuna girmektedir. Yani hastanın mahremiyeti olan kişisel özel bilgiler, aile verileri, güvenlik verileri, ayrımcılığa uğramasına sebep olabilecek unsurları barındırması sebebiyle başka kişilerin eline geçmesi insani haklardan mahrum kalmasına sebep olabilecek bir durumdur. Şekil 2.1'de görüldüğü gibi kişisel sağlık verileri bu verilerin kaynağı olan hasta, veri Sağlayanlar ve Toplayanlar olarak Elektronik Sağlık verilerinin oluşumu sağlanmaktadır. Bu sebepten Elektronik Tıbbi Kayıtlar (ETK) ve Elektronik Sağlık Kayıtları (ESK)'nın teknolojik olarak etik ve hukuk ilkeleri göz önüne alınarak ihtiyaç doğrultusunda kayıt altına alınıp ve işlenmesi gerekmektedir.

Genel anlamda günümüzde bilgi güç olarak kabul edilir durumdayken verilerin toplanması ve işlenmesi gibi süreçlerde mahremiyetin önemsenmemesi ve kişi mahremiyetine zarar verilmesi güçsüzlüktür. İnsanın varlığına saygı mahremiyeti korumayı gerektirir. Bunun sağlık sektörüne olan yansıması ise kişisel sağlık verilerinin korunmasına yönelik önlemleri oluşturur. Teknoloji sayesinde bilgiye akışındaki sonsuzluk ve kişiye sağladığı yarar ve bu sürecin getirebileceği çıkar ilişkileri yetkisi günümüzde yaşanan ikilemlere temel oluşturmaktadır. Bu durumun çözümü ise mahremiyet gereği ve birey olmanın getirdiği özerklik duygusu ile kişinin kendisine denetim yetkisinin sağlanmasıdır.

Ayrıca bireylerin kişisel hakları konusunda gerektiği şekilde aydınlatılması ve mahremiyet hakkına uygun farkındalıklarının artırılması da yasal düzenlemelerin yaşama geçirilebilme sini de arttıracaktır (İzgi, 2014).

2.3.1. Etik Açıdan İnceleme

Özel hayat kavramını incelediğimizde karşımıza iki temel boyut olarak çıkar. Bunlardan birincisi; kişinin kendini ifade etmek amacıyla diğer bireylerle paylaşmak istediği limittir. Kişi bu boyutta iken özel hayatıyla ilgili olayları başka kişilerin bilmesinden rahatsızlık duymaz çünkü paylaşım limiti kendi kontrol alanı içerisindedir. Diğer bir boyutta ise, diğer bireylerin kimsenin bilmesini istemediği mahrem ve gizli kalmasını istediği bilgilerdir. Bu durumda özel alan ve gizli alan kavramları devreye girer. Kişinin özel alanında; yaşadıklarını sadece paylaşmak istediği kişilerle paylaşması yer alırken gizli alanında ise sadece kendisinin bildiği ve bu olayların sadece kendisinde saklı kalmasını istediği bilgiler bulunmaktadır (Sert, 2008).

Kişisel sağlık veriler daha önceki bölümlerde bilgilendirildiği üzere koruma altına alınan kanunlar olmasına rağmen bazı durumlarda yarar göz önüne alındığında, özellikle hastanın veya diğer bireyler için ciddi risk teşkil etmesi durumunda gizliliğin korunması ihmal edilebilmektedir. Buna örnek olarak; hastanın bakımını yapan kişilere tedavinin süreci hakkında bilgi vermek, yabancı hastalar için tercüman desteği alınarak üçüncü kişinin hastayla ilgili bilgilere ihtiyaç duyması, eğitimin devamlılık süreci adına tıp öğrencilerine öğretim, bulaşıcı hastalık, ülkede zorunlu olarak bildirilmesi gereken hastalıklar, istismara uğrayan kişilerin bildirilme zorunluluğu, salgın hastalıklar ve genetik hastalıklar verilebilir (UNESCO, 2008). Ayrıca tedavinin yanı sıra hem finansal hem de devlet kurumlarına gönderilmesi gereken bilgiler bulunmaktadır. Örneğin özel sağlık sigortasının tedaviyi karşılayabilmesi için hastanın tanısını ve tedavi bilgilerini talep etmesi ya da gebe hastaların kontrol ve aşı takiplerinin yapılabilmesi için Sağlık Bakanlığı'na gebliz kaydının yapılması gibi.

Kişisel sağlık verilerinin, kaydının tutulması bireylerin ve kamunun yararı açısından hem insanın yararı açısından önemli ve oldukça da önemlidir. Kayıt altına alınan sağlık verileriyle kişinin tedaviye erişimi ve tedavinin bütüncül yöntemlerle yapılabilmesi imkânı oluşmaktadır (HASUDER , 2016). Ayrıca verilerin kayıt altına alınmasıyla insan ve toplum sağlığı açısından planlama ve araştırmalarda kullanılması

amaçlanırken, bireyin önceden bilgilendirilerek, aydınlatılması ve rızasının alınması bu sürecin mahremiyet ve meslek ahlakı değerleri ile yönetilmesi etik açıdan gereklidir. Özellikle "birinci basamak hizmetleri, gebeliğin izlemi, gebelikten korunma yöntemleri, üreme sağlığı takibi, ana çocuk sağlığı, aşılar ve bağışıklama, salgınlar ve bulaşıcı hastalıklarla mücadele, toplumda en çok öldüren ve hasta eden hastalıkların izlenmesi ve bunlardan korunma, hastalık yükünün, morbidite ve mortalitenin tespit edilmesi, genetik bilgiler ve tüm bu unsurlarla akılcı ve kanıta dayalı yöntemlerle mücadele için kişisel sağlık verilerinin tutulmasına; korunma ve önleme amaçlı olarak kaydedilmesi ve incelenmesi" gibi konularda bilimsel olarak kayıtlara ihtiyaç vardır. Bu sürecin insan onurunu ve kişi özerkliğine saygı değerleri gözetilerek yapılması oldukça önemlidir. Tıbbi kayıtlar, sahibinin bilgisi olmadan ve etik olarak gerekçe sunulmadan üçüncü kişilerle paylaşılmamalıdır (Slowther & Kleinman, 2009). Sağlık çalışanlarının tamamı, hastaların özel hayatına saygı duyulması gerektiğini ve hastanın böyle bir hakkının olduğunu bilmeli buna uygun bir biçimde davranması gerekmektedir (Şenyürek, 2017).

2.3.2. Hukuksal Açıdan İnceleme

Kişisel sağlık verisi kavramı, kişisel verilerin "özel ve hassas" bir türü olması sebebiyle ek bir koruma ihtiyacı doğmaktadır. Hukuki olarak uluslararası sözleşmeler ve düzenlemeler ile ulusal düzenlemelerde bulmak mümkündür. Hukuki zemin, Genel Verileri Koruma Tüzüğü (GVKT) gibi kişisel sağlık verilerinin korunmasıyla doğrudan ilişkili düzenlemelerle sağlanabilir (Orak, 2019).

2.3.3. Ulusal Kaynaklar

Kişisel verilerin korunması konusunda ulusal mevzuatımızda; hukuk önünde bireylerin, kendilerine ait verilerinin kullanımına ilişkin son karar yetkisini ellerinde tutabilmeleri amacıyla çeşitli düzenlemelere yer verilmiştir. Yapılan yasal düzenlemeler kronolojik sıra ile aşağıda mevcuttur;

2.3.3.1. 1982 TC Anayasası

Anayasanın ikinci bölümü bireyin temel hak ve ödevlerini düzenlenir. Bu kısımda özel hayatın gizliliği, kişinin temel haklarından biri olarak ele alınmaktadır. Söz konusu olan hak, Anayasa'nın 20. maddesinde güvence altına alınmıştır. Bu maddede; "Teknolojik gelişmelerin temel hak ve hürriyetlere müdahale edebilmeyi kolay hale

getirmiş olması ve bu durumun hukuki bir sorun olarak kendini göstermesi bu konuda yasal düzenlemeler yapmayı gerekli kılmıştır" olarak belirtilmiştir (Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler, 2019).

2.3.3.2. 5237 Sayılı Türk Ceza Kanunu

1 Haziran 2005 tarihinde yürürlüğe giren Türk Ceza Kanunu'nda (TCK) kişisel verilerin korunması amacına yönelik tanımlanan suçlar, Dokuzuncu bölümde yer alan "Özel Hayata ve Hayatın Gizli Alanına Karşı Suçlar" başlığı altında düzenlenmiştir. "TCK 135. maddesi, birinci fıkrasında kişisel verilerin hukuka aykırı olarak kaydedilmesini yaptırıma bağlamıştır. Ayrıca maddenin ikinci fıkrası ise hukuka aykırı kaydetme eyleminin konusunun kişisel sağlık verileri olması durumunda cezalandırılacağı belirtilmiştir. TCK 136. Maddede ise kişisel sağlık verilerinin hukuka aykırı bir şekilde işlenmesi ve paylaşılması halinde de cezalandırılacağına yer verilmiştir" (TCK, 2004).

2.3.3.3. Türk Borçlar Kanunu

1 Temmuz 2012 yılında yürürlüğe giren 6098 sayılı kanunda "Kişisel sağlık verilerinin hukuka aykırı işlenmesi neticesinde maddi ve manevi zarara uğrayan kimse, maddi ve manevi tazminat davası açarak zararının karşılanmasını talep edecektir. TBK hükümleri, failin sorumluluğunun kaynağının tespiti ve bu noktadan hareketle yöneltilecek istemler bakımından önemlidir" (TBK, 2012).

2.3.3.4. 6698 Sayılı Kişisel Verilerin Korunması Kanunu

Ülkemizde ilk defa 1989 yılında kişisel verilerin korunmasına ilişkin bir kanun çıkarılması amacıyla bir komisyon oluşturulmuştur. Ancak oluşturulan bu komisyon henüz çalışmalarını tamamlayamadan dağılmıştır. 2000 yılına gelindiğinde yeniden bir komisyon oluşturulmuş ve bu komisyon üç yıllık bir çalışmasının neticesinde bir kanun tasarısı hazırlamıştır. Fakat hazırlanmış olan kanun tasarısı çeşitli nedenlerle kanunlaşamamıştır. 2008 ve 2014 yıllarında, Adalet Bakanlığı öncülüğünde yeni bir tasarı hazırlanıp Türkiye Büyük Millet Meclisi'ne (TBMM) sunulmuşsa da yasalaşamayarak hükümsüz kalmıştır (Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler, 2019).

6698 sayılı Kişisel Verilerin Korunması Kanunu "95/46/EC Sayılı Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin Avrupa Parlementosu ve Avrupa Konseyi Direktifi" temel alınarak hazırlanmıştır (Gökçay & Arda, 2019).

Kişisel Verileri Koruma Kanununa göre; "Sağlık verileri özel nitelikli veri kapsamına sayılmıştır. Buna göre sağlık verileri, bazı durumlarda kişilerin açık rızası olmaksızın işlenemeyecektir. Açık rızanın aranmayacağı durumlarda ise sağlık verisi yalnızca halk sağlığının korunması, koruyucu hekimlik, tıbbî tanı, tedavi ve bakım hizmetlerinin yürütülmesi, sağlık hizmetleri ile finansmanının planlanması ve yönetimi amacıyla, sır saklama yükümlülüğü altında bulunan kimseler veya yetkili kurum ve kuruluşlar tarafından işlenebilecektir" (Orak, 2019).

2.3.3.5. Kişisel Sağlık Verileri Hakkında Yönetmelik

6698 sayılı Kişisel Verilerin Korunması Kanunu hükümleri kapsamında, sağlık hizmeti sunucularıyla bağlı çalışan ilgili kuruluşları tarafından yürütülen süreç ve uygulamalarda uyulacak usul ve esasları düzenlemektir (Resmî Gazete, 2016). Yönetmelikte, mevzuatta yer alan bilgiler daha detaylı ve spesifik konulara değinilerek hazırlanmıştır. Yedi bölümden oluşan yönetmelikte çocuklar ve ölü kişiler de dahil olmak üzere kişisel verilerin üçüncü kişilere paylaşımı süreci belirtilmiştir. Yönetmeliğe uyulmaması durumunda kanunda yer alan cezai yaptırım uygulanır.

2.3.4. Uluslararası Kaynaklar

2.3.4.1. Birleşmiş Milletler Örgütü

Mahremiyet kavramının bireyin hakkı olarak uluslararası alanda tanınması konusu ikinci dünya savaşını takip eden dönemlere dayanmaktadır (Holvast, 2007). BM İnsan Hakları Komisyonu tarafından hazırlanan ve 10 Aralık 1948'de kabul edilen İnsan Hakları Evrensel Beyannamesinin 12. Maddesi;

"Hiç kimse Özel hayatı, ailesi, meskeni veya haberleşmesi hususlarında keyfi müdahalelere, şeref ve şöhretine karşı tecavüzlere maruz bırakılamaz. Herkesin bu karışma ve tecavüzlere karşı kanun ile korunmaya hakkı vardır" (Resmî Gazete, 1948) şeklindedir.

Birleşmiş Milletler tarafından 1976 tarihinde kişisel verilerin korunmasına ilişkin standartları belirlemek amacı ile 45/95 sayılı Bilgisayara Geçirilmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeleri hazırlanmıştır. Bu belgenin yayımlanması ise ancak 14 Aralık 1990 tarihinde gerçekleşmiştir (Akçalı Gür, 2019).

2.3.4.2. Ekonomik Kalkınma ve İş birliği Örgütü

Kişisel verilerin korunmasıyla ilgili yayımlanmış ilk uluslararası belge OECD tarafından hazırlanan "Özel Yaşamın Korunması ve Kişisel Verilerin Sınır Ötesi Transferine İlişkin Rehber İlkelerini" temel alarak 1980 yılında yapılan bir çalışmadır. Rehber ilkelerin önemli bir tarafı da yurt dışına veri aktarımı konusuna özel olarak değinilmiş olmasıdır. OECD bu konulara öncelikli olarak ekonomik baktığı kabul edilirse kişisel verilerin yurtdışına aktarılması uluslararası ekonomik bir ölçüt olma potansiyeli olduğu gözükmektedir. Birçok ulusal düzenleme ise bu rehbere uygun olarak kaleme alınmıştır (Fred & Peter, 2014). Etki alanı olarak esnek hukuk kuralları alanına iyi bir örnektir (URL-4).

2.3.4.3. Avrupa Konseyi

a) 108 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi

Kişisel verilerin korunması konusunda yapılan çalışmalar neticesinde 28 Ocak 1981 tarihinde Strazburg'da imzalanan "Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi" 1 Ekim 1985 tarihinde yürürlüğe girmiştir. Ülkemizde ise; 28 Ocak 1981 tarihinde bu sözleşmeyi imzalayan ilk ülkelerden birisi olunmasına rağmen 17 Mart 2016 tarih ve 29656 sayılı Resmî Gazete'de yayımlanarak iç hukuka dâhil edilmiştir. Günümüzde 108 sayılı Sözleşme olarak da bilinen bu sözleşmenin temel amacı; "üye ülkelerde, uyruğu veya ikametgâhı ne olursa olsun gerçek kişilerin, temel hak ve özgürlüklerini ve özellikle kendilerini ilgilendiren, kişisel nitelikteki verilerin otomatik yollarla işleme tabi tutulması karşısında özel yaşam alanı haklarını güvence altına almaktır. 108 sayılı Sözleşmenin 4. maddesi çerçevesinde, iç hukukta kişisel verilerin korunmasına yönelik yasal düzenleme yapılması gerekli hale gelmiştir" (Wma Declaration, 2015).

b) 181 No'lu Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesi'ne Ek Denetleyici Makamlar ve Sınır Aşan Veri Akışına İlişkin Protokol

2001 yılında Avrupa Komisyonu 108 sayılı Sözleşme 'ye ek olarak 181 sayılı Protokolü (Ek Protokol) imzaya sunmuştur. Bu protokolle iki hedef gerçekleştirilmiştir. Bunlardan biri; "Öncelikle taraf ülkelere kişisel verilerin korunması alanında görevlerini tam bağımsızlıkla yerine getirecek denetleyici bir makam kurmaları şartı getirilmiştir. Bu durumda, kontrol edici makamlar araştırma ve müdahale etme yetkisine sahip olup aynı zamanda da hukuki süreçte aktif rol alabileceklerdir." "İkincisi ise taraf olan ülkeler taraf olamayan ülkelere kişisel veri aktarılmasına ancak ilgili devletin ya da organizasyonun denk bir koruma sağlayacağına emin olduktan sonra izin verebileceklerdir" (T.C. Resmî Gazete, 181 Sayılı Ek Protokol, 2001).

Türkiye, bu protokolü 8 Kasım 2001 tarihinde imzalanmış olmasına rağmen 5 Mayıs 2016 tarihli 29703 sayılı Resmî Gazete 'de yayımlanarak iç hukuka dâhil edilmiştir (Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler, 2019).

c) Avrupa İnsan Hakları Sözleşmesinin İlgili Hükümleri

Ülkemizin de kurucu üyeleri arasında bulunduğu Avrupa Konseyi tarafından hazırlanan ve 4 Kasım 1950'de Roma'da imzalanıp 3 Eylül 1953'te yürürlüğe giren "İnsan Hakları ve Özgürlüklerinin Korunmasına İlişkin Avrupa Sözleşmesi (AİHS)", kişisel verilerin işlenmesi hakkında doğrudan bir düzenleme içermemekle birlikte Avrupa İnsan Hakları Mahkemesi, geliştirdiği içtihatlarıyla kişisel verileri koruma altına almıştır. Diğer taraftan Sözleşme'nin "Özel ve Aile Hayatına Saygı Hakkı" başlıklı 8. Maddesinde;

1. Herkes özel ve aile hayatına, konutuna ve yazışmasına saygı gösterilmesi hakkına sahiptir.

2. Bu hakkın kullanılmasına bir kamu makamının müdahalesi, ancak müdahalenin yasayla öngörülmüş ve demokratik bir toplumda ulusal güvenlik, kamu güvenliği, ülkenin ekonomik refahı, düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için gerekli bir tedbir olması durumunda söz konusu olabilir olarak ifade edilmektedir.

d) İnsan Hakları ve Biyotıp Sözleşmesi

Sözleşme 03.12.2003 yılında kabul edilmiştir ve tam adı "Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Hakları ve İnsan Haysiyetinin Korunması Sözleşmesi: İnsan Hakları ve Biyotıp Sözleşmesi" dir. Sözleşmenin başlangıcında tarafların; 10 Aralık 1948 tarihinde Birleşmiş Milletler Genel Kurulu tarafından ilân edilen İnsan Hakları Evrensel Beyannamesi, 4 Kasım 1950 tarihli İnsan Hakları ve Temel Özgürlüklerin Korunması Sözleşmesi, 18 Ekim 1961 tarihli Avrupa Sosyal Şartı;16 Aralık 1966 tarihli Uluslararası Medenî ve Siyasî Haklar Sözleşmesini ve Uluslararası Ekonomik, Sosyal ve Kültürel Haklar Sözleşmesi, 28 Ocak 1981 tarihli Kişisel Verilerin Otomatik İşlenmesine Karşı Bireylerin Korunması Sözleşmesi, 20 Kasım 1989 tarihli Çocuk Hakları Sözleşmesini de göz önünde bulundurmasıyla Sözleşmede geçen hükümleri kabul ettiklerini belirtmektedir (5013 sayılı Kanun, 2013).

Sözleşmenin asıl amacı, "bireylerin insanların haysiyetini ve kimliğini koruyacak, biyoloji ve tıbbın uygulanmasında, ayrım yapmadan herkesin; bütünlüğüne ve aynı zamanda diğer hak ve özgürlüklerine saygı gösterilmesini de güvenceye alacak tedbirlerin alınmasını sağlamaktır." Bu hususstaki tedbirlerin alınması için taraf devletlere Sözleşmede yer alan hükümlerinin yürürlüğe sokulması bakımından gerekli hukuki düzenlemelerin yapılması yükümlülüğünü vermiştir (Kök, 2018).

2.3.4.4. Amsterdam Bildirgesi

1994 yılında Amsterdam'da yayınlanan ve Amsterdam Bildirgesi olarak da isimlendirilen Avrupa Hasta Haklarının Geliştirilmesi Bildirgesi, sağlık verilerinin işlenme sürecinde aynı zamanda etkin bir biçimde korunmasına yönelik olarak hastanın rızasının önemini özellikle belirtilmiştir. Altı bölümden oluşan bildirgenin, "Mahremiyet ve Özel Hayat" başlıklı dördüncü bölümünde, kişinin tıbbi durumu ve kimliğine ait bilgilerin ölümden sonra dahi gizli tutulması gerektiği belirtilmiştir. Ayrıca bu bölümde hastanın tıbbi bilgileri ve kimlik bilgilerinin hastanın açık rızası ve mahkeme izniyle açıklanabileceği, tıbbi bilgilerinin eksik, uygunsuz, eski olması sebebiyle yenileme, bazı kısımları çıkartma ve düzenleme gibi haklara sahip olduğu, kendi isteği dışında özel hayatına girilemeyeceği ve zorunlu durumlar haricinde hastanın onayı olmaksızın onayı dışında tıbbi müdahalenin gerçekleştirilemeyeceği

gibi hastalara ait genel hakları belirtmektedir (European Charter Of Patients' Rights, 2012). İçerik olarak benzer hükümler Dünya Tabipler Birliği Lizbon Hasta Hakları Bildirgesi'nde (Wma Declaration, 2015) yer almaktadır.

2.3.4.5. Direktifler

Direktifler; AB'nin ikincil mevzuatı kapsamında değerlendirilmekte ve üye ülkeler tarafından yerine getirilmesi zorunlu olan hukuki yükümlülükleri belirlemektedir. Ayrıca ilke olarak üye ülkelerin iç hukukunda doğrudan uygulanmasa da Direktifte öngörülen amaçların gerçekleştirilmesi açısından üye ülkeler için bağlayıcı olmaktadır (Özdemir, 2001). Kişisel verilerin işlenmesi, saklanması ve korunması alanında yayımlanan Direktifler 4 başlıkta incelenmektedir.

a) 95/46/EC Sayılı Veri Koruma Direktifi

Avrupa Komisyonu'nun 1990 yılında taslak Veri Koruma Direktifi'ni yayımlamıştır. Komisyonun hazırladığı bu metin daha sonra yapılan çalışmalarla gözden geçirilerek, Bakanlar Konseyi tarafından Kişisel Verilerin İşlenmesi ve Serbest Dolaşımı Bakımından Bireylerin Korunmasına İlişkin 95/46/EC sayılı Direktif adı altında 20 Şubat 1995 tarihinde kabul edilmiştir (95/46/EC Direktifi, 1990). Direktif yedi temel bölümden oluşmaktadır. Direktifte sırasıyla; "genel hükümler, hukuka uygunluk sebepleri, hukuki tedbirler, sorumluluk ve yaptırımlar, kişisel verilerin üçüncü ülkelere transferi, davranış kuralları, denetleyici otorite ve topluluk düzeyinde uygulama tedbirleri" bölümleri yer almaktadır (Civelek, 2011).

b) 2002/58/EC sayılı E-Gizlilik Direktifi

Elektronik haberleşme sektöründe, kişisel verilerin işlenmesi ve gizliliğin korunması amacı ile ilgili 12 Temmuz 2002 tarihinde "2002/58 / EC sayılı Avrupa Parlamentosu" tarafından "Konsey Direktifi" yayımlanmıştır. Teknolojinin gelişmesiyle elektronik haberleşmede yaşanan istenmeyen durumlar karşısında, kişisel verilerin işlenmeye karşı savunmasız hale gelmesi ve kişilerin özel hayatlarının gizliliğinin korunmasının zorlaşması karşısındaki olumsuz sonuçları engelleme amacını taşımaktadır (Hayrunnisa, 2009). E-Gizlilik Direktifinde 95/46/EC sayılı direktife göre daha koruyucu hükümler vardır ancak Verilerin Korunması Direktifi'ndeki gibi uygulanacak hukuk hükümlerinin mevcut olmaması sebebiyle uygulama alanı belirsiz kalmıştır.

