BAŞKENT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI
YÖNETİM BİLİŞİM SİSTEMLERİ TEZLİ YÜKSEK LİSANS PROGRAMI

SAYISAL SAĞLIK VERİLERİNDE FARKINDALIK

HAZIRLAYAN

Denizhan Yılmaz

YÜKSEK LİSANS TEZİ

ANKARA - 2021

BAŞKENT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI
YÖNETİM BİLİŞİM SİSTEMLERİ TEZLİ YÜKSEK LİSANS PROGRAMI

SAYISAL SAĞLIK VERİLERİNDE FARKINDALIK

HAZIRLAYAN

Denizhan Yılmaz

YÜKSEK LİSANS TEZİ

TEZ DANIŞMANI

Dr. Öğr. Üyesi Esma Ergüner Özkoç

ANKARA – 2021

BAŞKENT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
YÜKSEK LİSANS TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

Tarih:12/01/2021

Öğrencinin Adı, Soyadı: Denizhan YILMAZ

Öğrencinin Numarası: 21810259

Anabilim Dalı: Yönetim Bilişim Sistemleri Anabilim Dalı

Programı: Yönetim Bilişim Sistemleri Tezli Yüksek Lisans Programı

Danışmanın Unvanı/Adı, Soyadı: Dr. Esma ERGÜNER ÖZKOÇ

Tez Başlığı: Sayısal Sağlık Verilerinde Farkındalık

Yukarıda başlığı belirtilen Yüksek Lisans/Doktora tez çalışmamın; Giriş, Ana Bölümler ve Sonuç Bölümünden oluşan, toplam 119 sayfalık kısmına ilişkin, 12/01/2021 tarihinde tez danışmanım tarafından TURNITIN adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı %19'dur. Uygulanan filtrelemeler:

1. Kaynakça hariç
2. Alıntılar hariç
3. Beş (5) kelimeden daha az örtüşme içeren metin kısımları hariç

"Başkent Üniversitesi Enstitüleri Tez Çalışması Orijinallik Raporu Alınması ve Kullanılması Usul ve Esaslarını" inceledim ve bu uygulama esaslarında belirtilen azami benzerlik oranlarına tez çalışmamın herhangi bir intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

Öğrenci İmzası:

ONAY

Tarih: 12 /01/ 2021

Öğrenci Danışmanı Unvan, Ad, Soyad, İmza:

Dr. Esma ERGÜNER ÖZKOÇ

TEŞEKKÜR

Tezimin konusunun belirlenmesi ve yürütülmesinde desteğini esirgemeyen, değerli danışmanım Sayın Dr. Öğretim Üyesi Esma Ergüner ÖZKOÇ`a teşekkürlerimi ve saygılarımı sunarım.

Tez sürecim boyunca fikirlerinden yararlandığım, anket çalışmam ve tez sürecimde görüş ve desteğini esirgemeyen Sayın Öğretim Üyesi Gizem ÖĞÜTÇÜ`ye teşekkürlerimi ve saygılarımı sunarım.

Eğtim hayatım boyunca her zaman yanımda olan desteklerini esirgemeyen çok kıymetli annem ve babam Nurhan ve Yusuf YILMAZ`a sonsuz teşekkürlerimi sunarım.

ÖZET

Elektronik Sağlık Kayıtları (ESK) sistemleri, kişilerin, geçmiş ve şimdiki fiziksel ve ruhsal sağlık durumlarıyla ilgili tüm bilgilerin bilgisayar ortamında toplanmasını, kayıt altına alınmasını, saklanmasını, iletilmesini, erişilmesini, ilişkilendirilmesini, işlenmesini ve gerektiğinde kullanılmasını sağlayan sistemlerdir. İnsanların en mahrem bilgilerini ihtiva eden, hassas olarak adlandırılan sağlık verilerinin hukuka aykırı bir biçimde ele geçirilmesi, işlenmesi veya paylaşılması ayrımcılık başta olmak üzere ilgili kişinin ciddi zararlara uğramasına sebep olabilmektedir. Bu bilgilerin paylaşılması kişinin özel hayatının gizliliğine, hastanın mahremiyet hakkının korunmasına ve doktorun hastasına karşı sır saklama yükümlülüğünün ihlal edilmesine sebep olmaktadır.

Kişisel Elektronik Sağlık Kayıtları (KESK)'nın tutulduğu sayısal sistemlerin donanım veya yazılımlarında bulunan güvenlik zafiyetleri, sistemleri siber saldırılara açık hale getirmesi bir başka sorun olarak karşımıza çıkmaktadır. Sistemlere sızmayı başaran saldırganlar, burada tutulan sağlık verilerinde değişiklikler yapabilmekte ya da verileri başka amaçlarla kullanılmak üzere üçüncü şahıslara satabilmektedirler. Kişisel sağlık verilerin yitirilmesi veya yanlış şekilde anonimleştirilmesi diğer zafiyetler olarak değerlendirilmektedir. Oluşabilecek tüm bu zafiyetler konusunda gerek bireyler ve gerekse toplumsal hassasiyetler artmakta, tartışmalar ve çalışmalar kamuoyunun gündeminde gittikçe artan bir şekilde yer almaktadır.

Bu çalışmada, Türkiye'de yaşayan ve anket çalışmasına katılan farklı demografik özelliklere sahip bireylerin kişisel sağlık verileri ile ilgili farkındalık ve beklentilerinin ölçülmesi ve değerlendirilmesi istatiksel olarak incelenmiştir.

Çalışma kapsamında elde edilen sonuçlara göre, katılımcıların büyük çoğunluğu, iletişim, özlük, aile sağlık bilgileri, muayene sonuçları, geçirdikleri operasyonlarını kişisel bulduklarını ifade etmişlerdir. Aynı kapsamda aile hekimlerinin, uzman doktorlarının ve

sağlık kurumlarının adlarını ise kişisel bulmadıklarını belirtmişlerdir. Katılımcıların büyük çoğunluğu, bu bilgilerinin sayısal ortamlarda kayıt altına alındığını bildiklerini belirtmişlerdir. Katılımcılar sağlık verilerinin kötü amaçla kullanılabileceği ve verilerin gizliliğinin korunması konularında büyük oranda endişeli olduklarını belirtmişlerdir.