Bunun yanında E-Gizlilik Direktifi, 95/46/EC'nin tamamlayıcısı ve daha özel bir düzenlemesi olarak nitelendirilmekte, 2009 yılında ise 2009/136/EC sayılı Vatandaş Hakları Direktifi ile değiştirilmiştir (Atasoy, 2016).

c) 2009/136/EC sayılı Vatandaş Hakları Direktifi

2009/136/EC sayılı Vatandaş Hakları Direktifiyle, E-Gizlilik Direktifinde yer alan konum verisi tanımı genişletilerek, "elektronik haberleşme hizmeti aracılığıyla" işlenen veriler de konum verisi kapsamına dâhil edilmiştir. Direktife göre; saklanan veya elektronik haberleşme hizmetinin teminiyle bağlantılı olarak başka şekilde işlenen kişisel verilere yetkisiz erişim, söz konusu verilerin tedbirsizlikle veya hukuka aykırı olarak yok edilmesi, kaybolması, değiştirilmesi ya da yetkisiz olarak açıklanmasına neden olan güvenlik ihlali, kişisel veri ihlali olarak değerlendirilecektir (URL-5).

"Direktifinin kişisel verilerin korunmasındaki bir diğer etkisi, özellikle çerezlerin indirilmesine ilişkindir. Artık kendi kişisel verilerine ulaşımı sağlayan bu indirme işleminin yapılabilmesi için kullanıcıların öncelikli olarak iznin alınması şart koşulmaktadır" (Jones, 2010).

2.3.4.6. Genel Veri Koruma Tüzüğü

İletişim vasıtalarının teknolojinin gelişimiyle doru orantılı olarak değişmesiyle birlikte veri işleme mekanizmaları da değişmiştir. Yalnızca ülkemizde değil dünya genelinde veri işlenmesi konusunda hukuki koruma önlemlerinin alınması ihtiyacı doğmuştur.

Yönetmelik Avrupa Parlamentosu'nda 14 Nisan 2016 tarihinde onaylanmış, iki yıllık bir uyum sürecinden sonra 2018 yılında yürürlüğe girmiştir. GDPR'dan önce yürürlükte bulunan 95/46/EC sayılı Direktifi yürürlükten kaldırmıştır. Tüzük, Avrupa Birliği'ne üye devletlerin iç hukuku açısından herhangi bir uyumlaştırma gerektirmeksizin, doğrudan bağlayıcıdır.

General Data Protection Regulation (GDPR) yani Türkçe anlamıyla Genel Veri Koruma Yönetmeliği (GVKT) 2016/679, Avrupa Birliği hukukunda, tüm Avrupa Birliği ve Avrupa Ekonomik Alanı içerisinde yer alan bireyler için veri koruma ve gizliliğine ilişkin bir yönetmeliktir. GDPR öncelikle bireylere kendi kişisel bilgilerini kontrol altına almalarını ve AB içerisindeki şirketlerin bu yönetmeliklerle uyumlu hale

getirilmesini amaçlamaktadır. Kişisel verileri işleten tarafların veri koruma ilkelerini uygulamak için gerekli teknik ve kurumsal önlemleri alması gerekmektedir. Kişisel verilerin ele alındığı iş süreçleri, veri koruma ilkeleri göz önünde bulundurularak tasarlanıp yapılmalı ve verileri korumak için önlemler alınmalıdır. Hiçbir kişisel veri, yönetmelikte belirtildiği şekilde yapılmadığı veya ilgili kişiden (kişisel veri sahibinden) açık bir onay almadığı sürece işlenemez. İlgili kişi bu izni istediği zaman iptal etme hakkına sahiptir. Kişisel veri işletmecileri, her türlü veri toplama işlemlerinde verinin işlenme amacını, yasal dayanaklarını, verilerin ne kadar süreyle sakladığını ve herhangi bir üçüncü tarafla veya Avrupa Ekonomik Alanı dışında bir yerde paylaşılıp paylaşılmadığını açıkça belirtmesi gerekmektedir. Kişisel veri sahipleri, istediği zaman kendisine ait depolanan verilerin bir kopyasını talep etme ve bu verileri belirli koşullar altında silme hakkına sahiptir (GDPR, 2018).

2.4. Aydınlatma Yükümlülüğü ve Açık Rıza

Kişisel veri işleme faaliyetinin ilgili kişinin açık rızasına bağlı olması durumunda, veri sorumlusunun aydınlatma yükümlülüğü ve açık rıza alınması işlemlerini ayrı ayrı yerine getirilmesi gerekmektedir (Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, 2019).

2.4.1. Aydınlatma Yükümlülüğü

Genel anlamıyla kişisel verilerin işlenmesi konusunda bireyin bu konuda; bilgilendirmeye dayanan ve özgür iradeyle verilen açık rızası oldukça önemlidir. Sağlık ve cinsel hayat dışındaki özel nitelikli kişisel veriler sadece kanunlarda öngörülen hâllerde ilgili kişinin açık rızası aranmaksızın işlenebilmektedir (URL- 24). Veri sorumlusunun aydınlatma yükümlülüğünden muaf tutulduğu durumlar:

1. Kişisel veri işlemenin suç işlenmesinin önlenmesi veya suç soruşturması için gerekli olması.
2. İlgili kişinin kendisi tarafından alenileştirilmiş kişisel verilerin işlenmesi.
3. Kişisel veri işlemenin kanunun verdiği yetkiye dayanılarak görevli ve yetkili kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşlarınca, denetleme veya düzenleme görevlerinin yürütülmesi ile disiplin soruşturma veya kovuşturması için gerekli olması.

4. Kişisel veri işlemenin bütçe, vergi ve mali konulara ilişkin olarak Devletin ekonomik ve mali çıkarlarının korunması için gerekli olması (Resmî Gazete, 2016)

2.4.2. Açık Rıza Onamı

Açık Rıza onamının alınması, kişinin sahip olduğu verinin işlenmesinde kendi isteğinin olduğu veya karşı taraftan gelen talep üzerine, onay verdiği anlamını taşımaktadır. KVKK'da; "belirli bir konuya ilişkin, bilgilendirilmeye dayanan ve özgür iradeyle olarak açıklanan rıza" şeklinde tanımlanmıştır. Ayrıca Anayasa'nın 20. maddesinde kişisel verilerin, sadece kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebileceği hüküm altına alınmıştır. Açık rıza, "6698 sayılı Kanun'da hem özel nitelikli kişisel veriler hem de özel nitelikli olmayan kişisel veriler bakımından temel hukuka uygunluk sebebi olarak öngörülmüştür" (Açık Rıza Kılavuzu, 2019).

Özel nitelikli olmayan kişisel verilerin işlenmesinde açık rızanın aranmadığı durumlar Kanun'un 5. maddesinin 2. fıkrasında belirtilmektedir. Buna göre:

1. Kanunlarda açıkça öngörülmesi.
2. 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
3. Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması
4. Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması
5. İlgili kişinin kendisi tarafından alenileştirilmiş olması
6. Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması
7. İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması (URL- 24).

Kanun'un gerekçesinde de belirtildiği gibi; Avrupa Birliği 95/46 EC sayılı direktifine göre açık rıza; ilgili kişinin kendisiyle ilgili veri işlenmesine, özgürce, konuyla ilgili yeterli bilgi sahibi olarak, tereddüde yer bırakmayacak açıklıkta ve sadece o işlemle sınırlı olarak verdiği onay beyanı şeklinde anlaşılmalıdır. Açık rıza verildiği gibi geri alınma hakkına da sahiptir (URL-24).

Her iki kanunda da açık rıza zorunluluğu olsa da kullanım sebebi için ayrım bulunmaktadır. Avrupa Birliği'nin kullandığı GDPR'da yalnızca özel nitelikli (hassas) verilerin işlenmesi için açık rıza aranmaktadır. Ülkemizde yürürlükte olan KVKK'ya göre kural olarak her türlü kişisel verinin işlenmesi için açık rızaya ihtiyaç duyulmaktadır. Bu bakımından Kanun, Avrupa Birliği düzenlemelerine göre daha fazla koruma öngörmektedir (Açık Rıza Kılavuzu, 2019). Veri sahibinin kişisel verilerinin işlenmesine ilişkin sözleşmeye ait rızanın, serbestçe verilmiş, spesifik, bilgilendirilmiş ve açık bir dille anlatılan bir biçimde olması gerekmektedir ve aynı zamanda veri sahibinin rızasını geri çekme hakkı olmalıdır (Handbook GDPR, 2018). Bununla birlikte kanunda yer verilen açık rıza tanımı kapsamında, açık rızanın 3 unsuru bulunmaktadır:

Belirli Bir Konuya İlişkin Olması

Verinin işlenmesi için verilen açık rızanın geçerli olması için; "belirli bir konuya ilişkin ve o konu ile sınırlı olması gerekir. Aynı zamanda veri sorumlusu ve veri işleyenlerce açık rıza beyanının hangi konuya ilişkin olarak istenildiğinin açıkça ortaya konulması gerekmektedir. Kişinin kendi irade açıklaması ile "kişisel verilerimin işlenmesini kabul ediyorum" şeklinde açık uçlu ve belirsiz bir rıza tek başına Kanun bağlamında "açık rıza" olarak kabul edilemez" (Açık Rıza Kılavuzu, 2019). Örneğin; hastalara pazarlama faaliyetleri kapsamında hastanelerde olan güncel bilgileri aktarmak gerekiyorsa bu konu açık rıza formunda belirtilmelidir.

Rızanın Bilgilendirmeye Dayanması

Açık rıza bir irade beyanı olup, kişinin özgür bir şekilde rıza gösterebilmesi için, neye rıza gösterdiğini de bilmesi gerekir. Bu konu Kanun'un 10. maddesinde düzenlenen "aydınlatma yükümlülüğü" kavramı ile de ilişkilidir. Kişinin sadece konu üzerinde değil, aynı zamanda rızasının sonuçları üzerinde de tam bir bilgi sahibi olması gerekir. Örneğin iletişim bilgisinin işlenmesini istemeyen bir hasta için hastanede olan güncel bilgiler, kampanyalar veya yeniliklerin kendisine iletilemeyeceği formda yazmalıdır. Bilgilendirme, veri işleme ile ilgili bütün konularda anlaşılır, açık ve sade bir dille gerçekleştirilmelidir. Genel biçimde ve muğlak ifadelere yer verilmemelidir. Örneğin; "… gibi amaçlarla, diğer mevzuatlarla" gibi genel ifadelerin netliği olmaması sebebiyle muğlak ifade olarak tanımlanmaktadır (URL-24). "Bilgilendirmenin

mutlaka verinin işlemesinden önce yapılması gerekir. İlgili kişinin aydınlatılması aynı zamanda kişinin kendi geleceğini belirleme hakkının bir yansımasını oluşturmaktadır" (Açık Rıza Kılavuzu, 2019). Hangi verilerin işleneceğini, hangi amaçla işlendiğini eğer açık rıza vermeme durumu var ise sonucunun ne olabileceği ile ilgili bilgilendirme de yapılmalıdır.

Özgür İradeyle Açıklanması

Kişinin kendi iradesiyle verdiği rıza, bireyin davranışının bilincinde ve kendi kararı olması halinde geçerlilik kazanır. Kişinin iradesini sakatlayacak her tür fiil, kişisel verilerin işlenmesi için verdiği rızayı da sakatlayacaktır. Tarafların eşit konumda olmadığı veya taraflardan birinin diğeri üzerinde etkili olduğu durumlarda rızanın özgür iradeyle verilip verilmediğinin dikkatle değerlendirilmesi gerekir. Özellikle işçi-işveren ilişkisinde, işçiye rıza göstermeme imkânının etkin bir biçimde sunulmadığı veya rıza göstermemenin işçi açısından muhtemel bir olumsuzluk doğuracağı durumlarda, rızanın özgür iradeye dayandığı kabul edilemez (Açık Rıza Kılavuzu, 2019).

2.5. Sağlık Sigortacılığı ve KVKK

Günümüzdeki teknoloji ile geçmiş dönemlerde kullanılan sağlık verilerini oluşturma ve saklama yöntemleri olarak çok farklı bir boyuta doğru ilerlemekteyiz. Kişilerin sağlık bilgileri, hekimlerin kişisel notlarından bilgisayar ortamına aktarılmış, hastanelerin arşiv departmanından dijital saklama alanlarına taşınmıştır. Bu durum hem bireysel hem de toplumsal birçok fayda sağlasa da önemli sakıncaları da beraberinde getirmiştir (Küzeci, 2018).

Hasta kayıtlarının tek elden bir seferden dijital ortama kaydedilmesi bilginin elden ele geçerek değişmesi ihtimalini azaltmıştır. Ayrıca dijital ortamlarda tutulan kayıtlar hem sağlık çalışanlarının süreçlerini daha kolay ilerletmesini sağlamış hem de hastalar için verilerine ulaşılabilirliği kolaylaştırmıştır.

2016 yılında yürürlüğe giren KVKK; kişisel verilerin toplanması, işlenmesi, depolanması ve silinmesi ile ilgili kurallar ortaya koymaktadır. Bu kanun kuralları ihlal eden kişilere ve kurumlara ise yüklü miktarda para cezası ve hapis cezası verilmektedir. Bu nedenle KVKK, hastalar hakkında birçok bilgiyi bünyesinde tutan

sigortacılık sektörünü yakından ve derinden ilgilendirmektedir. Günümüzde sağlık sigortacılığı alanında önemli çalışmalar yapılan, sigortacılığın hasta memnuniyeti, mevzuatlara uyum ve karlılık yapısı üzerine kurulu hale geldiği dikkate alındığında hasta memnuniyetinin sağlanması ve kârlılığın sürdürülebilmesi açısından KVKK önemli bir noktadadır (Kartal, 2018).

2.5.1. Genel Sağlık Sigortasında KVKK İşleyişi

2.5.1.1. GSS Tarihçesi

İnsanlar yaşamları boyunca kendi iradeleriyle ya da iradeleri dışında ortaya çıkan birçok sosyal, mesleki veya psikolojik risklere maruz kalmaktadır (URL-6). "Bu ihtiyaçtan doğan "Sosyal Güvenlik" toplumun bütün bireylerinin hiçbir ayrım ve ayrıcalık gözetilmeksizin hem ekonomik hem de sosyal bakımdan bugünlerinin ve yarınlarının güvence altına alınmasını amaçlayan; birbirleri arasında sıkı bir birlik ve uyum kurulmuş olan bir sistemler bütünü olarak tanımlanmaktadır" (Dördüncü Beş Yıllık Kalkınma Planı, 1977).

Bugünkü kullanımıyla sosyal güvenlik sistemi 19. yüzyılın sonlarına doğru ortaya çıkmıştır. Alman devlet adamı Bismarck tarafından oluşturulan sistemde, finansmanının işçi ve işveren primlerine ek olarak devlet katkılarıyla sağlandığı bir sosyal sigorta sistemi oluşturarak önemli bir çalışmaya imza atmıştır (Güzel, Okur & Canikoğlu, 2019). Osmanlı Devleti'nde sosyal güvenlik anlamında ilk örgütlenme, 13. yüzyılda önce Ahilik yani esnaf, zanaatkar, çiftçi gibi bütün çalışma kollarını içine alan ocaklar olarak, sonra Lonca teşkilatı olarak belli bir iş kolunda usta, kalfa ve çırakları içine alan dernekler ile ortaya çıkmış ve 18. yüzyıla kadar etkinliğini hissettirmiştir (URL-6). Cumhuriyetin ilk yıllarında, sosyal sigortalara benzeyen, fakat kişiler ve riskler açısından çok dar kapsamlı olmasına rağmen sayıca oldukça fazla olan birtakım emeklilik ve yardımlaşma sandıklarının kuruluşunu öngören kanunlar çıkarılmıştır.

Günümüzdeki işleyişe baktığımızda ise 1961 Anayasası ile sosyal haklara ve bu arada sosyal güvenlik hakkına anayasal bir nitelik kazandırılmıştır. 1961 Anayasasında, "Herkes sosyal güvenlik hakkına sahiptir. Bu hakkı sağlamak için sosyal sigortalar ve sosyal yardım teşkilatı kurmak ve kurdurmak Devletin ödevlerindendir" hükümlerine yer verilmiştir. 2006 yılına geldiğimizde primli ve primsiz sistemler ile oluşturulan

SSK, Bağ-Kur ve Emekli Sandığı kurumları 5502 sayılı Kanunla "Sosyal Güvenlik Kurumu" çatısı altında birleştirilmiştir. İllerde ise bu kuruluşların il/bölge müdürlükleri "Sosyal Güvenlik İl Müdürlüğü" adı altında bir araya toplanmıştır. Kişinin statüsü; işçi, esnaf, çiftçi veya memur fark etmeksizin süreçler sosyal güvenlik il müdürlükleri veya sosyal güvenlik merkezlerinden yürütülmektedir (URL-22).

Ayrıca teknolojinin gelişmesi ile Sosyal Güvenlik Kurumu, vatandaşlara daha hızlı, kolay erişilebilir ve kaliteli hizmet alabilmelerini sağlamak amacıyla e-devlet uygulamasını kullanmaya başlamıştır. Bu sayede kişiler kendisiyle alakalı olarak SGK başta olmak üzere tüm devlet kurumlarıyla olan işlemlerini ve kişisel verilerini dijital platformlardan görüntüleyebilmektedir.

2.5.1.2. Genel Sağlık Sigortasındaki Kişisel Veriler

Genel Sağlık Sigortası Kanunu'nun ana hedefi hem genel sağlık sigortası hem de sosyal sigortalar bakımından tüm ülke vatandaşlarına güvence sağlamak Genel Sağlık Sigortasından yararlanacak kişilerle onlara sağlanacak hakları, kişilerin bu haklardan yararlanma şartlarını ve finansman yöntemlerini belirlemektir.

Finansmanı sağlamak amacıyla uygulanan "Medula" Sistemi 01.09.2007 tarihinden itibaren üniversite hastaneleri ve özel hastaneler dahil tüm faturalandırma işlemleri için kullanılmaya başlanmıştır. Kurumlar hastalara ait olan tanı ve uygulanan her türlü tedavi ve işlemi sisteme kaydedip SGK sistemine elektronik faturalandırma ve verilen hizmetlerin geri ödenmesini sağlama amacıyla kullanılmaktadır.

1) Biyometrik Yöntemler

Biyometrik yöntemde, kişinin fiziksel veya davranışsal özelliklerinkinden tanınmasını sağlayacak, diğer kişilerden ayırt edilebilir ve bilgisayar üzerinden kontrol edilebilen otomatik sistemlerin tamamına verilen isimdir (Akgül, 2015). GDPR md. 4/14'e göre, biyometrik veri "Teknik işlemlerden sonra oluşturulan, bir kişinin fiziksel, psikolojik veya davranışsal bir özelliğine bağlı olan ve aynı zamanda bu kişinin yüz görüntüsü veya el yazısı karakteri gibi sadece kendine ait bir özelliğin belirlenmesine imkân

sağlayan herhangi bir kişisel veri" şeklinde kaleme alınmıştır (Avrupa Parlamentosu Yönetmeliği, 2016). Bu yöntemler günlük hayatta DNA, el, yüz, retina, parmak izi, ses, kişisel imza, vücut özellikleri, ölçüsü gibi örneklerler karşımıza çıkar.

Son olarak 15.11.2019'da güncellenen Medula Kullanım Kılavuzunda Biyometrik kimlik doğrulama zorunluluğu birinci maddesinde "Sağlık kurum ve kuruluşlarınca, kişilerin müracaatı aşamasında, acil hallerde ise, acil halin sona ermesinden sonra, nüfus cüzdanı, evlenme cüzdanı, sürücü belgesi, pasaport veya verilmiş ise kurumların sağlık kartı belgelerinden biri ile kimlik tespiti ve biyometrik yöntemlerle kimlik doğrulaması yapılması zorunludur. Kimlik tespiti, biyometrik kayıt işlemi veya biyometrik kimlik doğrulama işlemini usulüne uygun yapmayan ve bu nedenle bir başka kişiye sağlık hizmeti sunulması nedeniyle Kurumun zarara uğramasına sebebiyet veren sağlık hizmeti sunucularından ödenen tutar geri alınır." şeklinde belirtilmiştir (Sağlık Yazılımı Daire Başkanlığı, 2019) ve biyometrik doğrulama zorunlu hala getirilmiştir. Bu bağlamda; "söz konusu sistem, yasal bir dayanağı olmaması nedeniyle eleştirilerin odak noktası olmuştur. Fatura ödemesi için kişilerin ne tür hizmetler aldığı aktarılması ve bu bilgilerin korumasının ne derece sağlandığı bilinmemekle birlikte, bu bilgilere kimlerin ulaşma ihtimalinin olduğu da bilinmemektedir. 2013 yılında "Genel Sağlık Sigortası MEDULA Web Servisleri Kullanım Kılavuzu"nda değişiklikler gerçekleşmiştir. Bu değişikten sonra özel ve üniversite hastanelerinde "Avuç İçi Damar İzi" uygulanmaya başlanmış ve tedavi görecek hastaların sigortalılara tüm süreçlerinde (muayene, kontrol muayenesi, diyaliz uygulaması, kemoterapi, radyoterapi ve fizik tedavi gibi) işlemlerin yapılacağı her seferde kimlik doğrulaması yaptırmak zorunluluğu getirilmiştir (Ömür, 2018).

Türk Tabipler Birliği tarafından ilgili Kılavuzun hükümlerinin iptali ve yürütmenin durdurulması isteminin kabulü için Danıştay'da dava açmıştır. Danıştay, 15.Dairesi 11.09.2014 tarih ve 2014/4652 sayılı kararla biyometrik kimlik doğrulama sisteminin uygulamasını durdurulmasına karar vermiştir (URL-20). 31.5.2006 tarihli ve 5510 sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanunu'nun "Sağlık Hizmetlerinden Yararlanma Şartları" başlıklı 67. maddesinin üçüncü fıkrasına, 1.3.2012 tarihli ve 6283 sayılı Kanun'un 1. Maddesine eklenen "Biyometrik yöntemlerle kimlik sorgulamasının yapılması ve/veya" ibaresinin Anayasa'nın 13. ve 20. maddelerine aykırı olduğunu ileri sürerek yürütmenin durdurulmasına ve iptal edilmesi için yine

konusu aynı olan E: 2014/1150 sayılı uyuşmazlık kapsamında Anayasa Mahkemesine başvurmuştur (URL-21). Anayasa mahkemesi; "itiraz konusu kuralla özel hayatın ve kişisel verilerin korunması haklarına yönelik olarak yapılan müdahalenin, öngörülen amaçla orantılı olduğu, müdahale edilen hakların özüne dokunmadığı ve demokratik toplum düzeninin gereklerine aykırılık teşkil etmediğine ve Anayasa'nın 13. ve 20. Maddelerine aykırı bir yönü olmadığından iptal isteminin reddine karar vermiştir" (Anayasa Mahkemesi Kararı, 2015).

Anayasa Mahkemesinin bu kararı vermesine rağmen belirtilmelidir ki; "parmak izi tartışmasız kişisel veridir. Yasal mevzuatımızda parmak izi alınması sınırlı şartların varlığı halinde 2559 sayılı Polis Vazife ve Salahiyet Kanunu (PVSK) ile kolluk kuvvetine verilmiştir. İç hukuk dikkate alındığında Anayasa'nın 17. maddesi ile düzenlenen; "Kişinin dokunulmazlığı, maddi ve manevi varlığı" hükmüne, 20. maddesi ile düzenlenen "herkesin, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahip olduğu, özel hayatın ve aile hayatının gizliliğine dokunulamayacağı" ve 13. maddede düzenlenen "temel hak ve hürriyetler özlerine dokunulmaksızın yalnızca Anayasanın ilgili maddelerinde belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilir." hükümlerine aykırı bir uygulama olduğu açıktır" (Ömür, 2018).

2) E - Nabız

E-Nabız Projesi, Sağlık Bakanlığı tarafından 2015 senesinde kurulmuştur. "E-Nabız Kişisel Sağlık Sistemi, sağlık hizmeti sunucusu olan hekim ile hizmeti alan kişi arasında, kişinin sağlığı hakkında doğrudan bilgi almasına, tıbbi görüntü ve raporlarının paylaşımına imkân sağlayan, arada herhangi bir üçüncü kişinin bulunmadığı, bu denli geniş kapsamlı ve güvenli bir hekim-hasta iletişim platformu olarak dünyada ilk ve tek sistemdir" (URL-7).

"Oluşturulan bu sistemle Sağlık Bakanlığı, işlenen bütün bilgileri kendisine aktarılması konusunda bir zorunluluk yaratmıştır. 2016/6 sayılı çıkarılan genelge ile hekimlere birçok sorumluluk yüklenmekte, kişisel verileri sisteme kaydetmeyen hekim hakkında yasal işlem uygulanacağı belirtilmektedir" (Sağlık Bilgi Sistemleri Genel Müdürlüğü, 2016).

3) Sağlık.net ve Sağlık.net2 Uygulamaları

Sağlık Bilgi Sistemleri Genel Müdürlüğü tarafından; "Ulusal Sağlık Bilgi Sistemi" kullanılmaya başlanmış ve bireyin doğmadan önce başlayıp tüm yaşamı boyunca sağlığıyla ilgili verilerin oluşturulduğu ve tüm vatandaşları kapsayan, bireyin sağlığıyla ilgili verilerin oluşturduğu işlevsel bir veri tabanının, tüm ülkeyi kapsayan bir iletişim sistemiyle paylaşılması ve tele-tıp uygulamalarına varan teknolojilerin mesleki pratikte kullanılmasını temel alan elektronik kayıt sistemidir. Bu sistem ayrıca sağlık hizmeti sunan tüm kurum ve kuruluşların insan gücü, taşınır, taşınmaz, idari ve mali verilerini de kayıt altına alacak şekilde tasarlanmıştır.' olarak ifade edilmiş olan, Ulusal Sağlık Bilgi Sistemi kapsamında, Sağlık.net ve Sağlık.net2 sistemleri gibi platformlar oluşturmuştur" (URL-8).

Sağlık.net, "Sağlık kurumlarında elektronik ortamda üretilen verileri, doğrudan üretildikleri yerden, standartlara uygun şekilde toplamayı, toplanan verilerden tüm paydaşlar için uygun bilgiler üreterek birinci, ikinci ve üçüncü basamak sağlık hizmetlerinde verim ve kaliteyi arttırmayı hedefleyen, entegre, güvenli, hızlı ve genişleyebilen bir bilgi ve iletişim platformudur" şeklinde açıklanmıştır (URL-8). Ancak daha sonra Sağlık Bakanlığı "Sağlık.net2 Veri Gönderimi" isimli bir Genelge yayınlamış ve burada sağlık hizmetinin gerçekleştiği bütün kurumların Ulusal Sağlık Veri Sözlüğü 2.0. (USVS) kapsamında yer alan tüm hastaların, sağlık verilerini, Sağlık.net2 sistemine göndermesini zorunlu tutarak kişilerin verilerini toplamaya devam etmiştir. Yayımlanan genelgede kişinin sağlığı ile ilgili olan ve olmayan çok sayıda özel bilginin kayıt altına alınmasının gerektiği belirlenmiştir" (Ömür, 2018).

17.11.2012 tarihinde yayımlanan genelgede; "Sağlık.net2 Veri Gönderimi için, Sağlık.net veri sistemine dahil olmayan, SGK ile sözleşmesi olmayan özel sağlık kuruluşlarını, muayenehaneleri, cezaevi hekimliklerini, aile hekimliği birimlerini de kapsayacak şekilde" genişletilmiş ve belirtilen sağlık kurum ve kuruluşlarında Sağlık.net2 sistemine veri göndermesi istenmiştir (URL-9). Ayrıca gönderilmesi gereken bilgiler arasında ; "adres, kimlik, iletişim bilgileri, hamilelik testleri, özürlülük durum sağlık geçmişi , özürlülük medeni hal, alkol madde-sigara kullanımı, iş, meslek, öğrenim durumu, gelir durumu, tetkik istenen kurumlar, hastalık şikayetleri, hastanın öyküsü, bütün tetkik sonuçları, 15-49 yaş arası kadınların, doğum, düşük türü ve

sayıları, kullanılan doğum planlaması yöntemi, kadın sağlığı işlemleri, kullanılan aile planlaması yöntemi, babanın kan grubu, son adet tarihi, gebe olduğu tespit edilmiş olsun ya da olmasın, doğum ya da düşükle sonuçlanan tüm gebelikler, ağız ve diş sağlığı ile ilgili tüm koruyucu hekimlik, teşhis ve tedavi işlemleri gibi birçok bilginin yer aldığı aktarılmaktadır" (Hakeri, 2018).

Bunların kayıt altında tutulması, işlenmesi veya paylaşılması da "insan onuruna aykırı bir durum oluşturabileceği düşünülerek genelgenin yayınlanmasının ardından, Türk Tabipler Birliği genelgenin iptal edilmesi isteği ve yürütmenin durdurulması amacıyla Danıştay'a başvurmuştur. Danıştay 15. Dairesi 12.6.2014 tarih ve 2013/2084 E. sayısı ile Genelge hakkında yürütmenin durdurulması kararı vermiştir" (Ömür, 2018). Yapılan hukuki bildirimler sonrası çıkarılan 663 sayılı KHK'de geçen 47/1 sayılı maddede; "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" şeklindedir (Ömür, 2018).

2.5.2. ÖSS'de KVKK İşleyişi

2.5.2.1. ÖSS Tarihçesi

Sigortacılığın varlık sebebi olan risk insanlık tarihi kadar eski bir kavramdır. Günümüzde olduğu kadar detaylı araştırmalar yapılmamış olsa dahi insanlar milyonlarca yıl önce de riskler ile başa çıkmak için bir takım risk yönetim teknikleri kullanmıştır (Yıldırım, 2012). Sigorta, sözcük kökeni olarak İtalyanca sicurta kelimesinden dilimize geçmiş olup esas itibariyle potansiyel bir riziko ve öngörülmeyen bir tehlike ihtimali sonucu ortaya çıkabilecek zararın sigorta şirketi tarafından karşılanmasıdır (Arseven, 1991). Türk Dil Kurumu'nun sözlüğünde ise, "sigorta" kelimesini, "bir şeyin veya bir kimsenin bir yönden ileride karşılaşabileceği zararı gidermek için, önceden ödenen prim karşılığında bu işle uğraşan kuruluşlarla yapılan iki taraflı bağlantısözleşmesi" olarak tanımlamaktadır (URL-1).

Sigorta kelimesi en geniş tanımıyla; "olabilecek zararların karşılanması amacıyla tarafların arasında yapılan özel sözleşme ile hukuksal bir çerçevede faaliyet gösteren, belirli bir prim karşılığında, kişi hayatının ya da organlarının veya kişi ve 08kuruluşların para ile ölçülebilir değerlerinin, sigorta kuralı, kanunu ve yönetmeliklerince belirlenmiş tesadüfi rizikoların gerçekleşmesinden doğacak maddi hasarlarını, ölçülen değer üzerinden ve gerçekleşen hasar oranında karşılayarak, sosyo-ekonomik zararları dağıtan ve önleyen, yatırımlara aktarılan fonları ile ekonomiye kaynak sağlayan işlemler bütünüdür" seklinde ifade edilebilir (Güvel, 2002).

Sigorta çeşitleri; "hayat dışı (elementer), hayat ve bireysel emeklilik" olmak üzere üç ana grupta toplanmaktadır. Özel sağlık sigortası, insan hayatının bir unsuru olması nedeniyle hayat sigortası grubu içerisinde gibi düşünülmesine rağmen, hayat dışı (elementer) bir sigorta türüne girmektedir. ÖSS gerekli primleri ödeyerek sisteme dahil olanların sigorta süresi içerisinde hastalanmaları veya herhangi bir kaza sonucu yaralanmaları halinde tedavileri için gerekli masrafları ile varsa gündelik tazminatları, sigorta şartları çerçevesinde, poliçede yazılı meblağlara kadar temin eden bir sigorta türüdür (Orhan T. & Mithat K., 2015).

Özel sağlık sigortacılığı uygulamaları ilk olarak günümüz gelişmiş ve sanayileşmiş ülkelerinde, bu ülkelerin sanayileşmeye başlamalarına tekabül etmektedir. Sanayileşme ile sendikalar, sendika dışı işçi örgütleri, işveren birlikleri gibi çeşitli meslek grupları kendi üyeleri için sağlık sigortası programları kurulmasını sağlamışlardır. Hastalık riskinin yüksekliği sebebiyle madencilik sektörü bu anlamda ilk uygulamaların yapıldığı alan olmuştur (Özsarı, 2003).

Ülkemizde, özel sağlık sigortacılığının uygulama alanı ilk olarak 1938 yılında Anadolu Sigorta A.Ş. tarafından riskli görevlerde bulunan işçiler için sağlık sigortası türevi bir teminat ile faaliyete başlamıştır. Bunu takip eden yıllarda bireysel sağlık sigortacılığına ağırlık veren "Halk Sigorta A.Ş." ile grup sağlık sigortalarına ağırlık veren "Genel Sigorta A.Ş., OYAK Sigorta A.Ş." ve beraberinde 1992 yılında kurulan "Bayındır Sigorta A.Ş." gibi sigorta şirketleri, bugün dahi farklı isimler ile özel sağlık sigortacılığı faaliyetine önemli katkılar sunarak ülkemiz sağlık sektöründe çalışmalarına devam etmektedirler (Pişkin, 2017). Özel Sağlık Sigortaları branşı olarak 1990 yılından itibaren aktif faaliyet gösterilmeye başlanmıştır. Sonra ise sayıları

artan özel sağlık sigorta şirketlerinin, piyasada yer edinmesiyle de poliçe teminat yapıları ve kapsamları belirlenmeye başlamıştır (Orhaner, 2018). Özel ve sosyal sigorta arasındaki farklılıkları aşağıdaki Tablo 2.1'de ki gibi özetlenebilir.

Tablo 2.1: Özel ve Sosyal Sigorta Arasındaki Farklılıklar (Güvel, 2002)

Kriter	Sosyal Sigorta	Özel Sağlık Sigortası
Menfaatler	Genel menfaatler	Özel menfaatler
Zorunluluk	Mecburi	İhtiyari
Kapsam	Belirli özelliklere sahip kimselere açık	Herkese açık
İlişki, Örgütlenme	Kanunla	Sözleşme ile
Ödeme, prim	Sigortalının gelirine ve mesleğine göre değişmekte	Ünitenin tehlike derecesine göre değişmekte
Garanti	Devlet garantisi söz konusu	Reasürans şirketine ihtiyaç bulunmakta
Gaye	Kamu hizmeti	Kar
Zararın tazmini	Kanunla tespit edilmekte	Ödenen primlerle sınırlı
Ortaya çıkışı	Amaçların sosyal politikaya olanak sağladığı bir düzen	Piyasa ekonomisinin hakim olduğu bir düzen ve sistemde

Ülkemizde kullanılan özel sağlık sigortalarının başlıca iki temel teminatı vardır. Bunlar; "ayakta ve yatarak" tedavi teminatlarıdır. "Ayakta tedavi teminatında; doktor, muayene, teşhis yöntemleri, küçük müdahalelerin girdiği ayaktan tedaviler ve ilaç giderlerini kapsamaktadır. Yatarak tedavi teminatında ise; ameliyatlı veya ameliyatsız, hastanede yatarak yapılan tedaviler için hastaneye yatış ve çıkış dönemi içindeki, doktor, ilaç, tıbbi tetkikler, oda ücreti, ameliyathane, gerekli ve zorunlu diğer tıbbi hizmetlere ait sigortalı kişinin hastanede tedavi gördüğü süre içerisinde oluşacak giderleri ve bazı durumlarda ambulans giderlerini de kapsamaktadır." Sağlık sigortası primleri yaşa, cinsiyete, kişinin sağlık öyküsüne, rizikosuna ve sigorta paketinin kapsamına göre belirlenmektedir.

2.5.2.2. Özel Sağlık Sigortası Kapsamında Kişisel Veriler

Dijital teknolojinin gelişmesi ile hastane sektörü ile doğru orantılı olarak sigortacılık sektörü de bu düzene uyum sağlamıştır. Dijital sigortacılık kapsamında; poliçe alımı ve uygulanması, provizyon ve tazminat işlemlerinin yapılması, sigortalı bilgilerine erişilmesi, fatura ve provizyon bilgilerine dijital platformlardan ulaşılması gibi işlemler

elektronik ortamda sigorta şirketlerinin bilgi sistemleri birimi tarafından oluşturulan ya da yazılımlarının dışarıdan satın alındığı bilgi sistemleri uygulamalarıyla mümkün olmaktadır (Yurdakul, 2016).

Özel sağlık sigortası şirketleri tarafından; sigortalıların almış oldukları ayaktan ya da yatarak tedavi faturaları, şirket içerisinde bulundurdukları tıbbi danışmanların desteği ile bireylerin poliçe limit ve teminatları çerçevesinde değerlendirerek ödeme kapsamına alıp almama kararı verilmektedir (https://www.tsb.org.tr, 11.03.2020). Bu kararın alınmasında hastaya ait geçmiş ve güncel tıbbi kayıtlar önemli rol oynamaktadır. Hastaların almış oldukları ve planlanan tedavilerine ait tıbbi kayıtlar, hastaneler tarafından sigorta şirketleri ile provizyon aşamasında paylaşılmaktadır. Tıbbi kayıtlar sigorta şirketinin bilgi sistemlerinin gelişmişliğine bağlı olarak elektronik provizyon sistemi üzerinden ya da e-posta yolu ile paylaşılmaktadır. Sigorta şirketleri ile paylaşılan tıbbi kayıtlar aşağıdaki gibidir (Kitapcı, 2019);

- Hastaya ait kimlik veya pasaport fotokopisi,
- Muayene formu,
- Laboratuvar ve görüntüleme sonuçları,
- Girişimsel işlem raporları,
- Patoloji raporu,
- Ameliyat raporu,
- Epikriz raporu,
- Konsültasyon raporu,
- Masak formu (75.000TL ve üzeri fatura bedellerinde)
- Kullanılan ilaç ve malzemelere ait detay bilgiler
- Adli vaka – trafik kaza tespit tutanağı ve alkol raporu
- E-devlet kayıtları

Sigorta şirketleri tarafından hastanın tedavi ödeme onayının alınması aşamasında paylaşılan bu tıbbi kayıtlar şirketlerin Elektronik Tıbbi Kayıt Sistemi'ne kaydedilir. Kaydedilen bu veriler sadece hastanın o anki tedavisine ait provizyon onayı ve fatura işlemlerinin gerçekleştirilmesi için değil hastanın bir sonraki sene satın alacağı

poliçenin ücret belirlemesi için aktüerya ismi verilen sigorta matematiği hesaplamasının yapılması ve ödemesi gereken poliçe ücretinin hesaplanmasında da kullanılmaktadır.

İlk defa özel sağlık sigortası alacak kişiler satın alma aşamasında sigorta şirketi tarafından kişinin geçmiş yıllara ait geçirdiği hastalıkların beyanı istenmektedir. Verilen beyan dahilinde özel sağlık sigortası karşılaşacağı riskleri hesaplamaktadır. Eğer daha önce geçirilmiş rahatsızlıklar var ise bunu kapsam dışına alıp muafiyet koyabilir. Dolayısıyla özel sağlık sigortaları gerçekleşmiş olan riskleri bir kenara koyarak henüz gerçekleşmemiş riskleri ele alır. Tüm bu süreç dahilinde sigortaların kişisel sağlık verilerine ulaşma gerekçeleri temelde risk analizi yapmalarıdır. Diğer sigorta türlerine göre risk hesaplamalarının daha fazla yapıldığı ve bu sebepten dolayı kişisel verilere en çok sağlık sigortacılığında ihtiyaç duyulmaktadır. İlgili süreç kapsamında özel sağlık sigortası şirketleri; kişisel verilerin toplanması, işlenmesi, aktarılması ve paylaşılması için Sigortacılık kanunun 9. Bölümde yer alan 31. Maddenin A ve B bentlerine dayanarak sağlık verilerine ulaşma hakkına ve bu verilerin sır olarak saklanması yükümlülüğüne sahiptir (Kişisel Sağlık Verileri II. Ulusal Kongresi, 2017).

Sigortacılık Kanunu 31. Maddesi a ve b bentlerin ilk bölümleri aşağıdaki şekilde açıklanmaktadır (5684 Sayılı Sigortacılık Kanunu, 2007);

Sır saklama yükümlülüğü

MADDE 31/A

1) Bu Kanunun uygulanmasında ve uygulanmasının denetiminde görev alanlar, bu Kanuna tâbi kuruluşların görevlileri ve yetkilileri, bu Kanuna tâbi kişiler ile bunların yanında çalışanlar ve dışarıdan hizmet alımı yoluyla sigortacılık sektöründe iş görenler, sıfat ve görevleri dolayısıyla öğrendikleri bu Kanun kapsamında faaliyet gösteren kişi ve kuruluşlar ile bunların iştirakleri, kuruluşları ve sigorta sözleşmesi ile ilgili kişilere ait sırları bu konuda kanunen açıkça yetkili kılınan mercilerden başkasına açıklayamaz, kendilerinin veya başkalarının yararlarına kullanamaz. Bu yükümlülük söz konusu sıfat ve görevlerin sona ermesinden sonra da devam eder.

2) Ancak, gizlilik sözleşmesi yapılması ve sadece risk değerlendirmesi amacıyla kullanılmak üzere sigorta şirketi, reasürans şirketi ve emeklilik şirketlerinin kendi aralarında doğrudan doğruya ya da Sigorta Bilgi ve Gözetim Merkezi vasıtasıyla yapacakları her türlü bilgi ve belge alışverişi sırasında sigorta şirketi, reasürans şirketi ve emeklilik şirketlerine ya da sigorta sözleşmesi ile ilgili kişilere ait, yanlış sigorta uygulamaları dâhil, sır niteliğindeki bilgilerin öğrenilmesi ve paylaşımı sır saklama yükümlülüğü dışındadır.

Sigorta Bilgi ve Gözetim Merkezi

MADDE 31/B

1) Türkiye Sigorta, Reasürans ve Emeklilik Şirketleri Birliği nezdinde, sigortalılar ve sigorta sözleşmesinden dolaylı da olsa menfaat sağlayanlara ilişkin olarak, yanlış sigorta uygulamaları dâhil, risk değerlendirmesine esas bilgileri toplamak ve bu bilgilerin sigorta, reasürans ve sigortacılık faaliyetinde bulunan emeklilik şirketleri ile Müsteşarlıkça belirlenecek kişilerle paylaşılmasını sağlamak amacıyla Sigorta Bilgi ve Gözetim Merkezi kurulur.

2) Bu maddenin birinci fıkrasında belirtilen şirketler, Sigorta Bilgi ve Gözetim Merkezine üye olmak zorundadır. Üye kuruluşlar, Sigorta Bilgi ve Gözetim Merkezince istenilen her türlü bilgiyi vermekle yükümlüdür.

2.5.2.3. Özel Sağlık Sigortalarında KVKK Sürecinde Mahremiyet Gerektiren Durumlar

Özel sigorta şirketlerinde elektronik sağlık kayıtlarının oldukça yaygın olarak kullanılması ve birçok çeşitli görevde personelin çalışma ortamında etkileşim içerisinde olmasından dolayı, bilginin gizliliği ve güvenliği özel sağlık sigortası sektöründe hassasiyet gerektiren bir durum haline gelmesine neden olmaktadır (Khan & Hoque, 2016, Kitapcı, 2019).

Hassas nitelikli veri olarak özel sağlık sigortalarıyla paylaşılan bu veriler hem uzun vadede ESK olarak sistemde tutulması hem de tedavinin karşılanıp karşılanmaması konusunda belirleyici olması sebebiyle sürece dahil olan kurumların, kişilerin ve teknolojik sistemlerin konunun önemine uygun olması gerekmektedir.

- Özel sağlık sigortası kuruluşlarında depolanan bu bilgiler sebebiyle sistem güvenliğinin bilgi sistemleri alt yapısının güvenli olması oldukça önemlidir. Özellikle sistem girişlerinde kullanıcı adı ve şifre ile giriş yapılmalı, şifreler diğer çalışanlar ile paylaşılmamalıdır.
- Provizyon sistemlerinin bütünleşmesi sebebiyle aracı sigorta şirketleri ile medula şifrelerinin paylaşılması bilgi güvenliğini tehdit etmektedir (Kitapcı, 2019).
- Sigorta şirketleri tarafından başka kurumlar ile paylaşılabilecek bilgiler için sigorta şirketleri kişisel verilerin korunması kanunu kapsamında hastadan mutlak açık rıza onayı almalıdır. Hizmet sunucusundan fatura ekine eklenmesi istenen ibranamesi için özel sigorta şirketleri önceden hastaya detaylı bilgi verilmelidir. Ayrıca sigorta poliçesi satın alınırken ve yıllık poliçe yenilenmelerinde hastalara bu konuda detaylı bilgi verilmelidir. Sigorta çalışanlarının, elektronik sağlık kayıtları ve kullandıkları bilgi yönetim sisteminde yer alan kayıtlara ulaşma, silme, paylaşma, değiştirme ve kopyalama gibi her türlü yetkinin bulunması elektronik sağlık kayıtlarının gizliliği ve güvenliği açısından risk teşkil etmektedir. Hassas verilerin her türlü mahremiyete aykırı kullanımı veri güvenliğini tehlikeye sokmaktadır. Bu sebepten dolayı çalışanların tüm işlem hareketleri sistem üzerinden kaydedilmeli ve belirli aralıklarla üst yönetim tarafından kontrol edilmelidir (URL-10).
- Hastaların onayı ve bilgisi dışında provizyon süreçleri ile ilgili ikinci bir kişiye bilgi verilmemelidir. Elektronik sağlık kayıtlarının, BYS üzerinden yaygın olarak kullanılmasından dolayı verilerin gizliliği ve güvenliğini kapsayan bir yönetmelik düzenlenmiştir. 23.10.2013 tarihinde yayınlanan Özel Sağlık Sigortaları Yönetmeliğinde yer alan 16. Madde ile bu konuda kişinin haklarını koruma altına almıştır (Özel Sağlık Sigortaları Yönetmeliği, 2020).

Bilgilerin gizliliği

MADDE 16

(1) Kişinin sigortalılık kayıtları ve yazılı onayıyla alınan sağlık bilgileri bireysel bazda tutulur.

(2) Şirket; sağlık bilgileri, sigortalılık kayıtları ve diğer bilgileri Sigorta Bilgi ve Gözetim Merkezi (SBGM) ve diğer yetkili merciler haricinde, sigortalının rızası olmadıkça, hiçbir gerçek ve tüzel kişiye veremez. ve Sigortalı hakkındaki sırlara vakıf

olan tüm gerçek ve tüzel kişiler, bu sırların saklı tutulmasından sorumludur. bentleri gereğince sigortalının yazılı onayıyla alınan sağlık bilgileri gizli tutulmaktadır.
(3) Sigortalı hakkındaki sırlara vakıf olan tüm gerçek ve tüzel kişiler, bu sırların saklı tutulmasından sorumludur.

2.5.3. Yurtdışı Bağlantılı Sigortalar İçin KVKK

Sağlık turizmine dahil olan kişiler farklı ülkelerde sağlık hizmetlerinden yararlanmayı tercih ettiklerinde hem hukuki olarak hem de kurum prosedürleri gereği hizmet aldıkları kuruluşlara birçok kişisel veri paylaşmak durumundadır. Kişinin paylaştığı bu bilgilerin gizli kalması, mevzuatların ve hastanın rızasının dışında açıklanmaması ve paylaşılmaması, sağlık turistinin özel yaşamının ve mahremiyetinin korunması açısından önem taşımaktadır (Sert, 2008, Akçalı Gür, 2019).

Yurtdışından tedavi amacıyla gelen sağlık turizmi hastalarının süreci aracı kurumlar tarafından başlatılmaktadır. Eğer sağlık turisti aracı bir kurum vasıtasıyla gelirse sağlık turistinin kişisel verileri, sağlık turizmi süreç akışı gereği öncelikli olarak aracı kurum ile paylaşılmakta ve bu kişisel veriler sağlık profesyoneli olmayan aracı kurum yetkilileri tarafından görüş fiyat veya tıbbi görüş alınması gibi amaçlarla elektronik ortamda başka kişilerle paylaşılmaktadır.

Yabancı özel sağlık sigortalı kişilerin, tedavi süreçleri gereği sigortalarından provizyon onayı alınması gerekmektedir. Çok büyük bir oranda ülkemizde bulunmayan yabancı özel sağlık sigortaların onay süreçleri için hastanın tedavisine ait tıbbi bilgiler ve kişisel veriler hastanın yurt dışında bulunan sigortası ile paylaşılmaktadır. 6698 sayılı KVKK Madde 9'da yurtdışına veri paylaşımı ile ilgili aşağıda yer 1. ve 2. fıkrası süreci net bir şekilde belirtmiştir.

(1) Kişisel veriler, ilgili kişinin açık rızası olmaksızın yurt dışına aktarılamaz.