Katılımcılar, sağlık verilerini ve sağlık harcamalarının kimlerin görebileceğinin yetkilendirmelerini kendileri yapmak istemektedirler. Sağlık bilgilerinin sayısal ortamda saklanması konusunda katılımcılar genel olarak sayısal ortamda saklanan sağlık bilgilerinin ve sayısal ortamları güvenilir bulduklarını belirtmişlerdir. Katılımcılar bu bilgilerin sağlık kuruluşları ve doktorlar tarafında kendi tedavileri için kullanılmasını yararlı bulduklarını belirtmişlerdir. Katılımcıların büyük çoğunluğu sağlık verilerinin güvenliğini sağlamaktan devletin sorumlu olduğunu ve sağlık verileri ile ilgili tüm hakların kendilerine ait olduğunu belirtmişlerdir. Sağlık verilerinin özel nitelikli kişisel veri olduğunu belirten katılımcıların oranı bir hayli yüksek olsa da KVKK kapsamından kişisel verilerinin korunduğunu bilen ve veri ihlaline uğradıklarında ne yapacağını bilen katılımcı oranı bu oran kadar yüksek değildir. Araştırma sonucunda elde edilen bulgular değerlendirildiğinde genel olarak sağlık sektöründe çalışan bireylerin kişisel sağlık verileri ile ilgili farkındalıklarının yüksek olduğu, diğer katılımcılarda ise eğitim seviyesinin yükselmesi ile birlikte farkındalığın arttığı saptanmıştır.

Anahtar Kelimeler: YBS, Bilgi Güvenliği, Kişisel Sağlık Verileri, Sayısal Sağlık Verileri, Sağlık Verileri Farkındalık ve Beklentileri

ABSTRACT

Electronic Health Records (EHR) systems are systems that allow people to collect, record, store, transmit, access, relate, process and use all information about their past and present physical and mental health conditions in computer environment. The illegal acquisition, processing or sharing of health data, which includes the most intimate information of people, may cause serious harm to the person concerned, especially discrimination. Sharing this information causes the privacy of the person's private life, the protection of the patient's right to privacy, and the violation of the doctor's obligation to keep secrets against his patient.

Security weaknesses in the hardware or software of the digital systems where Personal Electronic Health Records (PEHR) are kept, making the systems vulnerable to cyber attacks is another problem. Attackers who manage to infiltrate the systems can make changes to the health data stored here or sell the data to third parties for other purposes. The loss or incorrect anonymization of personal health data is considered as other weaknesses. Both individuals and social sensitivity about all these vulnerabilities increase, and discussions and studies are increasingly on the agenda of the public.

In this study, the survey living in Turkey and participating in the study with different demographic characteristics awareness and expectations regarding personal health data of individuals were examined statistically measured and evaluated.

According to the results obtained within the scope of the study, the majority of the participants stated that they found communication, personal information, family health information, examination results and operations they had personal. In the same context, they stated that they do not consider the names of family physicians, specialists and health institutions personal. Majority of the participants stated that they knew that this information was recorded in digital media. Participants stated that health data could be misused and were greatly concerned about data privacy protection.

Participants want to authorize themselves who can view health data and health expenditures. Regarding the storage of health information in digital environment, the participants generally stated that they found the health information stored in digital environment and digital media reliable. Participants stated that they found this information useful by health institutions and doctors for their own treatments. The majority of the

participants stated that the state is responsible for ensuring the security of health data and that all rights regarding health data belong to them. Although the rate of participants who state that health data is special personal data is quite high, the rate of participants who know that their personal data is protected and who know what to do in case of data breach is not as high. When the findings obtained as a result of the study were evaluated, it was found that the awareness of individuals working in the health sector about personal health data was high, while the awareness increased with the increase in the education level of the other participants.

Keywords: MIS, Information Security, Personal Health Data, Digital Health Data, Health Data Awareness and Expectations

İÇİNDEKİLER

TABLOLAR LİSTESİ

Adı **Sayfa**

GRAFİK LİSTESİ

Adı **Sayfa**

KISALTMALAR LİSTESİ

SB	Sağlık Bakanlığı
YBS	Yönetim Bilişim Sistemleri
ESK	Elektronik Sağlık Kayıtları
KESK	Kişisel Elektronik Sağlık Kayıtları
KVKK	Kişisel Verilerin Korunması Kanunu
USVS	Ulusal Sağlık Veri Sözlüğü
USBS	Ulusal Sağlık Bilgi Sistemi
MHRS	Merkezi Hastane Randevu Sistemi
SKRS	Sağlık Kodlama Referans Sözlüğü
BGYS	Bilgi Güvenliği Yönetim Sistemleri
KPS	Kimlik Paylaşım Sistemi
AFK	Away From Keyboard (Klavye Başında Değilim)

1. GİRİŞ VE AMAÇ

Hızla gelişen bilgi ve iletişim (bilişim) teknolojilerinde kaydedilen gelişmeler, tüm alanlarda olduğu gibi sağlık sektörünü de önemli derecede etkilemektedir. Bilişim teknolojilerindeki gelişmelerle birlikte sağlık alanında önemli değişimler ve dönüşümler yaşanmıştır. Dokümantasyon ve veri paylaşımı konusundaki gelişmelerin sağlık uygulamalarındaki etkisi bütün ülkelerde öne çıkmaktadır. Bilişim teknolojileri, sağlık verilerinin ve bilgi birikiminin yayınlanmasını, paylaşılmasını ve bilgiye ulaşmayı kolaylaştırmakta, klinik karar verme aşamalarında sağlık çalışanlarına destek sağlamaktadır. Bilişim teknolojileri hekimlerin diğer sağlık profesyonelleri ile olan çalışmalarını destekleyip bilgi paylaşımını hızlandırmaktadır. Bu nedenle, sağlık hizmetlerinde kişisel verilerin toplanması, korunması ve değerlendirilmesi gittikçe yaygınlaşmaktadır.

Türkiye'de, Elektronik Sağlık Kayıtları (ESK) ve Kişisel Elektronik Sağlık Kayıtları (KESK) ile ilgili ilk çalışmalar, 2003 yılı başında T.C. Sağlık Bakanlığı tarafından kamuoyuna duyurulan Sağlıkta Dönüşüm Programı kapsamında başlamıştır.

ESK sistemi, kişilerin, geçmiş ve şimdiki fiziksel ve ruhsal sağlık durumlarıyla ilgili tüm bilgilerin bilgisayar ortamında toplanmasını, kayıt altına alınmasını, saklanmasını, iletilmesini, erişilmesini, ilişkilendirilmesini, işlenmesini ve gerektiğinde kullanılmasını sağlayan sistemdir. ESK, hastalara ait KESK'nı, etik ve yasal kurallara uygun, zaman içerisinde elde edilen tüm kayıtların bütünlüğünü sağlayabilen, gizliliğini koruyan bir sistem olmalıdır.

Sisteme kayıt edilen bu bilgiler, farklı kurumlar arasında da paylaşılmakta, hastalara ait bilgilere birçok kişi tarafından erişilmektedir. Bu erişimler sağlanırken verinin gizliliği ve güvenliğine önem verilerek ele alınmalıdır. Özellikle "hassas veri" olarak adlandırılan sağlık verilerinin hukuka aykırı bir biçimde ele geçirilmesi, işlenmesi veya paylaşılması ayrımcılık başta olmak üzere kişinin bilgilerine göre ilgili kişi bakımından daha ciddi

zararlara yol açmasına sebep olabilmektedir. Bunun beraberinde bu bilgilerin paylaşılması kişinin özel hayatının gizliliği, hastanın mahremiyet hakkının korunmasına ve doktorun hastasına karşı sır saklama yükümlülüğünün ihlal edilmesine sebep olmaktadır.