(2) Kişisel veriler, 5 inci maddenin ikinci fıkrası ile 6. 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 yabancı ülkedeki veri sorumlularının yeterli bir korumayı yazılı olarak taahhüt etmeleri ve Kurulun izninin bulunması, kaydıyla ilgili kişinin açık rızası aranmaksızın yurt dışına aktarılabilir.

Veri İşleyen tarafların Sorumlulukları

Türkiye'de tedavi gören yabancı sigortalılara ait kişisel verilerin, Türkiye'de yerleşik olan veri sorumlusu tarafından, yeterli veri koruması bulunmayan ülkelerde yerleşik veri sorumlusuna aktarımına ilişkin olarak, 6698 sayılı Kanunun 9 uncu maddesinin ikinci fıkrasının (b) bendine yer alan hususlara asgari olarak yer verilmesi zorunlu kılınmıştır ve veri sorumlusu gerekli olan korumayı sağlayacağını taahhüt etmektedir (URL-11). Yeterli koruma yöntemlerine sahip olan ülkeler Kurulca belirlenerek ilan edilmektedir. Bu bağlamda yeterli koruma bulunmaması durumunda Türkiye'deki ve ilgili yabancı ülkedeki veri sorumlularının yeterli bir korumayı taahhüt etmeleri şartıyla söz konusu kişisel verilerin yurtdışına aktarılıp aktarılmayacağına Kurul tarafından karar verilmektedir (URL-12).

Veri aktaran, veri alıcısı, veri sorumlusu ve veri işleyen, aşağıda belirtilen ortak hükümlere ait yükümlülükleri yerine getirdiğini ve getireceğini bu taahhütnameler aracılığıyla garanti etmektedir;

- Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, belirtilen idari ve teknik tedbirlerin alınması hususunda veri işleyenle birlikte müştereken sorumludur.
- Veri sorumlusu ve veri işleyen, işledikleri kişisel verileri 6698 sayılı Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar.
- Veri sorumlusu ve veri işleyen için bu yükümlülük herhangi bir süre ile sınırlı değildir.

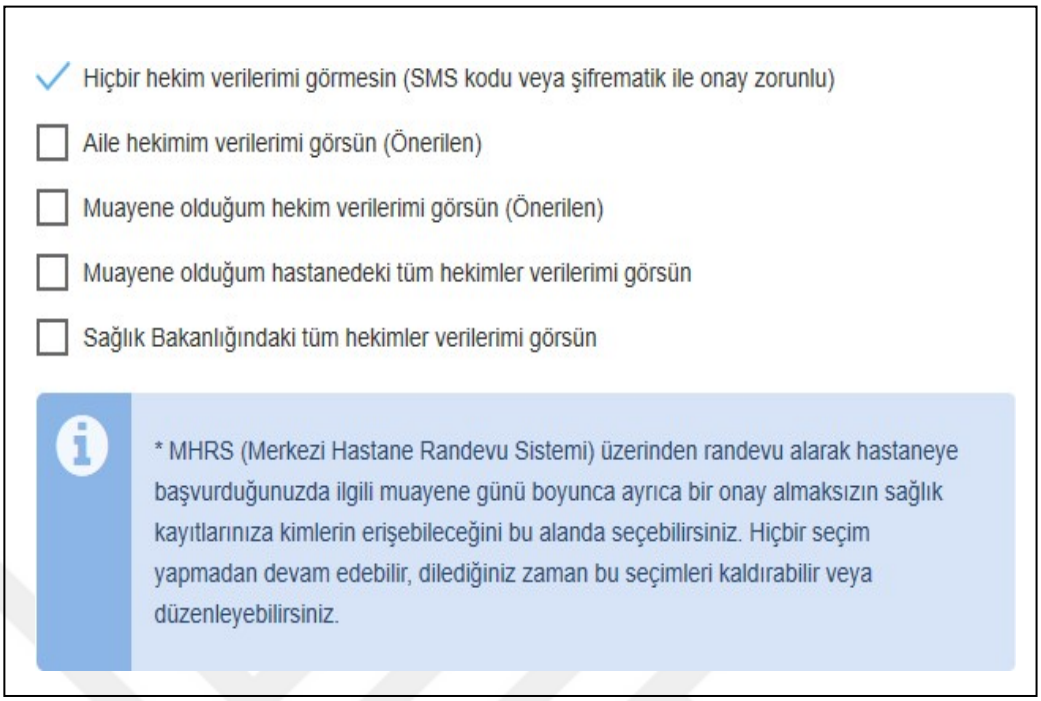
Ayrıca taahhütnamede veri aktaran ve veri alıcısı adına; "ad soyad, açık adres, irtibat numarası, e-posta, imza/ kaşe ve arsa sözleşmenin bağlayıcı olması için belirtilmesi gereken diğer bilgiler" eklenmelidir.

2.6. KVKK'nın Uygulamadaki Handikapları

Kişisel veriler günümüzde iş süreç zincirinin halkalarından biridir. Uzun yıllardan beri süregelen bu süreç zincirinde, ihtiyaçlar dahilinde güvenlik, hukuksal ve etik açıdan hakları koruma altına alacak hem dünyada hem de ülkemizde hukuki düzenlemeler yapılmıştır. Genel anlamda incelendiğinde ihtiyaç olunan düzenlemelerin yapıldığı ancak bazı dar alanlarda sahada yaşanan akışındüzenlenen ve kuralları belirtilen akışa uygulanamadığı durumlar olabilmektedir.

Sağlık sektöründe kişisel verilerin en çok paylaşıldığı alanlar SGK ve Özel sağlık Sigortalarıdır. Eğer hastalarımız aldığı sağlık sistemini sosyal güvencesi olan SGK sistemini kullanarak almak istiyorsa hastaneler bu hizmeti fatura etmek için hastane bilgi yönetim sistemi aracılığıyla "e- nabız" sistemine bilgi aktarmak zorundadır. 2015 yılında yayınlanan Kişisel Sağlık Verileri konulu "Hekimler ve Hastalar İçin El Kitabı"nda kişilere ait sağlık verilerin gönderimi için "Muayenehanelere, aile hekimliği merkezlerine, kamu-özel her türlü sağlık kuruluşuna başvuran kişilerin, (sağlıkları ile ilgili olanlar dahil) özel hayatlarına dair pek çok bilginin gönderilmesi istenerek, özel hayatın gizliliği ne bütünüyle müdahale edilmektedir." ifadesi yer almaktadır. Ayrıca başka bir ifadede de "Buna rağmen özel- kamu tüm sağlık kuruluşlarını ve hekimleri, kanuni bir dayanak ve hastaların aydınlatılmış onamı olmadan, hastalara ait kişisel sağlık verilerini göndermeye zorlayan Sağlık Bakanlığı, açıkça suç işlemektedir." açıklaması yapılıp hekimlere "Aydınlatılmış Onam Formu" olmadan bu sisteme entegre olmama çağrısı yapılmıştır (İstanbul Tabip Odası, 2015).

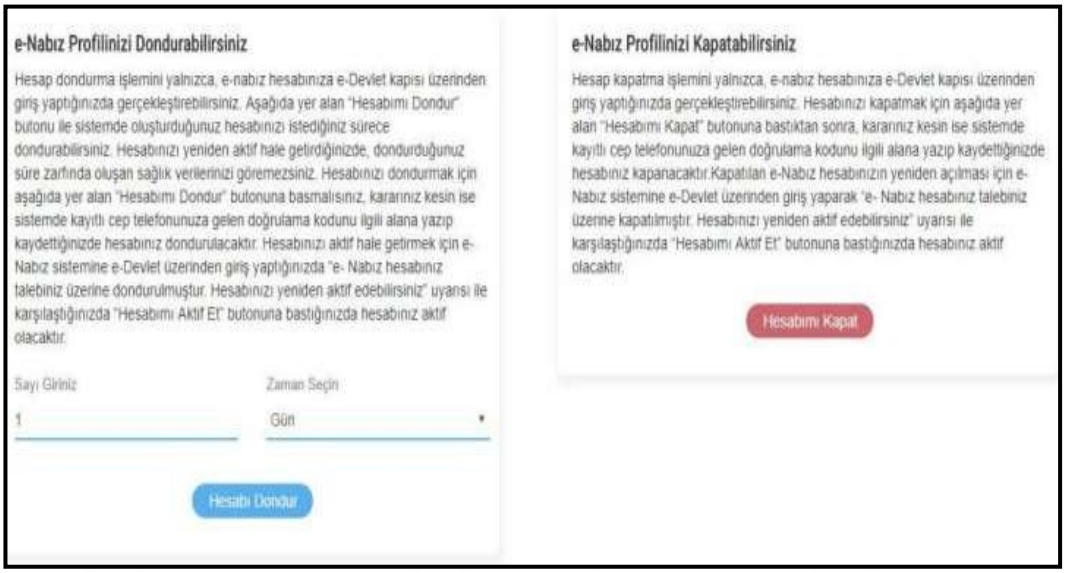
2016 yılında yayımlanan KVKK'dan sonraki süreçten günümüze hassas veri olarak tabir edilen sağlık verileri herhangi bir onam alınmaksızın e-nabız sistemine gönderilmektedir.



Şekil 2.2: E-Nabız Gizlilik ve Görünürlük Ayarları

E- nabız sistem entegrasyonu yapıldıktan sonra hekimler hastalara ait e-nabız kayıtlarına ulaşabilmektedir. Örneğin; kişi karın ağrısı şikayetiyle başvurduğu hekim, HBYS sistemi aracılığıyla e-nabız'a bağlanabilmekte ve hastanın geçmişe dönüş tüm kayıtlarına erişebilmektedir. Sistem multidisipliner bakım ihtiyaçları düşünülerek bu hastanın başvuru yapmadığı hekimlerde erişim sağlama imkânı bulunmaktadır.

Ancak bu durum her ne kadar ihtiyaçlar düşünülerek hazırlanmış olsa da farklı amaçlar ile kullanıma da açıktır. Bu sebepten dolayı Sağlık Bakanlığı'nın yaptığı güncelleme ile e-nabız sisteminde paylaşım ayarlarının düzenlenebilmesine izin vermiştir. Kişiler kendi profillerine ait kısımdan aşağıda yer alan alanı güncelleyip e-nabız verilerine kendi bilgisi dışında yapılan erişimi kısıtlayabilmektedir.



Şekil 2.3: E- Nabız hesabı Dondurma ve Kapatma

e-Nabız hesabınızı kişinin istediği süre boyunca dondurabilir veya kapatabilir. Hesabın dondurulduğu süre içerisinde ziyaret etmiş olduğunuz sağlık tesisi bilgileri ve detayları e-Nabız sistemine yansımamaktadır (URL-23). Sağlık Bakanlığı e-nabız gibi hasta bilgilerinin kaydedildiği uygulamanın dışında kendisine bağlı ya da denetiminde bulunduğu (Olca & Özgü, 2014) sadece İstanbul'da hizmet veren sağlık kurumlarından "Gebliz" adı verilen online sistem ile gebe olan kişilerin bilgileri sisteme işlenmekte ve kayıtlı bulundukları Aile Sağlığı Merkezleri tarafından takip edilmektedir. E-nabız sistemine tüm sağlık verilerinin kaydedilmesine rağmen ayrı bir gebe takip sisteminin oluşturulması verilerin farklı bir platformda paylaşılması açısından risk taşımaktadır. Gebliz, "İstanbul için Sağlık Bakanlığı'nın önerdiği değil, İstanbul Sağlık Müdürlüğü'nün uygulanmasını istediği bir sistemdir" (Kalelioğlu, 2016). Sistem, gebe, lohusa, çocukların ve bebeklerin İstanbul'da bir sağlık kuruluşuna başvurdukları zaman çok basit bir veri tabanına kaydedilmesi şeklinde ilerlemektedir. Basit olarak nitelendirilmesinin sebebi, sadece o kişinin bebek, çocuk, gebe ve lohusa olduğunu o sisteme kaydediyor. Birkaç tane kritere bakmasını sağlıyor. Bunun dışında hiçbir veriye bakılmamaktadır (Çeçen, 2016, 131). 'Aşınet', '15-49 Yaş Kadın İzlem', 'Kalıtsal Kan Hastalıkları Bildirim Sistemi', 'Acil Ünitesi İntihar Girişimi Sistemi' ve 'MORBİD (Obez Hasta Bilgi Formu)' gibi formlar ile hastaların sağlık verilerine ek olarak kişisel bilgileri de toplayıp aktif olarak işlemeye devam

etmektedir (Ekinci, 2018). Verilerin miktarı ve paylaşıldığı platformlar artarken, veriye erişim imkânı da sürece dahil olan birkaç uzmanlık kolları tarafından erişimi kolay bir şekilde gerçekleşmektedir.

Sadece SGK kapsamında değil Özel Sağlık Sigortacılığı alanında da KVKK dahilinde veri paylaşımı, işlenmesi ve aktarımı yapılmaktadır. Bu alanda SGK sistemine nazaran hastadan Açık Rıza Onamı alınması ve hastanın bilgilendirilmesinin daha ön planda olduğunu kurumların kendi adına düzenlemiş olduğu onam formlarından ve onam formu alınmadan işlemlerin başlatılmamasından anlaşılmaktadır. Onam alınacak bu formlar "6698 sayılı Kişisel Verilerin Korunması Kanununun 22. maddesinin birinci fıkrasının (e) ve (g) bentlerine dayanılarak" hazırlanan tebliğe göre hazırlanmış olmalıdır. Aydınlatılmış Onam ve Açık Rıza Onam formları bu tebliğe uygun olarak hazırlanmalıdır.

Yayınlanan tebliğde dikkat edilmesi gereken birçok noktaya değinilmiştir. Genel itibariyle maddelerin birbirinin ayrılmaz parçası halinde olan Tebliğ'in önemli noktalarından biri 6698 Sayılı Kanun'un 10. maddesine göre; kişisel verilerin elde edilmesi sırasında veri sorumluları veya yetkilendirdiği kişilerce, ilgili kişilerin bilgilendirilmesi gerektiğidir. Veri sorumluları bu yükümlülük yerine getirilirken, yapılacak bilgilendirmenin asgari olarak aşağıdaki konuları içermesi gerekmektedir:

a) Veri sorumlusunun ve varsa temsilcisinin kimliği,
b) Kişisel verilerin hangi amaçla işleneceği,
c) Kişisel verilerin kimlere ve hangi amaçla aktarılabileceği,
ç) Kişisel veri toplamanın yöntemi ve hukuki sebebi,
d) İlgili kişinin Kanunun 11 inci maddesinde sayılan diğer hakları (Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, 2019)

Genel anlamda bakıldığında birçok Özel Sağlık Sigorta şirketlerine ait onamlarda bu bilgilere yer verilmektedir. Ancak hazırlanan onam formları içerik anlamında kurumdan kuruma farklılık göstermektedir. Tebliğin 5. Maddesinin 'f' bendinde "Kişisel veri işleme faaliyetinin açık rıza şartına dayalı olarak gerçekleştirilmesi halinde, aydınlatma yükümlülüğü ve açık rızanın alınması işlemlerinin ayrı ayrı

yerine getirilmesi gerekmektedir" (Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi, 2019), ifadesine rağmen sigorta şirketleri Aydınlatma Onamı ve Açık Rıza Beyanı aynı form üzerinden almaktadır.

Özel sağlık sigorta poliçeleri ayaktan ve yatarak olmak üzere iki gruba ayrılmaktadır. Yatarak poliçe kapsamındaki tedavi sürecinde ön onay ve rakam onayı alınarak faturalandırma yapılmaktadır. Kurumlar, hastanelerin tedavi için başvuru yaptıkları ön onay aşamasında yapılacak işleme ait muayene formunun yanı sıra hastanın tanı koyma sürecinde yapılan tetkikleri ve e-devlet kayıtlarını isteyebilmektedir. Bunlara ek olarak hastayı tüm kurumlardan araştırabilmektedir. Özel sigortalarının en genel istisnalarından biri sigortalı olmadan önce var olan rahatsızlıkların kapsanmamasıdır. Bu sebepten dolayı poliçe satın alınırken hastadan geçmişine ait alınan hastalık beyanına istinaden araştırma yapılabilmektedir. Hastane ve Özel sağlık sigortası arasında gerçekleşecek süreç poliçe sahibine bilgilendirilerek paylaşılacak bilgiler konusunda aydınlatılma yapılmalı ve yazılı rıza onamı alınmalıdır. Onay alınmadan bilgi paylaşımının yapılması KVKK'ya aykırılık teşkil etmektedir.

Günümüzde birçok sağlık ve sağlık sigortacılığı işlemleri online platformlardan yapılabilmektedir. Bu platformlar kişiye özel hesaplar açılarak kullanılmakta ve kişisel işlemlerin yapılması sebebiyle üyelik gerektirmektedir. KVKK çıktıktan sonra hem sağlık ve sigortacılık hem de diğer sektörlerde bu tarz uygulamalara üye olunma esnasında "KVKK aydınlatma metnini okudum, kabul ediyorum." ifadesini onaylamadan üyelik kabul edilmemektedir.

Açık rızanın özgür irade ile açıklanması gerekmektedir. Bu sebepten dolayı, ilgili kişinin açık rızasının alınması, bir ürün veya hizmetin sunulmasının ya da ürün veya hizmetten yararlandırılmasının ön şartı olarak ileri sürülmemelidir. Örnek olarak; bir hizmetten yararlanılması konusunda üyelik şartı arandığı durumlarda, üye olması gereken kişinin, kişisel verilerine erişim onayının alınması ve işlenmesinin üyelik sözleşmesinin kurulması için zorunluluk olarak istenmesi hukuka aykırı olacaktır. Çünkü bu şekilde alınan açık rıza özgür irade ve ölçülülük ilkesine aykırı olmaktadır (Açık Rıza Revize Kılavuzu, 2019).

2.7. Bilgi Sistemleri Açısından KVKK

2.7.1. Çerez Kullanımı

Çerezler, online ziyaret edilen web siteleri tarafından tarayıcılara gönderilen küçük bir metin parçasıdır. Bilgisayarlarda, telefonlarda ve diğer cihazlarda kişiyi tanımlanabilir kılan bilgileri ve siteyi kullanırken yapılan hareketleri web sitesini yeniden ziyaret edilmesi durumunda bilgilerin hatırlamasına yardımcı olur. Yani bir sonraki ziyarette kolaylık sağlaması amacıyla daha kullanışlı hale getirmesini sağlamaktadır. Çerezler pek çok amaçla kullanılır. Tarayıcıların başlıca çerez kullanma sebepleri aşağıda yer almaktadır (URL-13);

- **Kişisel Tercih Çerezleri:** Bu çerezler web sitelerinin çalışma veya görüntülenme biçimini değiştiren bilgileri hatırlamasını sağlar. Örneğin, bir web sitesi bulunduğunuz bölgeyi hatırlayarak o bölgeyle ilgili hava durumu raporları veya trafik haberleri sağlayabilir. Bu çerezler aynı zamanda web sayfalarının metin boyutunu, yazı tipini ve kişiselleştirebileceğiniz diğer unsurlarını değiştirmede size yardımcı olabilir. Tercih ettiğiniz dil (ör. Türkçe), sayfa başına kaç tane arama sonucu görüntülenmesini istediğiniz (ör. 10 veya 20) ve tarayıcının Güvenli Arama filtresinin açık olmasını isteyip istemediğiniz gibi diğer bilgileri hatırlamak için kullandığı benzersiz bir kimlik içerebilir.

- **Reklam Çerezleri:** Reklamları kullanıcılar için daha çekici, reklam verenler içinse daha değerli hale getirmek için de çerezler kullanılır. Çerezlerin yaygın kullanım örneklerinden bazıları reklamları bir kullanıcı için alakalı olan şeylere göre seçme, kampanya performansı raporunu iyileştirme ve kullanıcının zaten görmüş olduğu reklamların görünmesini engelleme amaçlıdır. Örneğin kullanıcının daha önce arama motorunda aradığı hastane adının, girdiği farklı sitelerde önüne reklam olarak düşmesi verilebilir.

- **Oturum Durumu:** Web siteleri genellikle kullanıcıların web sitelerinde neler yaptığına ilişkin bilgiler toplamaktadır. Bu bilgiler, "kullanıcıların en sık ziyaret ettiği sayfaları ve belirli sayfalardan hata iletileri alıp almadığını" içerebilir. Bu çerezler, aynı zamanda tıklama başına ödeme ve satış ortağı reklamlarının verimini anonim olarak ölçmek için de kullanılabilir.

- **Analitik Çerezler:** Ziyaretçilerin web sitelerinde ve uygulamalarında neler yaptığını web sitesi ve uygulama sahiplerinin anlamasına yardımcı olan ücretsiz analiz aracıdır. Bu araç, ziyaretçilerin kimliklerini tespit etmeden bilgi toplamak ve site kullanım istatistiklerini sunucuya bildirmek için kullanılan çerezlerdir. Uygulamanın kaç kere açıldığı, hangi saatlerde kullanıldığı, uygulama içerisinde en çok kullanılan bölümlerin neler olduğu gibi bilgilerdir.

- **İşlemler:** İşlem çerezleri, web sitesinin çalışmasına ve ziyaretçilerin Web sayfalarında gezinmek ya da web sitesinin güvenli alanlarına erişmek gibi siteden bekledikleri hizmetlerin sağlanmasına yardımcı olur. Bu çerezler olmadan, web sitesi düzgün çalışamamaktadır.

- **Güvenlik:** Kullanıcıların kimliğini doğrulamak, giriş kimlik bilgilerini kullanarak sahtekarlık yapılmasını önlemek ve kullanıcı verilerini yetkisiz taraflara karşı korumak için güvenlik çerezleri kullanılır. Örneğin, bir kullanıcının Google hesap kimliğine ve en son oturum açtığı zamana ait dijital imzalı ve şifreli kayıtları içeren çerezler kullanılır. Kullanıcıların web sayfalarında doldurduğu form içeriklerini çalma teşebbüsleri gibi pek çok türden saldırıyı önlenmesine olanak tanımaktadır.

Çerezler virüs değildir ve yazılım olarak düz metin biçimi formatıyla kullanılır. Bunlar derlenmiş kod parçaları değildir bu yüzden çalıştırılamazlar veya kendi başlarına çalışamazlar. Buna göre, kendilerini kopyalayamazlar ve tekrar yürütmek ve çoğaltmak için diğer ağlara yayılmazlar. Bu işlevleri yerine getiremedikleri için standart virüs tanımının dışında kalırlar. Çerezler virüs değildir ancak kötü amaçlı amaçlar için kullanılabilir. Kullanıcının tarama tercihleri ve geçmişi hakkında, siteler de gezinirken bilgi depoladıkları için, çerezler bir casus yazılım biçimi olarak kullanılabilir. Birçok casus yazılım önleme programı bu sorunun farkındadır ve standart virüs ve / veya casus yazılım taramalarından sonra çerezleri rutin olarak silerler.

Web sitelerinin çoğunda çerez kullanımı kaçınılmazdır. Çerezleri devre dışı bırakmak internet sitesinin kullanımını güçleştirir. En basit örnekle dil ayarları bile çerez kullanımı gerektirmektedir. Bu durumda önemli olan tarayıcıların çerez ayarları bölümünden güvenli olarak çerez kullanımını yönetmektir (URL-14).

2.7.2. Kişisel Verilerin Korunması Hukukunda Çerez Kullanımı

AB hukukunda çerez kullanımı, 2018'de yürürlüğe giren General Data Protection Regulation (GDPR) ve 2002'den beri yürürlükte bulunan e-Gizlilik Direktifi ile düzenlenmektedir.

Her iki düzenlemenin içeriğine baktığımızda rıza gereksinimi haricinde GDPR'da yer alan tüm yükümlülüklerin (örneğin bilgilendirme yapılması), çerez kullanımı kapsamında gerçekleştirilen kişisel veri işleme faaliyetleri için de geçerli olduğunu görmekteyiz. ePrivacy Direktifi, GDPR'dan farklı olarak ayrıca kişisel veri niteliği taşımayan veriler için de uygulama alanı buluyor. Direktife göre internete erişimde kullanılan cihazlarda depolanan verilerin işlenmesi, GDPR'da tanımlandığı şekilde rıza alınmasına bağlıdır.