ESK sistemleri tasarlanırken, kişisel sağlık verilerine ilişkin yönetim yetkisi yalnızca kişilerin kendisinde olmalı ilkesi temel alınmalı, kişiler dilerse verilerini aile hekimleriyle, muayene oldukları başka bir hekimle, aile bireyleriyle veya başkalarıyla diledikleri gibi paylaşabilmeli, istediği verileri sistemden silebilmelidir. KESK bilgileri, kendi onayları olmaksızın veya yargı kararı ve/veya yasal bir yükümlülük söz konusu olmadığı sürece herhangi bir üçüncü şahıs, kurum veya kuruluşla hiçbir koşulda paylaşılmamalıdır.

Türkiye'de kullanılan ESK sistemlerinin en önemli paydaşlardan sağlık profesyonelleri ve hastalar gerek tasarım ve gerekse işletim süreçlerinden dışlanmaktadır. ESK'lar ile ilgili yapılan çalışmaların büyük bir kısmında sistemin teknik yapılarına ve hekim görüşleri üzerinde durulmaktadır (Öğütçü, 2011). Aslında hastaların kendi ESK'larının hassasiyeti ve güvenliği konusundaki farkındalık ve beklentileri sistem güvenliğinin temel unsurlarından biri olmalıdır.

Bu tezde, Türkiye Cumhuriyeti vatandaşlarının sayısal sağlık kayıtları hakkında bilgi düzeylerinin, beklentilerinin ve farkındalıklarının belirlenmesi için anket yöntemi ile nicel bir araştırma yapılmıştır.

Tezin ikinci bölümde sayısallaşma, sayısallaştırma, sayısal veri, kişisel veriler, mahremiyet, ve anonimleştirme gibi temel kavramlar ele alınmış ve Üçüncü bölümde Türkiye'de kişisel veriler kapsamında hastane ortamlarında bulunan dijital sağlık kayıtlarının yasal durumu incelenmiştir. Hastane Bilgi Yönetim Sistemlerinin çalışma şekilleri ve standartları hakkında bilgi verilmiştir.

Türkiye'de bulunan hastane bilgi sistemleri işleyişleri ele alınmış ve hasta bilgilerine erişim modellenmiştir.

2. GENEL BİLGİLER

Her sektörü ve alanı etkisi altına alan dijitalleşme ve dijital teknolojilerin yaygınlaşması kişisel verilerin dahi artık dijital ortamlarda kayıt altına alınması sebebiyle hayatımıza sayısallaştırma (Dijitalleştirme) ve Sayısallaşma (Dijitalleşme), Sayısal (Dijital) Veri, kişisel veriler, veri güvenliği, veri anonimleştirme, siber güvenlik gibi popüler ve araştırılıp geliştirilmeye devam eden konular ve terimler girmiştir.

2.1. Sayısallaştırma (Dijitalleştirme) ve Sayısallaşma (Dijitalleşme)

Sayısal veri (dijital veri) ve ondan türetilmiş sayısallaştırma (dijitalleştirme) ve sayısallaşma (dijitalleşme) kavramları sıklıkla birbiri yerine kullanılan ve karıştırılan iki farklı terimdir. Kavram kargaşasının önüne geçmek adına bu terimlerin tanımlanması gerekmektedir.

Sayısallaştırma (digitalization), analog bilgilerin elde edilip, bilgisayar mantığıyla (0-1) kodlanması anlamına gelmektedir. Böylece bilgisayarlar sayısallaştırılmış veriler (data)'ı depolayabilmektedir. Sayısallaştırma sayesinde günümüzde bilgi bilgisayar ortamlarında depolanabilmekte, istenildiği zaman istenilen ortamdan ulaşma kolaylığı ve sınırsız depolama fırsatı sunmaktadır. Bu gelişim ve dönüşüm, bilginin paylaşılabilirliğini ve erişebilirliğini kolaylaştırmaktadır (Bloomberg, 2018).

Bir dizi çalışmanın ardından yapılan değerlendirmeler göstermektedir ki bilginin sayısallaştırılıp, sayısal (digital) ortamlardan erişilebilir hale gelmesi bilgiyi kullanan bireyler ve örgütler için üretkenliği arttırmaktadır (Greenstein ve Ark., 2013).

Sayısallaşma (digitization) bir değişim sürecidir. Bilgi sayısallaştırılırken nasıl analog bilginin alınıp, bilgisayar çalışma mantığı ile kodlanması olarak tanımlanıyorsa, sayısallaşma da sayısallaştırılmış analog bilgilerin sayısal formlara dönüştürülerek dijital ortamlarda işlenilebilir hale getirilmesidir (Bloomberg, 2018).

Sayısallaştırma, bilginin dinamik bir şekilde saklandığı depodur. Günümüzde bilgiye erişmek isteyen kullanıcı sayısı her geçen gün artmaktadır. Sayısallaşma bilgiye erişmek isteyen kullanıcılara erişim fırsatı sağlarken bir yandan da erişilen bilgiye çok kısa sürede ve zahmetsiz bir şekilde ulaşma imkanı sağlamaktadır (Maurya, 2012).

Günümüzde çeşitli sektörlerde yer alan örgütlerin büyük bir çoğunun büyüklüğü ve gücü sayısallaşma oranları ile ölçülmektedir. Birçok araştırmaya göre örgütler hayatta kalıp, faaliyetlerine devam etmek istiyorlarsa sayısallaşmaya evrilmeleri gerekmektedir (Ritter ve Pedersen, 2020).

2.2. Sayısal (Dijital) Veri

Sayısal (Dijital) Veri, tüm farklı biçimde olan veri türlerini makinalar tarafından okunabilir olarak sayısallaştırılmış bir şekilde işlenmesiyle ortaya çıkan ve sayısal ortamlarda kayıt edilip, depolanabilecek şekle dönüştürülmüş verilere denilmektedir. Sayısal verilerin büyük bir kısmı kasıtlı olarak dijital ortamlarda üretilmektedir. Büyük miktarda veriler bireylerin sosyal medya uygulamaları gibi dijital ortamlara kişisel inisiyatif ve istekleri doğrusunda verdikleri bilgilerden oluşmaktadır. Dolayısıyla kişiler gün içerisinde dijital ortamlara erişim sağladıklarında kişisel bir çok verisini sayısal veri olarak bu ortamlara aktarmaktadır (Selwyn, 2015).