GDPR'ın getirdiği en önemli yenilik "açık rıza" ilkesidir. Diğer bir ifadeyle kullanıcılara seçim hakkı vermeden, varsayılan olarak kabul edilen seçenekler sunulamaz. Örnek olarak "Bu siteyi kullanmakla birlikte çerez kullanımına izin verirsiniz" ifadesi seçim hakkı vermemesi sebebiyle irade beyanına dayanmaktadır. GDPR, kullanıcıya seçim hakkı verilmemesi sebebiyle bu yaklaşımı kabul etmemektedir. Ancak Türk Hukukunda, özellikle "çerez politikası" için detaylı bir düzenleme bulunmaması sebebiyle 6698 sayılı kanun kapsamında yapılan bildirim ve aydınlatmalar da yeterli olarak kabul edilmektedir (URL-5).

Geçtiğimiz 2020 Şubat ayında Amazon.com.tr internet sitesine yapılan üyelik sırasında; "reklam, kampanya veya promosyon amacıyla elektronik ticari ileti" gönderebilmek için açık rıza alınmadığı, açık rıza dışında bir işleme nedeninin varlığına ilişkin açıklama yapılmadığı görülmüştür. Ayrıca amazon.com.tr "Gizlilik Bildirimi" sayfasının "Amazon Kişisel Bilgilerinizi Paylaşıyor mu?" kısmının "Kişisel Bilgilerin Türkiye Dışına Aktarılması" alt başlığı altında "Kişisel bilgilerinizi saklamak ve işbu Gizlilik Bildirimi'nde açıklanan amaçlar çerçevesinde işlemek için Avrupa Birliği'ne ve Avrupa Birliği'nden Amerika Birleşik Devletleri'ne aktarabiliriz." şeklindeki ifadeden kişisel verilerin yurt dışına aktarıldığının anlaşılmıştır. Bu durum sonrasında hukuki olarak; kişisel verilerin yurt dışına aktarılması için açık rıza alınmaması sebebiyle KVKK'ya aykırı hareket etmesi sebebiyle mahkeme tazminat ödemesine karar vermiştir (URL-19).

Sağlık sektöründe yer alan her kurumun pazarlama ve tanıtım faaliyetlerini sürdürebilmesi, geniş kitlelere ulaşabilmesi ve kitlelere sağlıkla ilgili konularda bilgilendirme yapabilmesi için web sitesi ve mobil uygulamaları bulunmaktadır. Kullanıcıların kurum ile iletişim kurması için iletişim formu doldurulup bu forma; isim soyisim, iletişim numarası, bilgi alınmak istenen branş veya konu gibi bilgiler istenebilmektedir. Ayrıca kurumların internet sayfasında veya mobil uygulamalarından hassas veri olarak belirlenen tetkik sonuçlarına ulaşılabilmektedir. Bu sebepten dolayı kullanılan internet sitelerinde ve mobil uygulamalarda mutlaka "Aydınlatılmış Onam Formu" ve "Açık Rıza Onamı" nın alındığına dikkat edilmelidir.

2.7.3. Mobil Sağlık Uygulamaları Açısından KVKK

Avrupa İnsan Hakları Mahkemesi açıkladığı bir kararlarından birinde; sağlık verilerinin korunmamasının hastaların tanı ve tedaviden kaçınmasına sebep olabileceğini belirtmiştir. Veri güvenliğinin güvenli ve güçlü bir sistemle sağlanması sağlık bilişim teknolojilerinin beklentileri gerçekleştirebilmesi için oldukça önemlidir. Bu husus, mobil sağlık uygulamaları üzerinden örneklendirilebilir. "Mobil Sağlık kapsamında geliştirilen uygulamalar gelecekte etkin ve erişilebilir sağlık hizmeti sunumuna önemli bir katkı sağlayacağı düşünülmektedir. Bu uygulamalar, hekime ve sağlık kuruluşuna ulaşamayan kişilere bu olanağı sunabileceği ve damgalanma endişesi ile sağlık hizmeti almaktan çekinen hastalara yardımcı olabilir" (EC, 2016) Ayrıca salgın hastalıklar gibi çeşitli sebepler ile sağlık kuruluşlarına gitmekten çekinen hastalar içinde ihtiyaçlar dahilinde kullanabileceği bir uygulamadır.

2.7.4. Bilgi Yönetim Sistemi Açısından KVKK

Bilgi yönetim sistemi, bireysel ve organizasyonel bilginin; "tanımlanması, oluşturulması, kullanımı ve paylaşımına imkân veren insanları, süreçleri, faaliyetleri ve teknolojiyi kapsar ve organizasyonel hedeflere ulaşmak için; bilginin yaratılma, dağıtılma ve kullanım yönetimini" kapsayan bir süreçtir. Bilginin gücünün ortaya çıkması için; yaratıcı uygulamaları, tutumları, sistemleri ve prosedürleri uygulamak gereklidir (Lehaney, Clarke, Coakes & Jack, 2004). Sonuç olarak bilgi yönetimi "organizasyonel hedeflere ulaşmak üzere, en iyi uygulamaları gerçekleştirme, en doğru karar kararları verme gibi organizasyonun gerçekleştirdiği tüm faaliyetlerde

bilgiyi gereken zamanda ve yerde kullanıma sunan, bilgi tanımlama, yaratma, paylaşma, depolama ve kullanma faaliyetlerini organize eden bir süreç" şeklinde tanımlanabilir (Altındiş, 2010). Bilgi yönetimi uygulamalarını gerçekleştirmek için karar destek sistemlerine, hastaların tanı ve tedavisindeki hataların azaltılarak hasta güvenliğini artırmak amacıyla sağlık hizmeti veren kurumlar temel bilgi faaliyetlerine gereksinim duymaktadır (Hirakis & Karakounos, 2008). Ancak sağlık profesyonellerinin isteği, sadece bilgiye kolayca ulaşmak değil aynı zamanda karar verme sürecini desteklemek için güncel ve mevcut bilginin klinik iş akışlarına kesintisiz olarak dahil edilmesini talep etmektedirler. Aynı zamanda hastalar da kendi aldıkları hizmet için süreci anlamaya yardım edebilecek bir haritalarını öğrenmek istemektedirler. Sağlık hizmetleri bilgisi; sadece bir kaynak değil, aynı zamanda ve daha çok bir hizmettir (Abidi, 2008).

Dijital bilgi depolamasının, ESK aracılığı ile oldukça fazla yapıldığı sigorta şirketlerinde birçok bilgi güvenliği ihlâlleri yaşanmaktadır. Bu ihlâllerin aşılması için teknolojik gelişmelerin takip edilerek sistem iyileştirmelerinin yapılması, yönetim ilkelerinde bilgi güvenliğinin önceliklendirilmesi ve çalışanlarda bilgi güvenliği bilincinin eğitimler ile oluşturulması gerekmektedir. Sigorta şirketlerinde meydana gelen bilgi güvenliği ihlâllerine aşağıdaki örnekler verilebilir (Altındiş, 2010).

- Sistem güvenliğinin yetersizliği sebebiyle sistem şifrelerinin kırılması ve sisteme izinsiz erişim sağlanması.
- Her çalışana özel verilen sistem kullanıcı adı ve şifrelerin başka personeller ile paylaşılması.
- Bütünleşmiş provizyon sisteminin oluşturulması amacıyla aracı sigorta şirketleri ile Medula şifrelerinin paylaşılması.
- Sigorta şirketleri arası çalışanların transferleri sonucu hasta kaydı ve sistem şifrelerinin başka şirketler ile paylaşılması (Kitapcı, 2019).
- Sigorta şirketlerinde elektronik sağlık kayıtlarının yaygın olarak kullanımı ve çok çeşitli personelin çalışma ortamında etkileşim içerisinde olması, bilginin gizliliği ve güvenliğinin sağlık sigortası sektöründe hassasiyet gerektiren bir konu haline gelmesine neden olmaktadır (Khan & Hoque, 2016).

- Hastanelerde sigorta yetkililerinin, hastanede sigorta süreçlerinden sorumlu personellerinin birlikte çalıştıkları ortamların oluşması sonucunda hasta bilgilerinin ve sözleşme detaylarının birbirleri ile paylaşılması ve bu bilgilerin şirketlerin lehine kullanılması (Altındiş, 2010).
- E-Nabız sistemine hekimlerin hastanede kullanılan programlar aracılığıyla kolaylıkla ulaşabiliyor olması.
- Özel Sağlık Sigortalarının provizyon aşamasında istenilen evrakların hastane çalışanı tarafından açık rıza bildirim formu alınmadan veya sorgulanmadan hasta kayıtlarının sigorta şirketleri ile paylaşılması.

Sonuç olarak, birçok sektörde olduğu gibi özel sağlık sigortası şirketlerinde de dijital çağa geçilmesiyle birlikte hastalara (sigortalılara) ait bilgiler ve kuruma ait bilgiler elektronik sistem üzerinden yönetilmektedir. Sağlık Sigortası şirketlerinde bilgi sistemlerinin kullanılmasının yaygınlaşması sonucu bilgi güvenliği ve bilgi ihlâlleri kavramları önem kazanmıştır. Bilginin gizliliğinin ve güvenliğinin sağlanması amacıyla Sigortacılık Kanunu, Özel Sağlık Sigortaları Yönetmeliği ve KVKK altında hastaya ait bilgilerin saklı olarak tutulması zorunlu tutulmaktadır. Özel sağlık sigortası şirketlerinde bilgi güvenliğinin sağlanması için ilgili kanunlar haricinde teknolojik ve insan faktörlü bazı önlemler alınmaktadır (Kitapcı, 2019).

Bilgi sistemleri güvenliğinde hatanın önlenebileceği kısım kişi kaynaklı yapılan hatalardır. Diğer ve önlenmesi güç kısım ise siber ihlallerdir. Bu sebepten dolayı bilgi güvenliği bilincinin oluşturulması için çalışanlara bu konuda belirli aralıklarla eğitimler verilmesi, uygulanabilir şirket politikalarının oluşturulması ve uygulanabilirliğinin kontrol edilmesi gibi çalışmalar büyük önem taşımaktadır.

Bilgi güvenliği ihlâllerinin teknolojik açıdan önlenebilmesi için, bilgi sistemleri yazılımlarının donanımlı olarak oluşturulması, anti virüs programları ile desteklenmesi ve kullanıcı hesaplarının kişiye özel şifreleme ile korunması gibi sistemsel tedbirlerin alınması gerekmektedir. Ayrıca çalışanlar tarafından BYS üzerinden bilgiye erişim yetkilerinin ve silme, kopyalama, değiştirme vb. işlem yetkilerinin aralıklar ile kontrol edilerek erişim yetkilendirmelerinin doğru yapılması ve tüm şirket çalışanlarının sorumluluklarının belirlenmesi de kontrol edilebilirlik ve sürekli gelişim anlamında da farkındalık sağlayacak uygulamalardır (Kitapcı, 2019).

2.8. Pandemi Döneminde Sağlık Sigortacılığı ve Mahremiyet Uygulamaları

2.8.1. Pandemi Sürecinde Sağlık Sigortacılığı Uygulamaları

Sosyal Güvenlik Kurumu Sağlık Uygulama Tebliğinde "Acil Hal" tanımı düzenlenmiş olup mevcut acil hal tanımına "pandemi süresince pandemi olgularına yönelik tanı ve tedaviler" ifadesi eklenmiştir. İlgili değişikliğin yürürlük tarihi 09.04.2020 olup bu tarih öncesi başvuruları kapsamamaktadır. Değişiklik Sonrası İlgili Madde:

"Acil hal; ani gelişen hastalık, kaza, yaralanma ve benzeri durumlarda olayın meydana gelmesini takip eden ilk 24 saat içinde tıbbi müdahale gerektiren durumlar ile ivedilikle tıbbi müdahale yapılmadığı veya başka bir sağlık kuruluşuna nakli halinde hayatın ve/veya sağlık bütünlüğünün kaybedilme riskinin doğacağı kabul edilen durumlar ile pandemi süresince pandemi olgularına yönelik tanı ve tedavileri kapsamaktadır. Bu nedenle sağlanan sağlık hizmetleri acil sağlık hizmeti olarak kabul edilir" (T.C. Resmî Gazete, 2020)

İlave ücret alınmayacak sağlık hizmetlerine "Pandemi süresince pandemi olgularının tanı ve tedavileri" de eklendi. İlgili değişikliğin yürürlük tarihi 09.04.2020 olup bu tarih öncesi başvuruları kapsamamaktadır (T.C. Resmî Gazete, 2020).

SGK anlaşması olamayan hastaneler özellikli bir uygulama ile Covid - 19 tedavisi için SGK'ya faturalandırma yapmıştır.

Özel Sigorta sektöründe yaygın olarak kullanılan "İstisna" terimi sağlık sigortacılığında da oldukça sık kullanılmaktadır. Poliçenin genel veya özel şartlarında belirtilen ve bütün sigortalılar için poliçe kapsamı dışında kalan durumlara istisna adı verilmektedir. Özel Sağlık Sigortacılığında "Salgın Hastalıklar" şimdiye kadar istisnalar listesinde yer almakta ve tedavisi özel sigorta kurumları tarafından ödenmemekteydi.

Mart 2019 yılında ortaya çıkan Covid-19 salgınında kurumlar şimdiye kadar uygulanan politikanın aksi bir politika izlemiştir. Sigorta sektörünün sigortalılarının her zaman yanında olduğunu belirten Türkiye Sigorta Birliği; "Mevcut durumda sigorta şirketleri, sağlık kurumlarına başvuran tüm sigortalılarının Covid-19 tanısı konulana kadar yapılmış tüm tetkik giderlerini ve test sonucu belirlenene kadar süren tedavi giderlerini üstlenmiştir. Covid-19 teşhisi pozitif olarak konduktan sonra oluşan tedavi giderleri

ise poliçe teminat kapsamına bağlı olarak ödenmektedir" açıklamasıyla Covid-19 tanısı alan hastaların tedavilerinin özel sağlık sigortası tarafından karşılanacağını bildirmiştir (URL-15).

Özel Sağlık Sigortası olan hastalar normal süreçte tedavilerini aldıktan sonra kurumlarına kesilen ve kişisel verilerinin de yer aldığı fatura eklerine imza atması gereklidir. Özel sigortalar faturası kesilen ancak fatura eki olarak gönderilen evraklarda hasta imzası bulunmadığı durumlarda sağlık hizmeti alınan sağlık kuruluşuna ödeme yapmama hakkına sahiptir. Pandemi sürecine kadar bu şekilde işleyen süreç sonrası TSB'nin açıklamasına istinaden bu süreçle ilgili olarak bazı yeni uygulamalara geçilmiştir. Virüsün yayılmasını önlemek adına kurumlar Covid 19 tanısı alarak tedavi gören Özel Sağlık Sigortalı hastaların fatura eklerine hasta imzası alınmadan da ödeme yapılacağını bildirmiştir. Böylece hem faturalandırmayı yapan personel ve buna bağlı olarak kurumda çalışan diğer kişilere, hem de sigorta şirketindeki çalışanlara bulaş riskinin azaltılmıştır.

2.8.2. Pandemi Sürecinde Mobil Uygulama Kullanımı

2020 Mart ayında ortaya çıkan salgın hastalık Covid-19 virüsünün yayılmasını engellemek ve etkilerini hafifletmek amacıyla tüm Dünya'da ve Ülkemiz 'de gerekli adımları atmakta ve çeşitli önlemler alınması suretiyle mücadele edilmektedir. Bu önlemlerin alındığı çoğu durumda özel nitelikli kişisel verilerdahil olmak üzere "TC kimlik no, ad, adres, işyeri, seyahat bilgileri gibi" pek çok kişisel verinin işlenmesi kaçınılmaz olmuştur. Kişilerin evlerinde izole kalması gerekmiş, işe, okula, alışveriş merkezlerine ve sosyal çevre ile iletişimin kısıtlanması sebebiyle kişiler dış dünya ile olan bağlarını mobil uygulamalar ile kurmuştur. İnternet üzerinden çeşitli programlar ile eğitim, konser, talk Show, konser, iş toplantısı, alışveriş, sosyal medya gibi birçok aktiviteyle hem günlük hayatlarındaki rutinlerin uygulanması sağlanmış hem de dünya genelindeki gelişmeler takip edilebilmiştir. Ayrıca geliştirilen mobil uygulamalar ile Covid-19 salgının önüne geçilebilmesi için önlemler alınmaya çalışılmıştır.

Salgını kontrol altına almak amacıyla Sağlık Bakanlığının HES (Hayat Eve Sığar) adı verilen uygulamadan alacakları kod ile Kontrollü Sosyal Hayat kapsamında, ulaşım ya da ziyaret gibi işlemlerde kurumlarla ve kişilerle, herhangi bir risk taşıyıp taşımadığın güvenli şekilde paylaşılması hedeflenmiştir. Paylaşılan HES kodları uygulama

üzerinden ya da kurumlara sağlanan servisler aracılığı ile sorgulanabilmektedir. Bu kod sadece kişilerin kullanacağı şehirlerarası toplu ulaşım araçlarında geçireceği süre boyunca karşılaşacağı bulaş riskini azaltmak amacına hizmet etmektedir. Bu sayede Covid-19 ya da temaslı olan vatandaşların toplu ulaşım aracı kullanması engellenmekte ve birlikte seyahat edilen diğer kişilerin sonradan Covid-19 testinin pozitif olması halinde kişinin bilgilendirebilmesi amacıyla kullanılmaktadır.

Uygulama kullanım zorunluluğu açısından kontrol edilebilir olumlu olmasına rağmen her vatandaşa yolculuk için test yapılma zorunluluğu olmaması sebebiyle taşıyıcı olup veya nu hastalığı geçirme aşamasında olan ancak test yaptırmamış kişilerde HES kodunu alıp risksiz grupta seyahat edebilmektedir. Bu durum test yapılan riskli kişilerin veri işleyişine imkân sağlarken test yapılmayan kişilerin kontrol edilebilirliğini zorlaştırmaktadır.

2.8.3. Konum Verisinin Paylaşımı açısından KVKK

Korona virüsünün yayılımını engellemek amacıyla; mobil uygulamalar vb. yöntemlerle; "bu hastalığı taşıyan veya taşıma riski bulunan kişilerle temasa geçenlerin tespit edilmesi, virüsün yayılma haritası çıkartılarak tedavi ve bu kişilere karantina uygulanması, karantinaya alınanların kontrolü, sokağa çıkma yasağının uygulanması, kalabalık yerlerin tespiti ve gerekli önlemlerin alınması" gibi amaçlar için kişilerin sağlık, konum ve iletişim bilgileri işlenmektedir. Salgın hastalık gibi toplumu ilgilendiren durumlarda işlenen verilerin önemi oldukça yüksektir ancak işleme süreci dahilinde verilerin güvenliğinin gözetilmesi gerektiği oldukça önemlidir.

Kullanıcıların konum bilgisinin hassasiyet düzeyi, kullanıcının hareket yönü, konumun kaydedildiği zaman, şebeke hücresinin kimliği gibi bilgiler konum verileri olarak değerlendirilebilmektedir (URL-17). Konum verisi, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelikte; "Kamuya açık elektronik haberleşme hizmeti kullanıcısına ait bir cihazın coğrafi konumunu belirleyen, elektronik haberleşme şebekesinde veya elektronik haberleşme hizmeti aracılığıyla işlenen belirli veri" olarak tanımlanmakta olup, gerçek kişileri belirlenebilir kılan konum verisinin 6698 sayılı Kişisel Verilerin

Korunması Kanunu kapsamında kişisel veri olduğu açıktır (URL-16). Konuyla ilgili olarak; "6698 sayılı Kişisel Verilerin Korunması Kanununun 28 inci maddesinin (1) numaralı fıkrasının (ç) bendinde" şu şekilde açıklanmıştır;

"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 halinde Kanun hükümlerinin uygulanmayacağı" düzenlenmiştir (Resmî Gazete, 2016, 29677).

"Salgın hastalık gibi kamu düzeni ve kamu güvenliğini tehdit eden durumlarda bu tehdidi ortadan kaldırabilmek amacıyla salgın hastalık teşhisi konmuş kişilerin bulaşıcılığının sürdüğü dönemde izolasyonlarının temin edilmesine, genel nüfusun konum verilerinin işlenmesi suretiyle kalabalık alanların tespit edilmesine ve bu kapsamda önlemler geliştirilmesine yönelik olarak yetkili kamu kurum ve kuruluşları tarafından gerçekleştirilecek veri işleme faaliyetleri Kanunun 28 inci maddesinin (1) numaralı fıkrasının (ç) bendi kapsamında değerlendirilmektedir." Bu duruma bağlı olarak Covid-19'un sebep olduğu salgın hastalığın kamu güvenliğini ve düzenini tehdit etmesi sebebiyle hastalığın yayılımını engellemek amacıyla konum verisinin kamu kurum ve kuruluşları tarafından işlenmesinin önünde herhangi bir engel bulunmadığı görülmektedir. "Diğer taraftan kişilerin konum verilerinin sağlık durumlarıyla ilişkilendirilmek suretiyle işlenmesi sürecinde söz konusu verilerin üçüncü kişilerce ele geçirilmesi halinde ilgili kişiler bakımından ciddi zararlar ortaya çıkabileceği dikkate alınarak, ilgili kurum ve kuruluşların kişisel verilerin güvenliğini sağlamaya yönelik gerekli her türlü teknik ve idari tedbirleri almaları ve bu verilerin işlenmesini gerektiren sebeplerin ortadan kalkması halinde söz konusu kişisel verilerin silinmesi veya yok edilmesi unutulmamalıdır" (URL- 14).

Sadece ülkemizde değil dünyada da salgını önlemek adına ülkeler birçok uygulamaya başvurmuştur. Aşağıda yer alan tabloda, ülkeler tarafından geliştirilerek yürürlüğe konulan mobil takip (gps, bluetooth, baz istasyonu vb.) ve fiziksel takip (CCTV kamerası, drone, yüz tanıma teknolojisi olan termal kameralar vb.) uygulamaları ile sansür uygulamaları (salgınla ilgili bilgi kirliliğini önlemeye yönelik sosyal medya ve internet kullanımını kısıtlamak vb.) gösterilmektedir.

Tablo 2.2: Covid-19 ile Mücadele Ülkelerin Başvurduğu Uygulamalar

Sıra	Ülke	Mobil Takip Uygulamaları	Sansür Uygulamaları	Fiziksel Takip Uygulamaları
1	ABD	X		X
2	Almanya	X		
3	Arjantin	X		
4	Avusturya	X		
5	Bahreyn			X
6	Belçika	X		X
7	Birleşik Krallık	X		X
8	Brezilya			X
9	Bulgaristan	X		
10	Ekvator	X		
11	Güney Afrika	X		
12	Güney Kore	X		
13	Hindistan	X		X
14	Hong Kong	X	X	
15	Kamboçya		X	
16	Kenya		X	
17	Mısır		X	
18	Nijerya		X	
19	Pakistan	X		
20	Polonya	X		
21	Rusya	X		X
22	Singapur	X	X	
23	Tayland		X	
24	Tayvan	X		
25	Türkmenistan		X	
26	Uganda		X	
27	Çin	X	X	X
28	İran	X	X	
29	İspanya			X
30	İsrail	X		
31	İsviçre	X		
32	İtalya	X		
33	İzlanda	X		

Covid-19 pandemisine karşı yapılan mücadelede %100 sonuç veren teknik bir önlem yoktur ancak mücadele için ana hedef; "temel insan hak ve özgürlüklerine en ufak müdahale ile en etkin mücadeleyi" sağlayabilmektir. Sağlık Bakanlığı tarafından eleştirilen uygulamaların da tam sonuç vermesinin beklenmesi mümkün değildir. Buna engel olabilecek basit sebeplerden biri de ülkemizde başkası adına

kayıtlı telefon hattı kullanım oranı diğer ülkelere kıyasla oldukça yüksektir, bu da izolasyon kurallarına kimlerin uymadığının tespitini ciddi anlamda zorlaştıran sebepler arasında yer almaktadır (URL-18).

3. GEREÇ VE YÖNTEM

3.1. Araştırmanın Amacı

Bu çalışmanın amacı hastaların kişisel verilerin korunması kanunu ve süreçleri hakkında farkındalıkları ölçülerek hem akademik alanda ilgili konuda daha önce yapılmayan bir çalışmanın oluşmasını sağlamak hem de sağlık hizmeti verilen kuruluşlarda hizmet alan kişilerin KVKK hakkındaki farkındalıklarını istatistiksel olarak tespit etmektir.

3.2. Araştırmanın Sınırlılıkları

Araştırmanın bazı sınırlılıkları vardır. Bunlar aşağıdaki şekildedir; Araştırma bulgu ve sonuçları, araştırmada kullanılan anket formu ile sınırlıdır. Araştırma, İstanbul ilinde özel bir Üniversite Hastanesi'nde ayaktan ve yatan hizmet alan Sağlık Sigortalı hastalara uygulanmıştır. Araştırmada, hastanede hizmet alan hastalara çevrimiçi anket yoluyla uygulanmıştır. Bu araştırmada elde edilen bulgular diğer hastanelerde hizmet alan hastaları genellemez.