Sayısal verinin popülerliği ve kullanımı her geçen gün artmaktadır. Parmak izi gibi kişisel her türlü bilgi dijitalleştirilmekte olup, dijital ortamlarda kayıt altına alınmaktadır (Boneh ve Shaw, 1998). Dijital ortamda oluşturulan, çoğaltılan, aktarılan her türlü bilgi dijital evreni oluşturur. Dijital evren her geçen gün büyümekte ve artık her türlü veriye dijital ortamlardan erişilebilmektedir. Bankacılık, sağlık, eğitim gibi sektörlerde kişisel verilerin neredeyse tümü dijital ortamlarda kayıt altına alınmaktadır (Gantz ve Reinsel, 2012).

Dijital ortamda oluşan, çoğaltılan, aktarılan her türlü bilgi dijital evreni oluşturur. Dijital evren her geçen gün büyümekte ve artık her türlü veriye dijital ortamlardan

erişilebilmektedir. Bankacılık, sağlık, eğitim gibi kişisel verilerin neredeyse tümü dijital ortamlarda kayıt altına alınmaktadır.

Sayısal teknolojilerin gelişimi günümüzde bireyleri, örgütleri, toplumları ve devletlerin yaşam ve yönetim biçimlerini değiştirip, doğrudan etkilemiştir. Sayısal veri bireylerden, devletlere kadar her kullanıcının işini kolaylaştırmanın yanı sıra sayısal verinin güvenliğinin sağlanması konusu, sayısal verinin saklanmaya ve kayıt edilmeye başladığı günden itibaren içinde bulunduğumuz çağın en büyük tartışma konularından biri olmuştur (Ritter ve Pedersen, 2020).

2.3. Kişisel Veri

Kişisel veri, bir bilginin kimliği belirli gerçek kişi ile ilişkili veya ilişkilendirilebilir her türlü bilgi olarak kabul edilmektedir. Kişisel veriler oldukça geniş bir yelpazeye sahiptirler. Kişisel veri kapsamında en önemlileri kanunlar ve yasalar ile güvence altına alınmış kişilerin özlük, sağlık bilgisi gibi mahremiyet içeren bilgileridir. Dijitalleşen ve kişisel verilerin dijital ortamlarda kayıt altına alınıp işlenmesiyle kişisel verilerin güvenliği ve korunması tüm dünyada tartışma konusu olmuştur (Knight, 2017).

Yaşadığımız çağda en büyük ekonomik getiri sağlayan bilgiler kişisel verilerdir. Dolayısıyla kişisel verilere ulaşabilen şirketler elinde bulundurdukları kişisel verileri kurumsal varlıkları olarak görmektedirler. Kişisel veriler bu yüzden çoğu sektörde ticari mal olarak geçmekte ve ticareti yapılmaktadır. Kişisel verilerin, kullanımı, aktarımı ve işlenmesini düzenleyen sosyal ve yasal normların kapsamı her geçen gün genişletilmeye ve gündem konusu olmaya devam etmektedir (Schwartz, 2003).

2.4. Kişisel Veri Gizliliği ve Güvenliği

Verilerin dijital ortamlarda kaydedilmesi ile birlikte en önemli tartışma konularından birisi de kişisel verilerin gizliliği ve güvenliği olmuştur. Bu konu için tüm devletler ulusal ve uluslararası çalışmalar gerçekleştirmiş ve gerçekleştirmeye devam etmektedirler (Chik, 2013).

OECD (Ekonomik Kalkınma ve İşbirliği Örgütü) ülkeleri gizlilik ihlalleri konusunda özel yönergeler ve araştırmalar yayınlamıştır. Bu araştırmalarda kişisel veriler ile ilgili hukuk sistemlerin kısıtlamalar üzerinde durulmuştur. Dolayısıyla OECD toplantılarında bile yer alan kişisel veriler ve bu verilerin korunması, gizliliği ve güvenliği devletler açısından ekonomik olarakta büyük bir öneme sahiptir (O'Leary ve Ark., 1995).

Kişisel veriler, gizlilik düzenlemesinde merkezi bir kavramdır. Kişisel veri gizliliği terimi bir çok gizlilik yasasının sınırlarını ve kapsamını tanımlamaktadır. Kişisel olarak tanımlanan her türlü veri gizlilik ilkeleri kapsamında değerlendirilebilir (Schwartz, 2014).

Kişisel verilerin erişimi ticari avantajların yanında verilerin sahiplerine kötü niyetli kişi veya kurumların eline geçmesi halinde büyük tehditler oluşturmaktadır. Bu tehditlerin oluşmasına sebep olacak verilerin başında sağlık verileri gelmektedir. Mahremiyet kavramının içinde bulunan kişisel sağlık verileri, kişinin işvereninden, sosyal ortamlarına, çalıştığı bankalardan, sigorta şirketlerine kadar bir çok ortamda olumsuzluklar ortaya çıkarabilmektedir. İşverenler bu bilgiler sayesinde personel seçim kararlarını değiştirebilirler. Bireyler sosyal çevrelerinde sorunlar yaşayabilirler. Bankalar sağlık sorunlarının olduğunu gördükleri müşterilerine kredi hizmeti vermek istemeyebilir. Sigorta şirketleri sağlık sorunları bulunan bireylere yüksek ücretli sigorta fiyatları sunabilmektedir. Dolayısıyla mahremiyet içeren kişisel veriler, kanunlar ve yasalar kapsamında korunmak durumundadır (Schwartz, 2003).

Sağlık alanında kişisel verilerin her geçen gün artması ve işlenmesi riskleri beraberinde getirmektedir. Bireyler her saniye veri üretmektedir. Sağlık verilerini dijital ortama taşımak ve bu ortamlarda kaydetmek için sadece bireylerin sağlık kuruluşlarına gitmesine ve verilerin bu kuruluşlarda kayıt altına alınmasına gerek olmamaktadır. Günümüzde akıllı cihazlar (Tablet, saat, telefon), giyilebilir teknolojinin kullanımı kişisel sağlık verisinin dijital ortamlarda artmasını sağlamaktadır. Dolayısıyla günümüzde bu cihazların her biri gizlilik ve güvenlik yasalarından sorumlu tutulmaktadır. Kullanıcılar cihazları kullanmaya başlamadan önce kullanım risklerine ait sözleşmeleri onaylamaktadırlar (Calvaresi ve Ark., 2020).

2.5. Veri Anonimleştirme

Veri anonimleştirmenin temel amacı, bilimsel olarak fayda yaratabilecek verilerin, gizliliğini koruyarak yayınlanması ve işlenmesini sağlamaktır (Lasko, 2009).

Ülkeler, sektörler, kuruluşlar tarafından en önemli bilgi kaynaklarından olan kişisel veriler bireylerin mahremiyetleri için gizlilik ve koruma kanunları ile korunma kapsamına alınmıştır. Bazı veriler özellikle sağlık verileri gibi bilimsel, ekonomik, politik çalışmalara konu olabilecek kişisel veriler anonimleştirilerek, yani kişisel verinin, kişi kimliğinden ayrıştırılarak anonim hale getirelerek kullanılması ve yapılacak bu çalışmalar için veri olarak kullanılması sağlanır (Bayordo, 2005).

2.6. Sağlık Bilişiminde Siber Güvenlik

Güvenlik: Kişilerin, kurumların, devletlerin maddi ve manevi sahip olduğu her şeye karşı yapılan ve yapılmaya çalışılan saldırı ve tehditler için alınacak önlemlerdir (Yılmaz, Halil ve Gönen, 2015). Siber güvenlik ise; sayısal ortamlardan yapılan çeşitli saldırı ve tehditlere karşı bilgi teknolojilerinin gizliliğini, bütünlüğünü, kullanılabilirliğini ve erişimini koruyan stratejiler ve çalışmaların bütünüdür. Gizlilik, bilgilerin ve belgelerin erişim izni

olmayan bireyler ve sistemlere karşı ulaşılmaz konuma getirilmesidir. Ulaşılabilirlik ise bilgi paylaşımı, depolama ve bilgi işleyen sistemlerin erişime açılması ve ihtiyaç duyan yetkililer tarafından gerektiği zaman erişilebilir konumda bulunmasıdır (Jackard ve Nepal, 2014). Siber güvenliğin ihlalinde ortaya çıkan tüm tehdit ve saldırılar ise siber saldırı kapsamına alınmaktadır. Kavram olarak tanımlandığında ise siber saldırı; başka bir kimsenin, kuruluşun, kurumun, devletin sistemine, ağlarına, erişim izni olmadan girmek; gizlilik, bütünlük ve ulaşılabilirliği yok etmektir bu bağlamda dünyanın her yerinde meydana gelen siber saldırılar; finans, sağlık, savunma, bilişim, gıda gibi birçok bireyin ihtiyaç duyduğu ve dahil olduğu sistemlere yapılmıştır (Hathaway ve ark., 2012). Siber saldırıların kaynağına ilişkin yapılan bir çalışmada ise; sağlık organizasyonlarına yönelik yapılan siber saldırıların %38'inin çevrimiçi dolandırıcılardan, %21'inin örgüt içi bireylerden ve %21'inin ise hackerlardan kaynaklandığı belirtilmiştir (HIMSS North America, 2018). Bir başka çalışmada ise siber saldırıların uğradığı sistemlere erişimin kolay olmasının nedeninin; medikal amaçlı kullanılan teknolojik cihazlar üretilirken sistemlerinde güvenlik yazılımlarının bulunmasına gerek duyulmaması olduğu belirtilmiştir (Ayala, 2016). Bu açıkların oluşmasının temelinde ise ülke sağlık politikaları ve sağlık bilişimi yazılım gereksinimleri hazırlanırken değerlendirilme ve planlama aşamalarında siber güvenlik konusunun göz ardı edilmesidir (Kruse, Frederick, Jacobson ve Monticone, 2017).

Walters tarafından siber saldırıya maruz kalmış büyük projelerden bazı örnekler sunulmuştur. Bir çevrimiçi sağlık portalı olan "Alliance Health" şirketinde sağlık sektöründe destek ve bilgi alışverişini sağlayan, yüzbinlerce kişinin kullandığı ve milyonlarca üyesi bulunan çevrimiçi platforma yapılan saldırı sonucunda binlerce kişinin sağlık bilgileri ifşa edilmiştir. "Banner Health" isimli şirkette ise 4 milyon doktor ve hastanın etkilendiği siber saldırıda ilk olarak ödeme ekranını barındıran sisteme saldırılmış ve sonrasında yetkisiz erişim ihlali ile hastaların kişisel bilgileri ele geçirilmiştir (Walters, 2014).

3. LİTERATÜR TARAMASI

Literatürlerde dijital sağlık verileri ile ilgili sayısız çalışma bulunmaktadır. Şüphesiz bunda en büyük etki popülerliği her geçen gün artan dijital veri ve sağlık verisi konularının çağımızın popüler çalışma konularından olmasıdır. Literatürde yapılan çalışmalardan dijital sağlık verileri ile ilgili en fazla dijital sağlık verilerinin güvenliği, dijital sağlık verilerinin korunması konuları üzerinde durulmuştur.

Safran ve arkadaşları tarafından 2007 yılında yapılan çalışmada kişisel sağlık verilerinin ikincil kullanımından bahsedilmiştir. Başka bir ifade ile sağlık verilerinin hastalık tedavisi dışında kullanıldığı alanlardan bahsedilmiştir. Bu alanlar; bilimsel araştırmalar, kalite ve güvenlik ölçümleri, halk sağlığı ödemeleri, pazarlama ve ticaret faaliyetleri gibi çeşitli alanlardır. Veriler anonimleştirildikten sonra bu alanlarda kullanılmasında hukuksal olarak bir engel bulunmamaktadır. Yapılan araştırmalar sonucunda kişisel sağlık verilerinin ticari değerinin milyonlarca dolarlarla ifade edileceği ortaya çıkmaktadır. Dolayısıyla sağlık verilerinin ikincil kullanımı ile ilgili çalışmada, veri sahipliğinden ziyade veriyi yönetmeye ve veriyi işlemeye odaklanmanın doğru olduğu, kişisel sağlık verilerinin güvenliği ile ilgili kamu bilinci ve güveni oluşturmanın gerekliliği görülmüştür.

Archer ve arkadaşları tarafından 2011 yılında yapılan, kişisel sağlık kayıtları kapsamının belirlenip incelenmesi ile ilgili bir çalışma yapmışlar. Amerika ve Kanada merkezli yapılan çalışma sonucunda dijital sağlık kayıtlarının doktor merkezli tutuldukları ve takibe alındığını ortaya koymuşlardır. Hastalar, doktora veya sağlık kuruluşlarına gittiklerinde sağlık verilerinin oluştuğu ortaya çıkmıştır. Ancak bu verilerin hastaların sağlıklarının olumlu yönden etkilenmesi ve doktorların işlerinin kolaylaşması için güvenliği sağlanmış portallar oluşturularak bu dijital ortamlar üzerinden sürekli sağlık kayıtlarını güncelleyebilmelerinin daha doğru kişisel ve toplumsal sağlık verilerine ulaşılacağı savunulmuştur.

Öğütçü ve arkadaşları tarafından 2011 yılında yapılan elektronik sağlık kayıtlarının içeriği, hassasiyeti ve erişim kontrollerine yönelik farkındalık ve beklentilerinin değerlendirilmesi adlı çalışmada, Elektronik sağlık kayıtlarına ilişkin bilincin tam olarak oluşmadığı, elektronik sağlık kayıtlarına ilişkin en büyük endişenin bu kayıtlara erişim konusunda duyulduğu ortaya çıkmıştır. Çalışma sonucunda ortaya çıkan bir başka sonuç ise hasta ve doktorların sağlık alanında teknolojinin kullanımı konusunda ki beklentilerinin oldukça yüksek olmasıdır.