3.3. Araştırmanın Evren ve Örneklemi

Araştırma süreci planlanırken ilk olarak araştırma yapılacak kurum belirlenmiştir. Bu kapsamda araştırmanın evreni İstanbul'da hizmet veren özel bir Üniversite Hastanesi'nden hizmet alan hastalardır. Araştırmanın örneklemi belirtilen sağlık kuruluşundan hizmet almış 169 sağlık sigortası mensubudur. Sağlık hizmeti alan ve elektronik posta ile gönderilen çevrimiçi anketi dolduranlar çalışmaya dahil edilmiştir. Araştırma için Etik Kurul Onayı alınmıştır (Ek-1). Çalışmanın yapıldığı kurumdan izin alınmıştır.

3.4. Araştırmanın Materyali ve Tipi

Bu araştırma Eylül 2020 ve Ocak 2021 tarihleri arasında yapılmıştır. Katılımcılardan onam formu alınmıştır (Ek-2). Araştırma online anket uygulaması kullanılarak 5 adet demografik özellikler ve 34 adet farkındalık ölçecek çoktan seçmeli sorular yer almaktadır (Ek-3). Katılımcılardan elde edilen veriler, SPSS 22.0 programında analiz edilmiştir. Analizde frekans ve yüzde dağılımları algı ve tutum farklılaşmasına yol

açan ANOVA, ki-kare ve t testi uygulanmıştır. 169 geçerli anketten oluşan çalışmamızın son sorularında daha önce yurtdışında benzer konularda yazılan makalelerde uygulanmış olan anket sorularının kullanımı için yazarlar ile görüşüp onay alınarak 23 madde 5'li likert şeklinde sorulmuştur. Bu maddelerin içsel geçerliliği Cronbach's Alfa testiyle sınanmıştır. Cronbach's Alpha değeri ".951"dir. Elde edilen bulgular tablo ve grafikler ile açıklanmıştır. Ankette yer alan sorular; 1)Annals of Family Medicine, 2) England University of Leeds, 3) Stevens Institute of Technology, 4) Kristiania University College kurumlarında daha önce KVKK konusunda yapılmış bilimsel çalışmaların yazarlarıyla iletişime geçilerek, anket sorularının kullanımı için onay alınmıştır.

4. BULGULAR

İstanbul'da bir özel Üniversite Hastanesi'nde hizmet alan Sağlık Sigortalı 169 hastaya anket uygulanmıştır. Katılımcıların demografik bilgileri Tablo 4.1'de gösterilmiştir.

Tablo 4.1: Katılımcıların Demografik Bilgileri

		n	%
Yaş	18-24	48	28,4
	25-34	81	47,9
	35-44	23	13,6
	45-54	13	7,7
	55-64	3	1,8
	65-74	1	0,6
Cinsiyet	Kadın	106	62,7
	Erkek	63	37,3
Eğitim	İlkokul	3	1,8
	Ortaokul	7	4,1
	Lise	46	27,2
	Üniversite	93	55
	Yüksek Lisans	18	10,7
	Doktora	2	1,2

Ankete katılan hastaların; "Kişisel sağlık verisini kavramını daha önce duydunuz mu?" sorusuna verilen cevapların %52,1'i daha önce bu kavramı duyduğunu, 47.9'u daha önce bu kavramı duymadığını belirtmiştir.

Ankete katılan hastaların; "Kişisel verilerin kaydedildiği veri tabanını düzenlemek ve özel ve güvenli tutmak için en çok kime güvenirsiniz?" sorusuna verilen yanıtlarda; %28,4 "Hükümet", %27,2 "Hastane", %26,6 "Diğer" cevabı verilirken, 17.8 ile en az orana sahip yanıt "Sigorta Şirketi" olmuştur.

Ankete katılan hastaların; “Farklı sağlık kurumu ziyaretlerinden ve sağlayıcılardan (sigorta şirketinizden veya mobil uygulamalardan) gelen tüm tıbbi bilgilerinizin veri tabanında otomatik olarak saklanmasını doğru buluyor musunuz?” sorusuna verilen yanıtlarda; %62,1 “Evet”, %37,9 “Hayır” olmuştur.

Ankete katılan hastaların; “Kişisel verilerinizin başkalarının erişimine kısıtlanabileceğini biliyor musunuz?” sorusuna verilen yanıtlarda %68,6 “Evet”, 31.4 “Hayır” olmuştur.

Ankete katılan hastaların; “Veri tabanına hangi bilgilerin gireceğini nasıl kısıtlamak isterdiniz?” sorusuna %40 katılımla en yüksek cevap; “Bilgilerim sisteme dahil edilmeden önce her bölümünü onaylamak istiyorum. (bireysel doktor notları ve test sonuçları dahil)” yanıtı olmuştur.

Ankete katılan hastaların; “Bir doktora elektronik tıbbi kaydınızı görüntüleme ve ekleme izni verdikten sonra, bu doktorun kaydınıza ne kadar süre erişmeye devam etmesi gerekir?” sorusuna %47,3 katılımla en yüksek katılımcı yanıtı; “Doktorum izin verdiğim sürece sürekli erişime sahip olabilir.” verilirken, %9,5 ile en düşük yanıt; “Doktorum 1 yıl boyunca sürekli erişime sahip olabilir.” olduğu gözlemlenmiştir.

Ankete katılan hastaların; “Acil bir durum sırasında eğer izin verebilecek durumda değilseniz, kimlerin tıbbi kayıtlarınızı görebilmesi gerektiğini düşünüyorsunuz?” sorusuna %34,3 katılımla en yüksek yanıt; “Tedavimden sorumlu doktorum” iken, %4,1 ile en düşük yanıtın “Acil bir durumda bile hiç kimse benim iznim olmadan tıbbi kayıtma erişemez.” olduğu gözlemlenmiştir.

Ankete katılan hastaların; “KVKK bireylerin kişisel verilerin toplanması ve depolanması konusunda yeni haklar kazandığı anlamına gelir. Bunun hakkında ne düşünüyorsunuz?” sorusuna %50,9 ile en yüksek katılım “Fikrim yok” olurken, %18,9 ile en düşük yanıt, “Haklarımın geliştiğini sanmıyorum.” olmuştur. %30,2 oranındaki kalıtımcı bu kanun ile haklarının geliştiğini düşünmektedir.

Ankete katılan hastaların "KVKK, sizinle ilgili bazı kişisel bilgilerin (şirketlerin topladığı) silinmesini talep etme konusunda daha büyük bir hak vermiştir. Bunun hakkında ne düşünüyorsunuz?" sorusuna %33,1 ile en yüksek yanıt "Fikrim yok" olurken, %8,9 ile en düşük yanıt "Bu hakkımı uyguladım" olmuştur.

Ankete katılan hastaların; "Cep telefonunuza bir uygulama indirdiğinizde veya dizüstü bilgisayarınıza bir program yüklediğinizde, şartlar ve koşullar ile çerezleri onaylamanız gerekir. Bu konudaki tipik tepkiniz nedir?" sorusuna %42,6 ile "Zaman zaman değişir (söz konusu uygulamaya / programa bağlı olarak) yanıtı verilirken, %14,8 ile en düşük yanıt "Uzun süre almasına rağmen metnin tamamını okurum" olmuştur. Yine ankette yer alan diğer çoğunluğa baktığımızda ise; %20,7 ile "Hızlıca tüm metni kaydırıyorum, ancak her şeyi okumuyorum" yanıtı verilirken, %21,9 ile "Metne bakmadan Katılıyorum / Kabul Ediyorum"u tıklıyorum" yanıtı verilmiştir.

Ankete katılan hastaların; "24 Mart 2016'da yürürlüğe giren Kişisel Verileri Koruma Kanunu (KVKK) hakkında daha önceden bir şeyler duydum" maddesine %27,8 ile "Katılıyorum" yanıtını %24,9 ile "Katılmıyorum" yanıtı izlemiştir.

Ankete katılan hastaların; "E- nabız uygulamasını kullanıyorum" maddesine %43,8 oranıyla "Kesinlikle Katılıyorum" yanıtı verilirken, %2,4 ile "Kararsızım" yanıtı alınmıştır.

Ankete katılan hastaların; "E- nabız uygulamasının bilgilerimi koruduğuna inanıyorum." maddesine %29,6 "Katılıyorum" yanıtı verilirken %5,9 ile "Katılmıyorum" yanıtı ile araştırmaya katılanların bu soruda ilgili uygulamada bilgilerinin korunduğunu düşündükleri gözlemlenmiştir.

Ankete katılan hastaların; "E- nabız kullanırken gizlilik sorunları konusunda endişeliyim" maddesine %29,6 "Kesinlikle Katılmıyorum" yanıtı verilirken, %4,1 "Kesinlikle Katılıyorum" yanıtı ile ilgili uygulamanın gizlilik sorunları konusunda endişeli olmadığı şeklinde düşünülebilir.

Ankete katılan hastaların; "E-nabız kullanmayı öğrenmenin benim için zor olacağını düşünüyorum" maddesine %48,5 "Kesinlikle Katılmıyorum" yanıtı verilirken, %7,1 "Kesinlikle Katılıyorum" yanıtı araştırmaya katılanların bu soruda ilgili uygulamayı öğrenmenin kolay olacağını düşündüklerini göstermektedir.

Ankete katılan hastaların; “E- nabız uygulamasının hayatımı kolaylaştırdığını düşünüyorum” maddesine %33,7 “Kesinlikle Katılıyorum” yanıtı verilirken %8,9 “Kararsızım” yanıtı ile katılanların ilgili uygulamanın hayatlarını kolaylaştırdığına katıldıklarını göstermektedir.

Ankete katılan hastaların; “Sağlık kaydımın gizli tutulacağını hissediyorum” maddesine verilen %30,6 “Kararsızım” yanıtı ile araştırmaya katılanların bu konuda genel olarak kararsız olduklarını göstermektedir.

Ankete katılan hastaların; “E- nabız web sitesindeki sorunlar için Sağlık Bakanlığı yardım masasının sorunların çözümünde her zaman yardımcı olduğuna inanıyorum” maddesine %33,7 “Katılıyorum” yanıtını %29,6 ile “Kararsızım” yanıtı izlemiştir. Katılımcıların genel olarak bu konuda katılmakla birlikte kararsızlık oranının yüksek olduğu görülmektedir.

Ankete katılan hastaların; “Mobil sağlık uygulamalarını bir doktora danışmak veya ikinci bir doktor görüşü almak için kullanırım” maddesine %36,1 ile “Katılıyorum” yanıtı verilirken bu yanıtı %20,7 ile “Kararsızım” yanıtı izlemiştir. Katılımcıların bu konuda Katılmak ve kararsızlık arasında kaldığı ancak katılımının ağır bastığı gözlemlenmiştir. Ankete katılan hastaların “Laboratuvar, ilaç ve tetkik sonuçlarımı bir sağlık uzmanıyla elektronik olarak paylaşırken bilgi güvenliğim konusunda endişe etmem.” maddesine %37,3 ile “Katılıyorum” yanıtı verilirken, %20,7 ile “Kararsızım” yanıtı verilmiştir. Katılımcıların kararsızlık ve katılmak arasında kaldığı ancak katılımının ağır bastığı gözlemlenmiştir.

Ankete katılan hastaların; “24 Mart 2016'da yürürlüğe giren Kişisel Verileri Koruma Kanunu (KVKK) hakkında daha önceden bir şeyler duydum” maddesine %27,8 ile “Katılıyorum”, %24,9 ile “Katılmıyorum” yanıtı verilmiştir.

Ankete katılan hastaların “Farklı işletmelerin veri tabanlarında depolanan kişisel bilgilerim üzerinde kontrol sahibi olduğumu düşünürüm” maddesine %32,5 “Katılıyorum” yanıtı verilirken %23,1 ile “Kararsızım” yanıtı verilmiştir. Katılımcıların katılmak ve kararsızlık arasında kaldığı ancak katılımının ağır bastığı gözlemlenmiştir.

Ankete katılan hastaların; “Özel sağlık sigortamın kişisel sağlık verilerimi koruduğuna eminim.” maddesine %29 “Katılıyorum” yanıtı verilirken %24,9 “Kararsızım” yanıtı verilmiştir. Katılımcıların katılmak ve kararsızlık arasında kaldığı ancak katılımının ağır bastığı gözlemlenmiştir. Ayrıca istatistiklerde p değeri

0,05ten küçük olan (0.038) bu soruya verilen cevaplarda gelir grupları yönünden anlamlı bir fark vardır.

Ankete katılan hastaların; “Özel sağlık sigortamın, sağlık kuruluşlarından benim için talep edilen belgeler süreç akışı gereği benden onay alınmadan da hastane tarafından kurumlar ile paylaşılabilir.” Maddesine %26,6 “Kesinlikle Katılmıyorum” yanıtı verilirken %10,7 “Kesinlikle Katılıyorum” yanıtı verilmiştir.

Ankete katılan hastaların; “Poliçe satın alırken poliçedeki tüm maddeleri okurum ve anlamadığım kısımları sigortacıma danışırım.” Maddesine %30,8 “Katılıyorum” yanıtı verilirken %8,3 “Katılmıyorum” yanıtıyla genel olarak katılımcıların yani poliçe satın alırken tüm maddeleri okudukları ve anlamadıkları danıştıkları görülmüştür.

Ankete katılan hastaların; “Kişisel verilerimin bazı durumlarda benden ekstra rıza alınmadan paylaşılabileceğini biliyorum.” maddesine %29,6 “Katılıyorum” yanıtı verilirken bunu izleyen %21,3 ile “Kararsızım” yanıtı olmuştur. Katılımcıların katılım ve kararsızlık arasında kaldığı ancak katılıyorum yanıtının ağır bastığı gözlemlenmiştir.

Ankete katılan hastaların; “Kişisel verilerime sahip olan veri sorumlusundan (hastane, sigorta şirketi); verilerin işlenme amacına uygun olarak işlenip işlenmediğini sorarım.” maddesine %31,4 ile “Katılıyorum” yanıtı verilirken %23,1 “Kararsızım” yanıtı verilmiştir. Katılımcıların katılım ve kararsızlık arasında kaldığı ancak katılıyorum yanıtının ağır bastığı gözlemlenmiştir.

Ankete katılan hastaların; “Eksik/yanlış işlenme durumunda veri sorumlusundan düzeltme hakkı talep ederim.” maddesine %37,3 “Katılıyorum” oranıyla katılımcıların düzeltme hakkı talep ettikleri gözlemlenmiştir.

Ankete katılan hastaların; “Kurumlarda silinmesini istediğim veriler olursa bunlar için başvuru yapabilirim.” maddesine %28,4 oranı ile “katılıyorum” yanıtı verilirken %7,1 “Katılmıyorum” yanıtı verilmiştir. Katılımcıların genel olarak silinmesini istedikleri verilerin yönetimi konusunda hak sahibi olduğu konusunda bilgi sahibi olduğu gözlemlenmiştir.

Ankete katılan hastaların; “Avrupa Birliğinde yayınlanan Kişisel Verilerin Korunması konusundaki yayınlar hakkında bilgi sahibiyim.” maddesine %29,9 “Kararsızım” yanıtı verilirken, bunu izleyen en yüksek katılım %22,5 ile “Kesinlikle Katılmıyorum” olmuştur. Katılımcıların genel olarak Avrupa Birliğinde KVKK konusunda yayınlanan yanınlar hakkında bilgi sahibi olmadığı gözlemlenmiştir.

5. TARTIŞMA VE SONUÇ

Günümüz teknoloji çağında teknolojinin, iletişimin ve erişilebilirliğin bu kadar yaygın olması kişisel veri gizliliğini akademik ve teorik uygulama dışında pratikte ve günlük hayatımızın merkezindedir. Kişisel sağlık verisi gizliliği dolaylı yönden uzun yıllardır koruma altında olduğu gözükse de ülkemizde ve dünya genelinde uygulanmaya başlanan yasalar ile bu alana özel olarak çok yeni bir geçmişe sahiptir. Veri gizliliğini ihlale sokacak bir durumda ise yaptırımları olması sebebiyle kişilerin bu konudaki duyarlılığı artacaktır.

Bu çalışmanın amacı, hastaların kişisel verilerin korunması kanunu ve süreçleri hakkında farkındalıklarını ölçerek sağlık alanında Kişisel Verilerin Korunması Kanunu hakkında hem akademik alana daha önce yapılmayan bir çalışmanın oluşmasını sağlamak hem de sağlık hizmeti verilen kuruluşlarda hizmet alan kişilerin KVKK hakkındaki farkındalıklarını istatistiksel olarak göstermektedir.

Kişisel verilerin sadece sağlıkta değil hayatımızın her alanında; alışverişte, trafikte, mobil oyunlarda, telefonumuzda... Özel bir hastanede hastalara sağlık alanında ve hayatımızın bu kadar merkezinde bulunan ve veri gizliliğinin korunabilmesi amacıyla çıkarılan 6698 Sayılı Kişisel Verilerin Korunması Kanunu kişilerin kanun hakkında net bir bilgiye sahip olmadıkları görülmüştür. Yine ankette yer alan ve sağlık verilerinin paylaşıldığı e-nabız isimli online uygulama hakkında hastaların genel olarak verilerinin korunduğunu ve uygulamayı kolayca kullanabildiklerini düşünmektedirler.

Onur Asan ve arkadaşlarının yaptığı çalışmada yetişkinlerin gençlere göre daha az online sağlık uygulamaları kullandığı görülmüştür. Bunun sebebi olarak gençlerin teknolojiye ile daha yakın olması ve kullanım kolaylıkları gösterilirken yaşı ilerlemiş olan yetişkinler için ise sağlık okur yazarlığının düşük olması, teknolojiyi kullanmaktaki zayıf beceriler ve görme bozukluğu gibi kronik rahatsızlıklar buna örnek verilmiştir.

169 kişilik hasta grubumuza uyguladığımız ankette yaş ve teknoloji kullanımı konusunda belirgin bir farklılık gözlemlenmemiştir. Ayrıca pandemi döneminde

hastaneye gidilemeyen dönemde tıbbi kayıtlarına ulaşma ihtiyacı, HES kodu uygulaması ve aşılama randevusu gibi devletlerin zorunlu tuttuğu uygulamalarda yaş fark etmeksizin online sağlık uygulamaları zorunlu hale getirilmiştir.

"Farklı sağlık kurumu ziyaretlerinden ve sağlayıcılardan (sigorta şirketinizden veya mobil uygulamalardan) gelen tüm tıbbi bilgilerinizin veri tabanında otomatik olarak saklanmasını doğru buluyor musunuz?" sorusuna verilen yanıtlarda; %62,1 "Evet", yanıtıyla katılımcıların büyük çoğunluğunun veri tabanına otomatik kaydı doğru bulduğu gözlemlenmiştir.

"Kişisel verilerinizin başkalarının erişimine kısıtlanabileceğini biliyor musunuz?" sorusuna verilen yanıtlarda %68,6 "Evet" yanıtıyla genel olarak kişilerin verilerini yönetmesi konusunda yetkisi olduğu bilgisine sahip olduğu gözlemlenmiştir. Gelir değişimine göre anlamlı fark gözlemlenmiştir (Pearson Chi-Square p değeri: 0.046). Gelir değeri yüksek kişilerin bu yetkiye sahip olduğunun daha çok farkında olduğu şeklinde yorumlanabilir.

"KVKK bireylerin kişisel verilerin toplanması ve depolanması konusunda yeni haklar kazandığı anlamına gelir. Bunun hakkında ne düşünüyorsunuz?" sorusuna %50,9 ile en yüksek katılım "Fikrim yok" olmuştur. Bu durum katılımcıların büyük bir çoğunluğunun kanun hakkında detay bilgisi olmadığını göstermektedir.

Alaa A. Abd-alrazaq ve arkadaşlarının yaptığı çalışmada online sağlık uygulamaları kullanımında kullanım niyetini belirleyen ve kullanımı arttıran üç konuyu kolay anlaşılabilir düzene sahip uygulamalar, internet erişimi ve gizlilik ve güvenlik endişeleri olarak belirtmiştir. Hasta grubumuza uygulamış olduğumuz ankette uygulanmakta olan e- nabız uygulamasının anlaşılabilir bir düzene sahip olduğu katılımcıların önemli çoğunluğu tarafından düşünüldüğü gözlemlenmiştir. Ayrıca yine Alaa A. Abd- alrazaq ve arkadaşlarının yaptığı çalışmada kullanım niyetini belirleyen üç faktörde cinsiyete göre anlamlı bir farklılık gözlemlenmezken yaptığımız çalışmada kadın katılımcıların bir sağlık uzmanıyla yapacağı veri paylaşımı için erkek katılımcılara göre daha az endişeli olduğu gözlemlenmiştir.

“Kişisel verilerinizin başkalarının erişimine kısıtlanabileceğini biliyor musunuz?” sorusuna verilen yanıtlarda gelir değişimine göre anlamlı fark gözlemlenmiştir. Ankete katılan hastaların; “E- nabız uygulamasını kullanıyorum.” maddesine %43,8 oranıyla “Kesinlikle Katılıyorum” yanıtı ile katılımcıların çoğunluğunun genel olarak ilgili uygulamayı kullandığını göstermektedir.

“Farklı işletmelerin veri tabanlarında depolanan kişisel bilgilerim üzerinde kontrol sahibi olduğumu düşünürüm.” maddesine verilen %32,5 “Katılıyorum” ve %23,1 ile “Kararsızım” yanıtı ile katılımcıların katılmak ve kararsızlık arasında kaldığı ancak katılımının ağır bastığı gözlemlenmiştir.

“E-nabız kullanmayı öğrenmenin benim için zor olacağını düşünüyorum.” maddesine %48,5 “Kesinlikle Katılmıyorum” yanıtı araştırmaya katılanların büyük çoğunluğunun soruda ilgili uygulamayı öğrenmenin kendileri için kolay olacağını düşündüklerini göstermektedir.

“E- nabız uygulamasının hayatımı kolaylaştırdığını düşünüyorum.” maddesine %33,7 “Kesinlikle Katılıyorum” yanıtı ile katılanların genel anlamda ilgili uygulamanın hayatlarını kolaylaştırdığına katıldıklarını göstermektedir.

“Özel sağlık sigortamın, sağlık kuruluşlarından benim için talep edilen belgeler süreç akışı gereği benden onay alınmadan da hastane tarafından kurumlar ile paylaşılabilir.” maddesine %26,6 “Kesinlikle Katılmıyorum” yanıtı verilirken %10,7 “Kesinlikle Katılıyorum” yanıtı verilmiştir. Katılımcıların bu konuda onayı olmadan paylaşım yapılmasını istemediği yorumlanabilir.

Ankete katılan hastaların; “Sağlık sigortalarının provizyon sürecinde beni tüm kurumlardan araştırması beni rahatsız etmez.” maddesine %27,8 “Katılıyorum” yanıtı verilirken %24,9 “Kesinlikle Katılmıyorum” yanıtı verilmiştir. Bu durum katılımcıların genel olarak bu konu hakkında da kararsız oldukları şeklinde yorumlanabilir.

“Özel sağlık sigortamın, sağlık kuruluşlarından benim için talep edilen belgeler süreç akışı gereği benden onay alınmadan da hastane tarafından kurumlar ile paylaşılabilir.” Maddesine %26,6 “Kesinlikle Katılmıyorum” yanıtı verilirken %10,7 “Kesinlikle Katılıyorum” yanıtı verilmiştir. Katılımcıların bu konuda onayı olmadan paylaşım yapılmasını istemediği yorumlanabilir.

“Acil bir durum sırasında eğer izin verebilecek durumda değilseniz, kimlerin tıbbi kayıtlarınızı görebilmesi gerektiğini düşünüyorsunuz?” sorusuna %34,3 ile en yüksek yanıt “Tedavimden sorumlu doktorum” olduğu gözlemlenmiştir. Katılımcıların genel olarak acil durumlarda verilerinin gizli kalmasını tercih etmediği yorumlanabilir.