Özkan tarafından 2011 yılında yapılan çalışmada elektronik sağlık bilgilerinin gizliliği ve mahremiyeti konusu ele alınmıştır. Çalışma sonucunda, çalışmaya katılan bireylerin, sağlık hizmetlerinde bilgisayar kullanımı ile ilgili bir endişelerinin olmadığı, fakat bilgilerinin güvenliğinin sağlanıp, sağlanmadığı konusunda kararsız oldukları ortaya çıkmıştır. Çalışmada ortaya çıkan bir başka sonuç ise katılımcıların doktorlarına, hemşirelerine, eczacılarına ve diğer sağlık çalışanlarına güvendiklerini ancak sigorta şirketleri, devlet, özel sektör sağlık araştırmacılarına, bilgisayar sistemlerini yöneten uzmanlara güvenmediklerini ortaya koymuştur.

Spencer ve arkadaşları tarafından 2016 yılında yapılan çalışmada dijital sağlık kayıtlarının anonimleştirilerek kullanılmasının her geçen gün arttığının ve çeşitli araştırmalarda kullanmak için büyük bir fırsat olarak görüldüğü söylenmiştir. Bununla birlikte verilerin uygunsuz kullanımına ilişkin kamuoyu endişelerinin göz önünde bulundurulması gerektiğine dikkat çekmişlerdir. Hastaların dijital sağlık kayıtlarına kimlerin ulaşacağına kendilerinin karar vermesini daha etik ve güvenilir olduğunu savunmuşlardır.

Eleni Entzeridou ve arkadaşları tarafından 2018 yılında yapılan çalışmada elektronik sağlık kayıtlarının etik kaygıları üzerinde durulmuştur ve elektronik sağlık kayıtlarının risklerinin, faydalarından daha ağır bastığı savunulmuştur. Çalışmada Hekimlerin ve sağlık kayıtları oluşan hastaların elektronik sağlık kayıtlarının etik endişeleri ile ilgili beklenti ve

farkındalıkları araştırılması planlanmış ve bunun ile ilgili bir anket çalışması yapılmıştır. Demografik soruların yanında sağlık kayıtlarının etki, algılanan riskler ve etik sorunları ile ilgili kapalı uçlu sorular sorulmuştur. Yapılan anket çalışmasının sonucunda halkın %46'sı hekimlerin ise %91'i Dijital sağlık kayıtlarının risklerinin farkında olduğu ortaya konmuş. Katılımcıların büyük bir çoğunluğu kişisel sağlık verilerinin üçüncü şahısların eline geçtiği takdirde büyük endişe duyacaklarını belirtmişlerdir. Hastalar ve hekimler, kişisel sağlık kayıtlarının gizliliği ve güvenliğinin sağlanması koşuluyla elektronik sağlık kayıtlarının faydasını kabul ettikleri ve destekledikleri görülmüştür.

Juha Häikiö ve arkadaşları tarafından 2020 yılında yapılan çalışmada sağlık sektörü şuanda dijital sağlık verileri ile daha aktif bir hizmet sağladığı savunulmuştur. Çalışmada kişisel veriler ile ilgili beklentileri ve değerleri hizmet sağlayıcıları ve bireysel kullanıcılar açısından incelemiştir. Çalışma görüşme yolu ile toplanan ampirik materyal analizine dayanmaktadır. Kişisel sağlık verileri ile ilgili güvenlik endişeleri olduğu görülse de hizmet sağlayıcı yani verilerin saklanmasında ve kayıt edilmesinde rol oynayan kurumlar yapılan araştırmada güvenilir bulunmuştur. Çalışma sonucunda kişisel sağlık verilerinin potansiyel faydalarına erişmek için güvenilirliği arttırmak ve veri güvenlik endişelerinin giderilmesi gerektiği ortaya çıkmıştır.

4. SAĞLIK HİZMETLERİNDE KİŞİSEL VERİ TOPLANMASI, KORUNMASI VE DEĞERLENDİRİLMESİ

Hızla gelişen teknoloji, dünya genelinde hızla artan küreselleşme, bilgi ve iletişim (bilişim) teknolojilerinde kaydedilen gelişmeler, tüm alanlarda olduğu gibi sağlık sektörünü de önemli derecede etkilemektedir. Bilişim teknolojilerindeki gelişmelerle birlikte sağlık alanında önemli değişimler ve dönüşümler yaşanmıştır. Dokümantasyon ve verilerin paylaşımı konusundaki gelişmelerin sağlık uygulamalarındaki etkisi bütün ülkelerde öne çıkmaktadır. Bilişim teknolojileri, sağlık verilerinin ve bilgi birikiminin yayınlanmasını, paylaşılmasını ve bilgiye ulaşmayı kolaylaştırmakta, klinik karar verme aşamalarında sağlık çalışanlarına destek sağlamaktadır. Bilişim teknolojileri hekimlerin diğer sağlık profesyonelleri ile olan çalışmalarını destekleyip bilgi paylaşımını hızlandırmaktadır. Bu nedenle, sağlık hizmetlerinde kişisel verilerin toplanması, korunması ve değerlendirilmesi gittikçe yaygınlaşmaktadır.

Özel ya da kamu sağlık kuruluşlarında hastaların sağlık geçmişine ilişkin bilgiler, tahlil sonuçları, kendilerine konulan tanılar, tedavileri ve bunların süreleri sayısal ortamda yer almaktadır (Dülger, 2015) Hastaların geçmişteki tanı ve tedavilerine hekimlerin ulaşabilmesi yeni tanıların doğru bir şekilde konulmasını, müdahalenin daha çabuk ve daha az riskli gerçekleştirilmesini sağlayabilir. Sağlık alanında yapılan araştırmalarda da hasta bilgilerinin ulaşılabilir olması önemli yarar sağlar. Ancak diğer yandan kişinin sağlık durumuna ilişkin bilgiler bir hayli kişiseldir. Bu tür hassas veriler için konuya ilişkin hukuksal metinlerde yüksek düzeyde koruma öngörülmektedir (Küzeci, 2019). Kişiler bu tür verilerinin gizli tutulmasını isteyebilirler. Zira bu bilgiler dolayısıyla kişiler tehdide maruz kalabilirler, sevdikleri tarafından terk edilebilirler, işlerinden kovulabilirler, sosyal ayrımcılığa uğrayabilirler, sigorta hizmetine erişimde sorun yaşayabilirler (Başalp, 2015).

Bu tür kişi üzerinde baskı ve korku oluşturabilecek durumlar kişiler üzerinde korku ve baskı ile sınırlı kalmayabilir, kişiler sağlık hizmeti almaktan çekinebilirler ve böyle bir durum gerçekleştiği takdirde kişilerin yaşamlarına yönelik büyük bir risk söz konusu olabilir (Başalp, 2014).