Wanda Prestus ve Hanne Sorum’un yaptığı çalışmada mobil uygulama kullanımındaki güvenilirliği ölçmek amacıyla sorulan çerez güveliği ile ilgili bilgilendirme metnini anket katılımcılarının büyük bir çoğunluğu okumadan kabul ettiği belirtilmiştir. Yaptığımız anket çalışmasında bahsi geçen soruda katılımcılarımızın büyük bir çoğunluğu okumadan kabul ettiği gözlemlenmiştir. Bilgilendirme metinlerinin uzun ve detaylı olması kullanıcılar açısından pratikliğin zıt versiyonu konumundadır. Kişiler daha pratik ve hayat kolaylaştırıcı uygulamaları kullanırken uzun metinler bu konuda karşıtlık oluşturduğu söylenebilir.

“Kişisel verilerin kaydedildiği veri tabanını düzenlemek ve özel ve güvenli tutmak için en çok kime güvenirsiniz?” sorusuna Rasha Mahmoud ve arkadaşlarının yaptığı çalışmada Hastane ve Hükümet ağırlıklı yanıtı katılımcıların ağırlıklı olarak katıldığı seçenek olurken, özel sektör konusunda endişeleri olduğu gözlemlenmiştir. Yapılan ankette GDPR a olan farkındalık düzeyi orta ve yüksek çıkmış ve sonucun daha düşük farkındalık olması beklenirken bu sonucun kendileri için şaşırtıcı olduğunu belirtmişlerdir. Ardından anketi uyguladıkları büyük bir kesimin kolej mezunu olduğunu belirtip öğrenim durumunun bu oranı yükselttiği belirtilmiştir. Katılımcılarımızın yanıtında da yine Hastane ve Hükümet yanıtı ağırlıklı iken Özel Sağlık Sigorta şirketlerine katılımcıların güvenmekte endişeli olduğu gözlemlenmiştir. Özellikle sağlık ve sağlık sigortacılığı alanında sürekli güncel gelişmelerin olması, yeni uygulamaların kısa sürede uygulamaya alınması gibi aktif bir sürece sahip olan sektörde handikap yaşanan konular, ihlale açık alanlar, bu konunun önemini henüz kavramamış kurumlar, çalışanlar ve hastaların da olduğu hem sahada hem de KVKK mevzuatına aykırı meydana gelen durumlarda uygulanan cezalardan anlaşılmaktadır.

Ayrıca GDPR’ın ülkemizde uygulanan versiyonu KVKK mevzuatı ise bizim uyguladığımız ankette yarıya yakını kişisel sağlık verisi ve KVKK mevzuatı konusunda farkındalığı olmadığı gözlemlenmiştir. Kişisel veri kavramında farkındalık

düzeyi yaptığımız anket çalışmasında daha çok gelire göre anlamlı bir farklılık göstermiştir. Mezuniyet dereceği arttıkça bu konuda olan farkındalık düzeyinin arttığı gözlemlenmiştir.

Kişisel veri kavramının temelini oluşturacak olursak, kişiyi "Ben" yapan tüm bilgiler hassas veya özel nitelikli veri olarak tanımlanmaktadır. Bu verilere ulaşımın ve işlenmesinin bir şekilde kişinin izni dışında yapılması önemli sonuçlar doğurabilir ve kişiyi toplum içerisinde etiketleyip, toplumsal alanda ayrımcılığa uğratabilir ve en sonunda kişiyi sağlık hizmeti almaktan vazgeçirebilir. Bu süreçte başta sağlık çalışanları olmak üzere bu süreç içerisinde yer alan herkese önemli görevler düşmektedir. Gerek kişilerin bu konuda bilinçlendirilmesi ve gerekse bilgi sistemlerinde bu konu için yapılacak iyileştirmeler yasal düzenlemelerle desteklenirse sürece olumlu katkı sağlayacaktır.

"KVKK, sizinle ilgili bazı kişisel bilgilerin (şirketlerin topladığı) silinmesini talep etme konusunda daha büyük bir hak vermiştir. Bunun hakkında ne düşünüyorsunuz?" sorusuna %33,1 ile en yüksek yanıt "Fikrim yok" olarak verilmiştir. Genel olarak bu hak konusunda katılımcıların bilgi sahibi olmadığı görülürken uygulamada da verilmiş bu hak konusunda netleştirilmemiş noktalar bulunmaktadır. Kişilerin unutulma hakkı ve kurumların sır saklama yükümlülüğü sebebiyle olan tıbbi evrakları saklama zorunluluğu konusunda mevzuatta GDPR'da olduğu kadar net bir ayrıma yer verilmemiştir.

Serdar Gülener'in 2012 yılında yaptığı çalışmasında; unutulma hakkının gün geçtikçe üzerinde tartışılan ve gerek ulusal gerekse uluslararası insan hakları belgeleri ile temel bir insan hakkı olarak yeni düzenlemelere konu olması muhtemel bir hak olarak karşımıza çıktığını ancak unutulma hakkı içinin doldurulması noktasında çeşitli pratiklere ve uygulamalara ihtiyaç duyulduğunu belirtmiştir. Bunun temel nedeni olarak kavramın sınırlarının çok net bir biçimde çizilemediğini göstermiştir.

"Sigorta şirketi faturalandırması için imzaladığım evrakların tamamını okumadan imzalamam." maddesine katılımcılar genel olarak evrakları okuduklarını belirtmiş olsa da sahada ve pratikte her hastada aynı dikkatin ve farkındalığın olduğunu söylemek güçtür.

Bu maddede p değeri 0,05'ten düşük olduğu için gruplar arası varyans eşit değildir bu durumda ANOVA testinin alternatifi olan Welch ve Brown Forsythe testlerine bakılmıştır. Welch testinin p değeri 0,000 olduğu için farklı gelir gruplarına sahip bireylerin gelir grubuna göre bu maddeye verdikleri cevaplar değişmektedir. Gruplarda ikili karşılaştırma testi olarak Tamhane testi kullanıldı;

"2500-4999" ile "1000-2499" gelir grupları arasında istatistiki açıdan anlamlı bir fark vardır. İlk grubun ortalaması ikinciden yüksek olduğu için bu grubun evrakları imzalama konusunda daha dikkatli olduğunu söyleyebiliriz.

Tablodaki p değerlerine baktığımızda "2500-4999" ile "5000-9999" gelir grupları arasında istatistiki açıdan anlamlı bir fark vardır. İkinci grubun ortalaması ilk gruptan yüksek olduğu için bu grubun evrakları imzalama konusunda daha dikkatli olduğunu söyleyebiliriz.

Ayrıca sigortaların fatura için imzalanması istediği evrakların içerisinde yer alan "Aydınlatılmış Onam Formu" bulunmaktadır. KVKK gereği veri paylaşım süreçlerinde aktif olarak kullanılması gerekmektedir. Ancak aydınlatılmış onam formunun tek bir formatı bulunmamakta her sigorta şirketinin belirlediği maddelerin yer aldığı bir form olması sebebiyle kapsamının ihtiyacı karşıladığını söylemek güçtür. Özel sigorta şirketlerine ait formların birçoğunda hastanın veri paylaşımına onay vermediğini belirtecek bir alan bulunmamakta olup, KVKK ile ilgili temel bilgilerin açıklanmasından sonra hasta onayının yer aldığı alan bulunmaktadır. Farkındalığı yüksek olmayan sigortalılar onam formunu madde detaylarını okumadan veri gizliliği uygulamalarını kabul ettiği anlamına gelmektedir. Tüm bu yanlış anlaşılmaya sebebiyet verebilecek uygulamalara engel olmak adına kişilerin veri paylaşımını onayladığı ve onaylamadığı alanların formda net olarak belirtileceği alanın yer alması gerekmektedir.

"Sigorta şirketi için imzaladığım ve fatura ekinde yer alan Kişisel Verilerin Korunmasına Dair Açık Rıza Beyanına ait maddeler konusunda bilgi sahibiyim." maddesine %29,6 en yüksek katılım oranıyla "Kararsızım" yanıtı verilmiştir. Katılımcıların genel olarak bu konuda da kararsız oldukları K.V.K. Dair Açık Rıza Beyanına ait maddeler konusunda bilgi sahibi olmadıkları şeklinde yorumlanabilir.

5’li likert ölçeği kullanılan değişkenlerin normal dağılıma uyup uymadığını tespit etmek için (örnek sayısı 50’den fazla) Shapiro-Wilk testi yerine Kolmogorov- Smirnov testi sonuçlarına bakılmıştır (Sipahi, Yurtkoru, Çinko 2010). Bu test sonucunda normal dağılım gözlenmese de (Genelde 5’li likert vb. şekilde ölçülen değişkenlerde bu sorunla karşılaşılması çok doğaldır) skewness (basıklık) ve kurtosis (çarpıklık) değerlerinin normal dağılım için -1 ve +1 arasında olması nedeniyle bu sorudaki değişkenlerimizin normal dağıldığını kabul edildi (Hair, Black, Babin & Anderson (2013) ve parametrik testler uygulamaya karar verildi.

5’li likert ölçeğinde yer alan 23 maddeye cinsiyet değişkeni yönünden t-testi uygulandığında p değeri 0,05’ten büyük olan değerler cinsiyet yönünden ortalamalarda fark olmadığını göstermektedir. Sadece 2 madde p değeri 0,05’ten küçük olduğu için o maddelerde verilen cevaplarda cinsiyet yönünden fark vardır. Bunlar;

1) “Laboratuvar, ilaç ve tetkik sonuçlarımı bir sağlık uzmanıyla elektronik olarak paylaşırken bilgi güvenliğim konusunda endişe etmem.” (p değeri: 0,023) Ortalamalara baktığımızda kadınların ortalaması daha yüksek olduğu için(3.42>2.97) erkeklere göre laboratuvar, ilaç ve tetkik sonuçlarını bir sağlık uzmanıyla elektronik olarak paylaşırken bilgi güvenliği konusunda daha az endişeli oldukları söylenebilir.

2) “Sigortaya beyan etmediğim hastalığımın poliçeyi satın aldıktan sonra sigorta tarafından araştırılması sigorta şirketine olan güvenimi azaltır.” (p değeri: 0,012) Ortalamalara baktığımızda kadınların ortalaması daha yüksek olduğu için (3.25>2.70) erkeklere göre poliçe satın aldıktan sonra sigorta tarafından beyan etmedikleri hastalıklarının araştırılması konusunda daha hassas oldukları ve erkeklere göre güvenlerinin daha çok azaldığı söylenebilir.

Özel sağlık sigortacılığında veri işleme süreci için onam alınırken devlet sigortasının kullanıldığı SGK kurumunda bu form kullanılmamakta ve bu forumun yerine geçecek farklı bir uygulama da bulunmamaktadır. Bu da yine KVKK mevzuatında Aydınlatılmış Onamı konusundaki hassasiyete rağmen uygulanmayan bir süreçtir.

Daha önce uygulanmakta olan Sağlık.net uygulaması hakkında açılan davalarda belirtildiği üzere sağlık verilerinin sağlık hizmeti verilen tüm kuruluşlardan, Sağlık Bakanlığı'na ve Sağlık Bakanlığı'na bağlı olan kuruluşlara, hizmet alan bütün kişilere ait kişisel sağlık verilerinin aktarılması öngörülmesiyle her türlü vasıtayla "toplama, işleme ve paylaşma" hakları verilerek geniş bir yetkilendirme yapılmıştır. Günümüzde uygulanmakta olan e-Nabız uygulaması için de tüm sağlık kuruluşlarından e-nabız sistemine tüm sağlık verileri kaydedilmektedir ancak bunun için öncesinde kişilerden herhangi bir onam alınmamaktadır. E-Nabız uygulaması yaptığımız anket sonuçlarından da anlaşıldığı üzere kullanımı katılımcılar için kolay ve erişilebilir bir sistemdir. Kişiler kolaylıkla tıbbi raporlarına erişim sağlayabilmektedir. Sağlık verilerimizin bu alana aktarılması için onay alınmayan bir süreç olduğu gözlemlenmiş olsa da uygulama içerisinde kişilerin verilerine erişim limitini kendilerinin belirlediği ve sahip olduğu sağlık verilerini kısıtlama hakkına sahip olması uygulamanın avantajlı yönlerinden birisidir. Böylece kullanıcılar istemediği kişilerin farklı ağlar üzerinden bilgilerine erişim sağlamasını engelleyebilmektedirler. Ancak yine de bu konuda yetkililerin uygulamada yer alan hukuki boşlukları değerlendirmeleri gerekmektedir.

Kişiler özel sağlık sigorta poliçesi satın almadan sigorta şirketler tarafından detaylı sağlık özgeçmişine ait soruları yanıtlaması gerekmekte ve buna göre bir poliçe ücreti belirlenmektedir. Hasta poliçeyi satın aldıktan sonra kullanacağı ilk ve sonraki tüm işlemlerinde sigorta şirketi tarafından geçmiş sağlık kayıtları araştırılmakta eğer beyan edilmeyen bir sağlık kaydına ait tedavi için başvuru yapılmış ise özel sigorta firması tarafından beyan edilmeyen rahatsızlık olması sebebiyle karşılanmamaktadır. Bu konu özel sigortacılığın kuralıdır ve süreç araştırması yapılmadan önce hastadan onam alınmaktadır. Onam alınmadan hasta verilerinin araştırılması mevzuata aykırıdır.

Sağlık verileri ayrıca hassas veri olması sebebiyle oldukça önemlidir. Birçok uygulamanın gerçekleşebilmesi için hastaların tanı ve tedavi bilgilerine ihtiyaç duyulmaktadır. Buna; özel sağlık sigortasının tedaviyi karşılayabilmesi için hastanın tanısını ve tedavi bilgilerini talep etmesi ya da gebe hastaların kontrol ve aşı takiplerinin yapılabilmesi için Sağlık Bakanlığı'na gebliz kaydının yapılması zorunluluğu örnek verilebilir. Veri paylaşımı hassasiyetinin hem kurumlar hem de

kurum çalışanları tarafından öneminin kavranması son derece hassastır. Konuyla ilgili olarak bakanlığın kurum içi idari veya yargısal denetimleri yapması kişisel hakların korunması sürecini perçinleyecektir.

Sağlık Sigortacılığında KVKK mevzuat işleyişi güçlendirmek ve hastaların hukuki olarak sahip oldukları hakların teoride olduğu gibi pratikte de da hassasiyetle uygulanmasını sağlamak için özel sigortacılık adına Türkiye Sigortalar Birliği ve Sigorta Bilgi ve Gözetim Merkezi, devlet uygulamaları adına ise Sağlık Bakanlığı ve Sosyal Güvenlik kurumu arasında ortak çalışmalar yapılarak süreç zinciri güçlendirilmelidir. Ayrıca Serpil Özcan'ın 2018 yılında yaptığı çalışmada da önemini belirttiği üzere kamu ve özel sektör çalışanlarının, veri işleme süreciyle ve güncellenen mevzuatlar konusunda fazla bilgiye sahip olmadıkları görülmektedir. Bu konuda sürece dahil olan tüm çalışanlara kurum içi eğitimler verilerek sürecin önemi anlatılmalıdır.

6. KAYNAKLAR

Abidi, S.S.R. (2008). Healthcare Knowledge Management: The Art Of The Possible. D. Riano,(Ed.) In Knowledge Management For Health Care Procedures: From Knowledge To Global Care: 1-20.

Abd-Alrazaq AA, Bewick BM, Farragher T, Gardner P. Factors that affect the use of electronic personal health records among patients: A systematic review. Int J Med Inform. 2019 Jun;126:164-175. doi: 10.1016/j.ijmedinf.2019.03.014. Epub 2019 Apr 5. PMID: 31029258.

Açık Rıza Kılavuzu. (2019). Kişisel Verileri Koruma Kurumu, Ankara: Balgat.

AİHM (1997). Avrupa İnsan Hakları Mahkemesi Z, Finlandiya kararı, Sayı No: 22009/93, 25 Şubat 1997.

Akçalı Gür B. (2019). Uluslararası Hukuk ve AB Hukuku Boyutuyla Kişisel Verilerin Yurt Dışına Aktarılması. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Cilt 25, Sayı 2.

Akgül A. (2013). Danıştay Kararları Işığında Kişisel Sağlık Verilerinin Korunması; Danıştay Dergisi, 133.

Akgül A. (2015). Kişisel Verilerin Korunması Bağlamında Biyometrik Yöntemlerin Kullanımı ve Danıştay Yaklaşımı, 118- 220.

Akıncı A.N. (2017). Avrupa Birliği Genel Veri Koruma Tüzüğü'nün Getirdiği Yenilikler ve Türk Hukuku Bakımından Değerlendirilmesi. Kalkınma Bakanlığı, İktisadi Sektörler ve Koordinasyon Genel Müdürlüğü. Ankara.

Aksoy H. C. (2010). Medeni Hukuk ve Özellikle Kişilik Hakkı Yönünden Kişisel Verilerin Korunması, Çakmak Yayınevi, Ankara, 1.

Altındiş S. (2010). Kurt M. Bilgi Yönetim Uygulamalarının Hasta Güvenliğine Etkisine İlişkin Bir Araştırma: Afyonkarahisar İlinde Bir Uygulama. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, Sayı: 24, 45-61.

Anayasa Mahkemesi Başkanlığı (2014) Esas No: 2013/114 Karar Sayısı: 2014/22 .
Anayasa Mahkemesi Kararı. (2015). 19.03.2015, Esas No: 2014/180.
Arseven H. (1991). Sigorta Hukuku, 2. Baskı, İstanbul, 3.

Asan O, Cooper II F, Nagavally S, Walker R, Williams J, Ozieh M, Egede L Preferences for Health Information Technologies Among US Adults: Analysis of the Health Information National Trends Survey

Atasoy K. (2016). Kişilik Hakkı Kapsamında Sosyal Medyada Kişisel Verilerin Korunması ve Veri Sahibinin Rızası. Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi, Sayı: 22(3), 269-301.

Avrupa Parlamentosu ve Konsey Yönetmeliği. (2016). Madde 4/14, Brüksel, Belçika.
Aydınlatma Yükümlülüğünün Yerine Getirilmesi Rehberi. (2019). Kişisel Verileri Koruma Kurumu, Ankara.

Başalp N. (2004). Kişisel Verilerin Korunması ve Saklanması, 50.

Bilgi Edinme Hakkı Kanunu (2003). Madde 21, 24/10/2003, Sayı : 25269, Başbakanlık Basımevi, Ankara.

Bioethics Core Curriculum (2008) " Privacy and confidentiality (Article 9)'' UNESCO Division of Ethics, Science and Technology. :41-43

Biyoloji ve Tıbbın Uygulanması Bakımından İnsan Hakları ve İnsan Haysiyetinin Korunması Sözleşmesi: İnsan Hakları ve Biyotıp Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun. Başlangıç Maddesi; 03.12.2013 Sayı: 5013, Ankara.

Civelek, Dilek Y. (2011). Kişisel Verilerin Korunması ve Bir Kurumsal Yapılanma Önerisi. Ankara: T.C. Başbakanlık Devlet Planlama Teşkilatı, 73.

Çeçen O. (2016). Türk Tabipleri Birliği, Kişisel Sağlık Verileri Ulusal Kongresi Kitapçığı . İstanbul: Türk Tabipleri Birliği Yayınları, 72.

Data Protection & Research, Version 1. (2018). Information Compliance Team, University Of Oxford , 2.

Dawson, A., Verweij, M., (ed.). (Bulut, A., Bilgin, A. C., Çokar, M., Yardım, M., Çev. Ed.), (2016). Etik, Önleme ve Halk Sağlığı, HASUDER.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Belgium; 2002.

Dördüncü Beş Yıllık Kalkınma Planı. (1977). Sosyal Güvenlik Ö.İ.K. Raporu, DPT, Ankara.

EC.(2016) European Commission: Green paper on mobile Health, Nisan 2016, 4.

Ekinci N. (2018). Ankara İlinde Yaşayan Kişilerin Genel Sağlık Sigortası ve Özel Sağlık Sigortalarına İlişkin Görüşlerin Değerlendirilmesi. Yüksek Lisans. Ankara: Gazi Üniversitesi.

European Charter Of Patients' Rights. (2012). Rome.

Fang, K., Jiang, Y. ve Song, M. (2016). Customer Profitability Forecasting Using Big Data Analytics: A Case Study of the Insurance Industry. Computers & Industrial Engineering, Sayı: 101, 554-564.

Fred H. Cate, Peter Cullen, (2014) Viktor Mayer-Schönberger, Data Protection Principles for the 21st Century, Mart 2014, Oxford Internet Institute: Oxford University.

GDPR; Council of the European Union; Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. URL:"Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)" [Erişim Tarihi: 22.03.2020].

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

Groves, P., Kayyali, B., Knott, D. ve Kuiken, S. V. (2013).The "Big Data" Revolution in Healthcare, Accelerating Value and Innovation. Washington, DC, U.S.A.: Center of US Health System Reform Business Technology Office, McKinsey & Company, 3.

Gülener S.(2012). Dijital Hafızadan Silinmeyi İstemek: Temel Bir İnsan Hakkı Olarak "Unutulma Hakkı", 226.

Güvel A.(2002). Sigortacılık, Seçkin Yayınları, Ankara.

Güzel A. Okur A. R. Caniklioğlu N. (2009). Sosyal Güvenlik Hukuku, 12. Basım, İstanbul.

Hakeri H. (2018). Tıp Hukuku, Seçkin, 13. Baskı, İstanbul, 91-92.

Handbook on European data protection law. (2018). Luxembourg. Imprimerie Centrale in Luxembourg, 92.

Hayrunnisa Ö. (2009). Elektronik Haberleşme Alanında Kişisel Verilerin Özel Hukuk Hükümlerine Göre Korunması, Seçkin Yayınları, Ankara, 36.

Henkoğlu T. (2015). Bilgi Güvenliği ve Kişisel Verilerin Korunması, Yetkin Yayınları, Ankara.

HIPAA, (2018). Health Insurance Portability and Accountability Act of 1996, Public Law No: 104-191. November 30, 2018.

Hirakis O. & Karakounos S. (2008). Goals And Benefits Of Knowledge Management İn Healthcare. In Murray E. J. (Ed.) Knowledge Management: Concepts, Methodologies, Tools, And Applications (2232-2239). New York: Information Science Reference.

Holvast J. (2007). The History of Information Security, Chapter, 2007; 27, s.737- 769

İstanbul Tabip Odası. (2015). Hekimler ve Hastalar İçin El Kitabı Kişisel Sağlık Bilgileri, 9.

İzgi M.C. (2014). Mahremiyet kavramı bağlamında kişisel sağlık verileri, Türkiye Biyoetik Dergisi, Cilt No: 1, 25-37.

Jones R. Tahri D. (2010). EU law requirements to provide information to website visitors, Computer Law & Security Review, Vol. 26, 613-620.

Kart A.(2013) 'Live Case Demonstration' ve Aydınlatılmış Onam Bağlamında Kişisel Verilerin Korunması. 3. Uluslararası Bilişim Hukuku Kurultayı, İzmir, 135- 141.

Kartal M.T. (2018). Kişisel Verilerin Korunması: Türk Bankacılık Sektörü Üzerine Kavramsal Bir Değerlendirme, Uluslararası Ekonomi ve Yenilik Dergisi, Sayı: 4 (1), 1-18.

Khan S. Hoque A. (2016). Digital Health Data: A Comprehensive Review of Privacy and Security Risks And Some Recommandations. Computer Science Journal of Moldova, vol.24, Sayı: 2(71).

Kişisel Veri İşleme Envanteri Hazırlama Rehberi. (2019). Ankara, Sayı:30.

Kişisel Verilerin Korunması Alanında Uluslararası ve Ulusal Düzenlemeler. (2019). Kişisel Verileri Koruma Kurumu, Ankara.

Kitapçı Şişman N. (2019). Özel Sağlık Sigorta Şirketleri Çalışanlarının Elektronik Sağlık Kayıtlarının Gizliliği ve Güvenliği Hakkında Görüşlerinin Değerlendirilmesi. İstanbul: Marmara Üniversitesi. Yüksek Lisans.

Kohli R. Swee-Lin Tan S. (2016). Electronic Health Records: How Can Is Researchers Contribute To Transforming Healthcare? MIS Quarterly Vol. 40 Sayı:3.

Korkmaz İ. (2016). Kişisel Verilerin Korunması Kanunu Hakkında Bir Değerlendirme; Tbb Dergisi. Sayı:124, 83.

Kök A.H. (2018). İnsan Hakları ve Biyotıp Sözleşmesi'nin Uygulanmasında Türkiye İnsan Hakları ve Eşitlik Kurumu, Sayı:1, 155.

Küzeci, E. (2018). Kişisel Verilerin Korunması (2. Baskı), Ankara :Seçkin, s. 466

KVKK Yayınları, Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular; Ankara: KVKK Yayınları; 22.