Hastalar tedavi süreleri boyunca gerek hekimlere gerekse sağlık kurumu çalışanları ve kurumlara kendileri ile ilgili pek çok bilgi vermek durumundadırlar. Ayrıca yine aynı bağlamda kişiye uygulanan tedavi, tetkik, operasyonlar aracılığıyla ortaya çıkan veriler de hekimlerin ve sağlık kurumlarının kontrolüne geçmektedir. Hekimlerin hastalarının bilgilerini gizli tutması, mesleki değer ve etik bir vazife olarak görülmesine rağmen, teknoloji gelişmeler ve dijitalleşmenin etkisiyle "sır saklama" yerine getirilmesi güç bir sorumluluk haline gelmiştir. Günümüzde artık hastalara ait sağlık verileri sadece hekimlerin elinde bulunmamaktadır. Sağlık hizmetlerinin, sağlık kurumlarında ekiplerce verilmeye başlanmasının ardından, sağlık verileri sistematik bir biçimde dijital ortamlarda kayıt altına alınmaya başlamıştır (Çobanoğlu, 2010). Sağlıkta gizliliği korumanın en temel yöntemi hasta mahremiyeti ve gizliliğini bir hasta hakkı olarak gören sağlık kurumu çalışanlarının olmasıdır. Bütün seviyelerdeki sağlık çalışanları bu hususta sorumluluk taşımaktadırlar (Arslan, Demir, 2016). Hastalarla ilgili sağlık kayıtları ancak doğrudan ilgili kişiler görebilirler; harici sağlık personellerinin dahi başka kişilerin görmesi bu bilgilere ulaşmasının mümkün olmaması sağlanmalıdır (Dülger, 2015).

4.1. Sağlık Bilişiminin Tarihsel Gelişimi

Sağlık ve teknoloji günümüzde tüm dünya ülkelerinde hızla büyüyen, devletler tarafından yapılan ekonomik yatırımların çok fazla olduğu iki temel sektördür. Teknolojik gelişmelerle her geçen gün bilgiyi oluşturan verilerin çoğalmasıyla beraber, bilgi sistemleri günümüzde birçok sektörde kullanılmaya ve aktif rol almaya başlamıştır; bu tercihin

artmasındaki en büyük etken ise bilgi sistemlerinin bilgiyi erişilebilir hale getirmesi ve istenildiği her zaman bilgiye ulaşılmasına olanak vermesidir.

Teknolojik gelişmelere paralel artan bu veri yoğunluğuyla birlikte sağlık sektöründe de var olan servisleri daha etkili ve ekonomik bir biçimde sağlayabilen bilişim sistemlerine yer verilmeye başlanmıştır (Karaarslan ve ark., 2015). Buna paralel bir şekilde sağlık sektöründeki hızlı büyüme de bilişim teknolojilerinin bu sektörde de kullanımını zorunlu hale getirmiş ve E-sağlık sistemleri ortaya çıkmıştır (Gül ve ark., 2016). E-sağlık sistemlerini tanımlayacak olursak temelde; tıbbi bilişim, halk sağlığı ve iş dünyasının kesişiminde yer alan internet ve ilgili teknolojiler aracılığıyla sunulan veya geliştirilen sağlık hizmetleri ve bilgilere atıfta bulunan yeni bir alan olarak öne çıkmaktadır. Daha ayrıntılı ifade etmek gerekirse; e-sağlık sistemleri yalnızca bir teknik bir gelişimi değil aynı zamanda düşünce biçimi ve tutum değişikliğine neden olmakta ve sağlık hizmetini yerel, bölgesel ve dünya çapında iyileştirmek için bilgi ve iletişim teknolojisini kullanarak ağa ve küresel düşünmeye yönelik bir bağlılığı karakterize etmektedir (Eysenbach, 2001).

E-sağlık sistemindeki gelişmelere paralel olarak gelişen alanlardan biri olan Hastane Bilgi Yönetim Sistemleri (HBYS) ise bir hastanenin tüm adımlarını idare edebilmek adına oluşturulmuş bütünleşmiş bir bilgi sistemidir (Ahmadi, İbrahim ve Nilashi, 2015). Hastane yöneticilerinin karar destek sistemlerini en etkin şekilde kullanması ve bilgiyi en iyi şekilde değerlendirmesi açısından HBYS içerisinde bulundurduğu modüllerle hem hastane yöneticilerine hem de sağlık çalışanlarına karar destek ve iş akışı açısından büyük kolaylıklar ve farklı olanaklar sağlamıştır (Yaldır ve Taşer, 2016).

Eylül 1967'de Prof. Dr. İhsan Doğramacı, Aydın Köksal'a bölgeyi Center of Excellence (Yetkinlik Merkezi) ve Bilgisayar Bilimleri Merkezi yapmak istediğini göstermiş ve "Günümüzde HBYS olarak adlandırılan Hastane Bilgi Yönetim Sistemleri işleyişini, bütün hastaların bilgilerini Bilgisayar Bilimleri Merkezinde tutacağız." diyerek

Amerika'da yeni yeni işlemeye başlayan merkeze Aydın Köksal'ı göndererek incelemeler yaptırmıştır. Ülkemizde temelleri 1967'den de önce atılmaya başlanan sağlık bilişimi bu örnekte de gördüğümüz gibi geçmişte ve günümüzde ülkelerin büyük araştırmalar yaptırıp büyük bütçeler ayırdığı bir alandır (Ak, 2009).

Türkiye'de bu sürece geçişte ise; Sağlık Bakanlığı'nın Dünya Bankası ile olan ortak çalışması sonucunda HBYS çalışmalarının başlaması önemli bir adımdır (Ak, 2009). HBYS'nin geçmişten günümüze kullanımındaki en önemli tartışma noktası ise; verilerin ve bilgilerin güvenliği ile ilgili endişeler olmuştur.

4.2. Elektronik Sağlık Kayıtları

T.C. Sağlık Bakanlığı, elektronik sağlık kayıtları (ESK)'nı, "Kişilerin fiziksel ve ruhsal sağlığı veya hastalıkları ile ilgili elektronik sistemler kullanılarak kayıt altına alınan, saklanan, iletilen, erişilen, ilişkilendirilen ve işlenen her türlü bilgi olarak tanımlamaktadır. Elektronik hasta kayıtları, hasta hakkında tüm bilgilerin bilgisayar ortamında toplanmasını ve gerektiğinde kullanılmasını sağlayan bir bilgi deposudur. Bu sistemler hastalara ait elektronik sağlık kayıtlarının faydalı, etkili, etik ve yasal kurallara uygun, kolayca iletilebilen, zaman içerisinde elde edilen tüm kayıtların bütünlüğünü sağlayabilen bir sistemdir" şeklinde tanımlamaktadır.