Lehaney, B., Clarke, S., Coakes, E., Jack, G.,(Ed.). (2004). Beyond Knowledge Management. Hershey, PA: Idea Group Publishing, 12.

Mahmoud, R., Moody, A., Foster, M., Girdharry, N.R., Sinn, L., Zhang, B., Afshin, M., Vivekanandan, T., Santoro, S., & Tyrrell, P. (2019). Sharing De-identified Medical Images Electronically for Research: A Survey of Patients' Opinion regarding Data Management. Canadian Association of Radiologists Journal, 70, 212 - 218.

Marşap A. Akalp G., Yeniman E. (2010). Sağlık İşletmelerinde İnsan Kaynağının Kurumsal Bilgi ve Güvenliği Kültürü Gelişimi. Bilişim Teknolojileri Dergisi, Cilt: 3, Sayı:1,31.

Naik, K. ve Joshi, A. (2017) Role of Big Data in Various Sectors. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), Tirupur, India, Sayı: 117, 122.

Olca Emre, Özgü C. (2014). Ulusal ve Uluslararası Yönetmeliklerde Kişisel Sağlık Verisi Mahremiyetinin Korunması; 5.

Orak B. (2019). Kişisel Sağlık Verilerinin Korunması. Yüksek Lisans. Ankara: Hacettepe Üniversitesi.

Orhan T. Mithat K. (2015). Türkiye ve Avrupa'da Özel Sağlık Sigortaları, JEFA, Sayı:2, 409-425.

Orhaner E. (2018). Türkiye'de Sağlık Sigortası, 1.Baskı, Ankara, Siyasal Kitabevi.

Ömür R.C. (2018). "Kişisel Sağlık Verilerinin Korunması ve Hastanelerin Sorumluluğu", YÜHFD,C.XV, Sayı:1,133-180.

Özdemir H. (2009). Haberleşmenin Gizliliği ve Kişisel Veriler, Erzincan Üniversitesi Hukuk Fakültesi Dergisi, Cilt: XIII, Sayı: 1–2, 291.

Özdemir S. (2001). T.C. Başbakanlık Devlet Planlama Teşkilatı, Avrupa Topluluğunda İkincil Mevzuat ve Karar Alma Usulleri, 4.

Özsarı H. (2003). Bir Özel Sağlık Sigortacılık Kurumunda Kullanıcıların Özellikleri ve Risk Grupları, Ankara: Hacettepe Üniversitesi. Doktora Tezi, 42.

Presthus, Wanda & Sørum, Hanne. (2018). Are Consumers Concerned About Privacy? An Online Survey Emphasizing the General Data Protection Regulation. Procedia Computer Science. 138. 603-611. 10.1016/j.procs.2018.10.081.

Pişkin B. (2017). Sağlık Sistemleri İçerisinde Özel Sağlık Sigorta Şirketleri ve Türkiye. Edirne: Trakya Üniversitesi. Yüksek Lisans, 57.

Sağlık Yazılımı Daire Başkanlığı. (2019). Medula Web Servisleri Kullanım Kılavuzu, Ankara, 40.

Sarıusta K. (2018). Kişisel Verilerin Ceza Hukuku Yoluyla Korunması. Yüksek Lisans. Gaziantep; Gaziantep Üniversitesi, 82.

Sert, G.S. (2008). Tıp Etiği ve Mahremiyet Hakkı. İstanbul-Babil, 103.

Slowther A and Kleinman E. (2009) “Confidentiality”, The Cambridge Textbook of Bioethics, ed. Peter A Sin ger, A.M. Viens, Cambridge University Press, New York USA, Third Printing, 43-48.

Soykan C. (2006) “Avrupa İnsan Hakları Mahkemesi İçtihatlarında Bilgi Edinme Hakkı: Özel Hayatın Gizliliği X İfade Özgürlüğü”, A.Ü. Siyasal Bilgiler Fakültesi İnsan Hakları Merkezi Çalışma Metinleri III, 3.

Şenyürek G. (2017). Etik Açıdan Kişisel Sağlık Verileri ve Korunması. Yüksek Lisans. İstanbul: Acıbadem Üniversitesi, 156.

Şimşek O. (2008). Anayasa Hukukunda Kişisel Verilerin Korunması, 91.

T.C. Resmî Gazete. Kişisel Verilerin Korunması Kanunu. 24.03.2016. Sayı: 29677, Başbakanlık Basımevi, Ankara.

T.C. Resmî Gazete. Birleşmiş Milletler Genel Kurulu, İnsan Hakları Evrensel Bildirgesi, 10.12.1948. Sayı No: 7217.

T.C. Resmî Gazete. Kişisel Verilerin Otomatik İşleme Tabi Tutulması Karşısında Bireylerin Korunması Sözleşmesine Ek Denetleyici Makamlar ve Sınır aşan Veri Akışına İlişkin Protokol (181 Sayılı Ek Protokol), Madde 1, 05/05/2016 Sayı: 29703, Ankara.

T.C. Resmî Gazete. Sosyal Güvenlik Kurumu Başkanlığı. Sosyal Güvenlik Kurumu Sağlık Uygulama Tebliğinde Değişiklik Yapılmasına Dair Tebliğ; Madde 1(*); 09.04.2020, Sayı: 31094, Ankara

Sağlık Bilgi Sistemleri Genel Müdürlüğü (2016), Sağlık.Net Online ve e-Nabız Hk., Sayı:67189002; Ankara.

TBK, Türk Borçlar Kanunu (2011). RG, 27836, 11/01/2011, Başbakanlık Basımevi, Ankara.

TCK, Türk Ceza Kanunu(2004), Madde 136; 12/10/2004. Sayı: 25611, Başbakanlık Basımevi, Ankara.

Tekin, N . (2014) "Kişisel Verilerin Korunması ile İlgili Türkiye'deki Kanun Tasarısının Avrupa Birliği Veri Koruma Direktifi Işığında Değerlendirilmesi". Uyuşmazlık Mahkemesi Dergisi, Sayı: 222-262, 292

Türkiye Cumhuriyeti Anayasası; Madde 20; 18/10/1982. Sayı: 17863, Başbakanlık Basımevi, Ankara.

URL-1: Türk Dil Kurumu; http://tdk.gov.tr/ [Erişim Tarihi: 08.12.2019].

URL–2: Avrupa Birliği Hukuku; https://eur-lex.europa.eu/, [Erişim Tarihi: 12.12. 2019].

URL-3: Hayat Eve Sığar (HES); https://hayatevesigar.saglik.gov.tr/hes.html [Erişim Tarihi: 02.08.2020].

URL-4: OECD Privacy Guidelines. (2013). http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm [Erişim Tarihi: 02.05.2020].

URL-5: Nitelikli Veri, Gizlilik ve Çerez Politikası,

http://nitelikliveri.com/kvkk-kavramlar/gizlilik-ve-cerez-politikasi-nedir/

[Erişim Tarihi: 30.04.2020].

URL-6: T.C. Sosyal Güvenlik Kurumu, Kurumsal Tanıtım, http://www.sgk.gov.tr/wps/portal/sgk/tr/kurumsal/kurumsal_tanitim [Erişim Tarihi: 12.12.2019].

URL-7: T.C. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü'nün 75730711 sayılı yazısı http://khgm.saglik.gov.tr/Dosyalar/a1d4643811c74bba9949f8e57731634e.pdf [Erişim Tarihi: 12.11.2019].

URL-8: T.C Sağlık Bakanlığı - Sağlık Bilgi Sistemleri Genel Müdürlüğü, Sağlık.NET Hakkında; https://e-saglik.gov.tr/TR,6212/sagliknet-hakkinda.html [Erişim Tarihi: 08.03.2020].

URL-9: İstanbul Tabip Odası. (2012). 25 soruda "Sağlık.NET 2" sistemi. https://istabip.org.tr/icerik/net2sorucevap.pdf [Erişim Tarihi: 02.01.2019].

URL-10: Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü. (2014). Bilgi Güvenliği Politikaları Kılavuzu: https://bilgiguvenligi.saglik.gov.tr/files/BilgiGüvenliğiPolitikalarıKılavuzu.pdf [Erişim Tarihi: 14.03.2020].

URL-11: Kişisel Verileri Korkuma Kurumu, Yurtdışına Veri Aktarımında Veri Sorumlularınca Hazırlanacak Taahhütnamede Yer Alacak Asgari Unsurlar https://www.kvkk.gov.tr/Icerik/4236/Yurtdisina-Veri-Aktariminda-Veri-Sorumlularinca-Hazirlanacak-Taahhutnamede-Yer-Alacak-Asgari-Unsurlar [Erişim Tarihi: 18.03.2020].

URL-12:Siberasist.com https://www.siberasist.com/images/files/kvkk100soruda.pdf [Erişim Tarihi 22.03.2020].

URL-13: Google, Gizlilik ve Şartlar, https://policies.google.com/faq?hl=tr , [Erişim Tarihi 04.04.2020].

URL-14: All About Cookies.org, https://www.allaboutcookies.org/, [Erişim Tarihi: 04.04.2020]

URL-15: Türkiye Sigortalar Birliği, https://www.tsb.org.tr/koronavirussalginibasinaciklamasi.aspx.aspx?pageID=409&nID=16437&NewsCatID=%20331 [Erişim Tarihi: 02.08.2020].

URL-16: Kişisel Verileri Korkuma Kurumu. https://www.kvkk.gov.tr/Icerik/6726/COVID-19-IL-E-MUCADELEDE-KONUM-VERISININ-ISLENMESI-VE-KISILERIN-HAREKETLILIKLERININ-IZLENMESI-HAKKINDA-BILINMESI-GEREKENLER-2-

[Erişim Tarihi: 18.05.2020].

URL-17: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML [Erişim Tarihi: 23.03.2020].

URL-18: Berktaş A.E. (2020) Mahremiyet Hukuku Danışmanı, Covid-19 kapsamında Mobil Takip Uygulamaları. https://mahremiyet.info/covid-19-kapsaminda-mobil-takip-uygulamalari [Erişim Tarihi: 02.08.2020].

URL-19: Amazon Turkey Perakende Hizmetleri Limited Şirketince işlenen kişisel veriler hakkında yapılan başvuru ile ilgili Kişisel Verileri Koruma Kurulunun 27/02/2020 Tarihli ve 2020/173 Sayılı Karar Özeti. https://www.kvkk.gov.tr/Icerik/6739/2020-173 [Erişim Tarihi: 18.05.2020].

URL-20: Danıştay, 12.06.2014, Esas No. 2014/4562.

https://www.istabip.org.tr/icerik/biyometrikyurutmeyidurdurma.pdf

[Erişim Tarihi: 27.02.2020].

URL-21: Danıştay, 12.06.2014, Esas No. 2013/2084.

https://www.ttb.org.tr/images/stories/file/2014/ydkabul.pdf

[Erişim Tarihi: 27.02.2020].

URL-22: Levent R. (2013). Dünyada ve Türkiye'de Sosyal Güvenliğin Gelişimi.

:https://www.isvesosyalguvenlik.com/dunyada-ve-turkiyede-sosyal-guvenligin-gelisimi/

[Erişim Tarihi: 10.12.2020].

URL-23:T.C. Sağlık Bakanlığı e-Nabız Kişisel Sağlık Kaydı Sistemi: https://enabiz.gov.tr/document/KILAVUZ_.pdf [Erişim Tarihi: 01.05.2021].

URL-24: Turan H. Kişisel Verinin 7 Hali. 2016.: https://hsturan.com/kisisel-verinin-7-hali [Erişim Tarihi: 03.01.2020].

Wma Declaration Of Lisbon On The Rights Of The Patient; Oslo, Norway, April 2015

World Health Organisation. (2016). Global diffusion of eHealth: Making universal health coverage, Report of the third global survey on eHealth, Global Observatory for eHealth, İsviçre, 109.

Yıldırım H.H. (2012) Sağlık Sigortacılığı- T.C. Anadolu Üniversitesi Yayını No: 2527 Açıköğretim Fakültesi Yayını, Sayı: 1498, 72.

Yurdakul M. Dalkılıç N. (2016). Sigortacılık Sektöründe Dijital Çağ. Sosyal Bilimler Dergisi, Sayı:50.

EKLER

EK-1: Etik Kurul Onayı

T.C.
İstanbul
YENİ YÜZYIL
ÜNİVERSİTESİ

FEN,SOSYAL VE GİRİŞİMSEL OLMAYAN SAĞLIK BİLİMLERİ ARAŞTIRMALARI ETİK KURULU

08.09.2020

Sayı : 2020/09-497
İlgi : Etik Kurul Onayı,

Sayın
Ayşe Gizem UNUR

İstanbul Yeni Yüzyıl Üniversitesi Etik Kurulunun 07.09.2020 tarih ve 2020/ 09-497 sayılı toplantı sonucunda **'' Sağlık Sigortacılığı alanında kişisel verilerin korunması kanunu hakkında hastaların yaklaşımının değerlendirilmesi''** başlıklı çalışmanız Fen, Sosyal ve Girişimsel Olmayan Sağlık Bilimleri Araştırmaları Etik Kurul Kurulumuzca oy birliği ile **UYGUN** bulunmuştur.

Araştırmanız süresince çalışmanızda özellikle konu başlığı, gereç ve yöntemler konusu ile ilgili olarak değişiklikler söz konusu olursa tekrar değerlendirilmesi gereklidir.

Not: İşbu belge İstanbul Yeni Yüzyıl Üniversitesi Fen, Sosyal ve Girişimsel Olmayan Sağlık Bilimleri Araştırmaları Etik Kurul Yönergesi temelinde kaleme alınmıştır.

İş bu belge kurum onayı dahilinde geçerlidir.

İstanbul Yeni Yüzyıl Üniversitesi
Fen,Sosyal ve Girişimsel Olmayan
Sağlık Bilimleri Araştırmaları
Etik Kurulu Başkanı

www.yeniyuzyil.edu.tr e:tanitim@yeniyuzyil.edu.tr
Dr. Azmi Oflueoğlu Yerleşkesi Yılanlı Ayazma Cd. No:26 Cevizlibağ / İSTANBUL Tel: 444 50 01 Faks: 0.212 481 40 58

EK-2: Aydınlatılmış Onam

AYDINLATILMIŞ ONAM

Sayın Katılımcı;

Bu araştırmada elde edilecek bilgiler, İstanbul Yeni Yüzyıl Üniversitesi Sağlık Bilimleri Enstitüsü Sağlık Yönetimi Yüksek Lisans programında Doç. Dr. Itır ERKAN Danışmanlığında, Yüksek Lisans Öğrencisi Ayşe Gizem Unur'un "Sağlık Sigortacılığı Alanında Kişisel Verilerin Korunması Kanunu Hakkında Hastaların Yaklaşımının Değerlendirilmesi" başlıklı tez araştırmasında kullanılacaktır. Sorulara içtenlikle vereceğiniz cevaplar araştırmanın güvenilirliği için büyük bir önem taşımaktadır. Ankette vereceğiniz yanıtlar gizli tutulacak olup, kişi ve kurum bilgisi paylaşılmadan bilimsel amaçlı kullanılacaktır.

Ayşe Gizem UNUR
Sağlık Yönetimi Yüksek Lisans Öğrencisi

Anket sorularına vereceğim cevapların araştırma amaçlı olarak kullanılması konusunda bilgilendirildim ve hiçbir baskı altında kalmadan elde edilen sonuçların anonim bir şekilde bilimsel yayınlarda kullanmalarını kabul ediyorum.

Tarih:

İmza:

EK-3: Anket Soruları

1) Yaşınız?

- o 18-24
- o 25-34
- o 35-44
- o 45-54
- o 55-64
- o 65-74
- o 75 ve üzeri

2) Cinsiyetiniz?

- o Kadın
- o Erkek

3) Mezuniyet dereceniz nedir?

- o İlkokul
- o Ortaokul
- o Lise
- o Üniversite
- o Yüksek Lisans
- o Doktora

4) Aylık geliriniz ?

- o 0 TL – 1.000 TL
- o 1.000 TL – 2.500 TL
- o 2.500 TL – 5.000 TL
- o 5.000 TL -10.000 TL
- o 10.000 TL ve üzeri

5) Kişisel sağlık verisini kavramını daha önce duydunuz mu?

- Evet
- Hayır

6) Kişisel verilerin kaydedildiği veri tabanını düzenlemek ve özel ve güvenli tutmak için en çok kime güvenirsiniz? Lütfen birini seçiniz.

- Sigorta Şirketim
- Hastaneler
- Hükümet
- Diğer, lütfen belirtiniz _____

7) Farklı sağlık kurumu ziyaretlerinden ve sağlayıcılardan(sigorta şirketinizden veya mobil uygulamalardan) gelen tüm tıbbi bilgilerinizin veri tabanında otomatik olarak saklanmasını doğru buluyor musunuz?

- Evet
- Hayır

8) Bilgilerinizin kısıtlayabileceğinizi biliyor musunuz?

- Evet
- Hayır

9) Veri tabanına hangi bilgilerin gireceğini nasıl kısıtlamak isterdiniz ?

- Hangi sağlayıcılarımın veri tabanına dahil edilecek tıbbi bilgileri gönderebileceğine karar vermek istiyorum.
- Hangi ziyaretlerimin veri tabanına dahil edileceğine karar vermek istiyorum (poliklinik ziyaretleri, acil servis ziyaretleri veya hastanede kalışlar, vb.)
- Veri tabanına ne tür tıbbi bilgilerin dahil edileceğine karar vermek istiyorum (Örneğin, tüm test sonuçlarımı ve ilaçlarımı dahil etmek isteyebilirim, ancak belirli teşhisler hakkında bilgi vermek istemiyorum).
- Bilgilerim sisteme dahil edilmeden önce her bölümünü onaylamak istiyorum (Bireysel doktor notları ve test sonuçları dahil).

10) Sizce kimin elektronik tıbbi kayıtlarınızı görebilmesi gerekir ve görüntüleme için izniniz gerekiyor ?

	Evet, iznim olmadan erişebilir	Evet, bakabilir ama sadece iznimle	Kayıtlarıma asla bakma izni verilmemeli
Belirlenmiş aile üyeleri veya arkadaşlar			
Tedavi sürecimden sorumlu hekim görebilir.			
Bana bakan diğer doktorlar veya sağlık hizmeti sağlayıcıları (klinikte, acil serviste veya hastanede)			
Sigorta Şirketim			
Bir doktora elektronik tıbbi kaydınızı görüntüleme ve ekleme izni verdikten sonra, bu doktorun kaydınıza ne kadar süre erişmeye devam etmesi gerekir?			
Hükümet yetkilileri			

11) Bir doktora elektronik tıbbi kaydınızı görüntüleme ve ekleme izni verdikten sonra, bu doktorun kaydınıza ne kadar süre erişmeye devam etmesi gerekir? Lütfen birini seçiniz.

- Doktorum sonsuza kadar sürekli erişime sahip olabilir.
- Doktorum izin verdiğim sürece sürekli erişime sahip olabilir.
- Doktorum 1 yıl boyunca sürekli erişime sahip olabilir.
- Doktorum onlarla yaptığım ziyaretten sonra yalnızca bir hafta süreyle erişime sahip olabilir.

12) Acil bir durum sırasında eğer izin verebilecek durumda değilseniz, kimlerin tıbbi kayıtlarınızı görebilmesi gerektiğini düşünüyorsunuz? Lütfen geçerli olanların tümünü kontrol edin.

- Belirlenmiş aile üyeleri veya arkadaşlar
- Tedavimden sorumlu doktorum
- Bana bakan diğer doktorlar veya sağlık hizmeti sağlayıcıları (klinikte, acil serviste veya hastanede)
- Acil bir durumda bile hiç kimse benim iznim olmadan tıbbi kayıtma erişemez

13) Son 12 ay içinde kişisel sağlık bilgilerinize çevrimiçi olarak güvenli bir web sitesi veya uygulama üzerinden kaç kez eriştiniz?

- 1 - 2
- 3-5
- 6-9
- 10 ve üzeri
- Hiçbiri

14) KVKK bireylerin kişisel verilerin toplanması ve depolanması konusunda yeni haklar kazandığı anlamına gelir. Bunun hakkında ne düşünüyorsun?

- Haklarım gelişti
- Haklarımın geliştiğini sanmıyorum
- Fikrim yok

15) KVKK, sizinle ilgili bazı kişisel bilgilerin (şirketlerin topladığı) silinmesini talep etme konusunda daha büyük bir hak vermiştir. Bunun hakkında ne düşünüyorsun?

- Bu hakkımı uyguladım
- Bu hakkımı uygulayabilirim
- Büyük olasılıkla bu hakkımı uygulamayacağım
- Fikrim yok

16) Cep telefonunuza bir uygulama indirdiğinizde veya dizüstü bilgisayarınıza bir program yüklediğinizde, şartlar ve koşulları onaylamanız gerekir. Bu konudaki tipik tepkiniz nedir?

- Uzun süre almasına rağmen metnin tamamını okurum
- Hızlıca tüm metni kaydırıyorum, ancak her şeyi okumuyorum
- Metne bakmadan “Katılıyorum / kabul ediyorum”u tıklıyorum
- Zaman zaman değişir (söz konusu uygulamaya / programa bağlı olarak)

17) Aşağıdaki ifadelerden durumunuzu /görüşünüzü en iyi şekilde yansıtan seçeneği işaretleyiniz.

	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum
23 Mart 2016'da yürürlüğe giren Kişisel Verileri Koruma Kanunu (KVKK) hakkında daha önceden bir şeyler duydum.	1	2	3	4	5
E- nabız uygulamasını kullanıyorum	1	2	3	4	5
E- nabız uygulamasının bilgilerimi koruduğuna inanıyorum.	1	2	3	4	5
E- nabız kullanırken gizlilik sorunları konusunda endişeliyim.	1	2	3	4	5
E-nabız kullanmayı öğrenmenin benim için zor olacağını düşünüyorum.	1	2	3	4	5
E- nabız uygulamasının hayatımı kolaylaştırdığını düşünüyorum.	1	2	3	4	5
Sağlık kaydımın gizli tutulacağını hissediyorum.	1	2	3	4	5
E- nabız web sitesindeki sorunlar için Sağlık Bakanlığı yardım masasının sorunların çözümünde her zaman yardımcı olduğuna inanıyorum.	1	2	3	4	5
Mobil sağlık uygulamalarını bir doktora danışman veya ikinci bir doktor görüşü almak için kullanırım.	1	2	3	4	5

Farklı işletmelerin veri tabanlarında depolanan kişisel bilgileriniz üzerinde kontrol sahibi olduğumu düşünürüm.	1	2	3	4	5
Özel sağlık sigortamın kişisel sağlık verilerimi koruduğuna eminim.	1	2	3	4	5
Özel sağlık sigortamın, sağlık kuruluşlarından benim için talep edilen belgeler süreç akışı gereği benden onay alınmadan da hastane tarafından kurumlar ile paylaşılabilir.	1	2	3	4	5
Sağlık sigortalarının provizyon sürecinde beni tüm kurumlardan araştırması beni rahatsız etmez.	1	2	3	4	5
Sigortaya beyan etmediğim hastalığımın poliçeyi satın aldıktan sonra sigorta tarafından araştırılması sigorta şirketine olan güvenimi azaltır.	1	2	3	4	5
Poliçe satın alırken poliçedeki tüm maddeleri okurum ve anlamadığım kısımları sigortacıma danışırım.	1	2	3	4	5
Sigorta şirketi faturalandırması için imzaladığım evrakların tamamını okumadan imzalamam.	1	2	3	4	5
Sigorta şirketi için imzaladığım ve fatura ekinde yer alan Kişisel Verilerin Korunmasına Dair Açık Rıza Beyanına ait maddeler konusunda bilgi sahibiyim.	1	2	3	4	5
Kişisel verilerimin bazı durumlarda benden ekstra rıza alınmadan paylaşılabileceğini biliyorum.	1	2	3	4	5
Kişisel verilerime sahip olan veri sorumlusundan; verilerin işlenme amacına uygun olarak işlenip işlenmediğini sorarım.	1	2	3	4	5
Eksik/yanlış işlenme durumunda veri sorumlusundan düzeltme hakkı talep ederim.	1	2	3	4	5
Kurumlarda silinmesini istediğim veriler olursa bunlar için başvuru yapabilirim.	1	2	3	4	5
Avrupa Birliğinde yayınlanan Kişisel verilerim Korunması konusundaki yayınlar hakkında bilgi sahibiyim.	1	2	3	4	5