ESK sistemleri birbirleri ile yakından ilişkili olan; sağlık bilgisinin toplanması, saklanması, işlenmesi, iletişimi, güvenliği ve sunulması işlevlerinden oluşur. Sistem; genelde hastaların kimlik bilgilerini, hastalığının sınıflamasını, demografik faktörler çerçevesinde kayıtların indekslenmesini içerir. Böylece herhangi bir araştırma ve denetimde kayıtları geri çağırmak mümkündür. Bazı sistemler, bağlı sistem olarak geri çağırma imkânına sahiptir. Bu şekilde hastalık kayıt özetleri acil serviste, ayakta tedavi veren polikliniklerde ve hasta giriş ekranlarında görülebilmektedir. Böyle bir sistemin mahremiyet

(confidentiality), güvenlik (security) izlenebilirlik (accountability) ve veri bütünlüğü (data integrity) özelliklerini sağlaması gerekir.

Bir elektronik hasta kayıt sisteminin taşıması gereken özellikler;

1. Hasta ile ilgili tüm bilgiler tek bir kayıt numarası ile ilişkilendirilmelidir,
2. Sisteme girilen tüm hasta bilgilerine kurumun her yerinden ulaşılabilmelidir,
3. Hastaların yakınmaları ve tüm sağlık bakım süreci kaydedilmelidir,
4. Tanısal süreçlerde bilgisayar yardımı sağlanabilmelidir,
5. Bir bakım planı geliştirilip izlenebilmelidir,
6. Sistem kullanılarak isteklerde bulunulabilmeli ve istek sonuçları otomatik olarak alınabilmelidir,
7. Verilere kolayca erişim ve kullanma olanağı vermelidir.
8. Bir elektronik hasta kayıt sistemi aşağıdaki fonksiyonları da desteklemelidir:
9. Hasta randevuları (muayene, yatış, tetkik vb.),
10. Yönetim fonksiyonları (finansal yönetim, malzeme yönetimi, insan kaynakları yönetimi),
11. Otomatik hastalık ve tıbbi girişim kodlamaları,
12. Tanısal tetkik isteklerin üretilmesi ve iletilmesi.

4.3. Türkiye'de Kişisel Sağlık Verileri Hakkındaki Yasal Düzenlemeler

Kişisel verilerin korunması, Türkiye Cumhuriyeti Anayasası ile teminat altına alınmıştır. Anayasanın "Özel hayatın gizliliği" başlıklı 20/3 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." Hüküm, kişisel verilerin ancak kanunla öngörülen durumlar ve kanuna dayalı düzenlemelerle işlenebileceğini ve kişisel verilerin mutlak korunmasını öngörmektedir.

Ülkemizde Kişisel Sağlık Veriler ile ilgili temel düzenleme 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanununda yapılmıştır. Türkiye'de Elektronik Sağlık Kayıtlarının tutulması, kişisel sağlık verilerine erişim, kişisel sağlık verilerinin gizlenmesi ve düzeltilmesi, imha edilmesi ve aktarılması, kişisel sağlık verilerini bilimsel amaçlarla işleme ve açık sağlık verilerine dönüştürme, sağlık verileri ve bilgilerinin güvenliği T.C. Sağlık Bakanlığının yükümlülüğündedir. Bakanlık kişisel sağlık verileri ile ilgili yürütülen süreç ve uygulamalarda uyulacak usul ve esasları 21 Haziran 2019 tarih ve 30808 sayılı Resmi Gazete'de yayınlanan "Kişisel Sağlık Verileri Hakkında Yönetmelik" ile belirlemiştir. Bakanlık bu yönetmelikte Elektronik Sağlık Kayıtları ve Kişisel Elektronik Sağlık Kayıtları ile ilgili kavramları, süreç ve işlemleri tanımlamıştır.

Yönetmelik, herkesin sağlık durumunun takip edilebilmesi ve sağlık hizmetlerinin daha etkin ve hızlı şekilde yürütülmesi maksadıyla, Bakanlık ile bağlı ve ilgili kuruluşlarınca gerekli kayıt ve bildirim sistemi kurulmasını öngörmektedir. Yönetmelikte kişisel sağlık verisi, kimliği belirli ya da belirlenebilir gerçek kişinin fiziksel ve ruhsal sağlığına ilişkin her türlü bilgi ile kişiye sunulan sağlık hizmetiyle ilgili bilgiler olarak tanımlanmıştır.

Yönetmelik hiç kimsenin, sağlık hizmeti sunumu için gerekli olan durumlar haricinde geçmiş sağlık verilerinin dökümünü sunmaya veya göstermeye zorlanamayacağını belirtmektedir. Yönetmelik, sağlık hizmeti sunucuları tarafından; banko, gişe ve masa gibi bölümlerde yetkisi olmayan kişilerin yer almasını önleyecek ve aynı anda yakın konumda hizmet alanların birbirlerine ait kişisel verileri duymalarını, görmelerini, öğrenmelerini veya ele geçirmelerini engelleyecek nitelikte gerekli fiziki, teknik ve idari tedbirlerin alınmasını zorunlu tutmaktadır. Yönetmelikte sağlık hizmeti sunucularının, tahlil ve tetkik sonuçları gibi hastaya ait kişisel sağlık verilerini içeren basılı materyal üzerinde gerekli kısmî kimliksizleştirme veya maskeleme tedbirlerini uygulaması ve söz konusu materyalin

yetkisiz kişilerin eline geçmesi hâlinde kime ait olduğunun tespit edilmesini zorlaştıracak diğer tedbirlerin alınması gerektiği belirtilmektedir.

Bakanlık yönetmelikte sağlık personelinin, ilgili kişinin sağlık verilerine ancak, verilecek olan sağlık hizmetinin gereği ile sınırlı olmak kaydıyla erişebileceği hüküm altına alınmıştır. Yönetmelik, açık sağlık verisini, ücretsiz olarak veya hazırlanma maliyetini geçmeyecek şekilde internet üzerinden herkesin erişimine sunulan, üzerinde herhangi bir fikri mülkiyet hakkı bulunmayan ve herhangi bir amaçla serbestçe kullanılabilen, makineler tarafından okunabilen ve böylelikle diğer veriler ve sistemlerle birlikte çalışabilen, anonim hale getirilmiş sağlık verisi olarak tanımlamıştır. Yönetmelikte anonim hale getirilmiş kişisel sağlık verilerin, başka verilerle eşleştirilerek dahi hiçbir surette kimliği belirli veya belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hâle getirilmesi zorunlu tutulmuştur.

Sağlık bilişimi alanında faaliyet gösteren tedarikçiler ile tüm kamu ve özel sağlık kurum ve kuruluşlarının uyması gereken kurallar ve sağlık bilişimi konusunda izlenmesi gereken yol haritası, T.C. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü'nün 2015/17 sayılı Sağlık Bilgi Sistemler Uygulamaları genelgesi ile düzenlenmiştir (Türkiye Cumhuriyeti Sağlık Bakanlığı, 2015).

Sağlık. Net Online Sistemi ve bu sisteme bağlı çalışarak, ilgili kişilerin kendilerinin veya yetki verdikleri üçüncü kişilerin sağlık verilerine erişimini sağlayan e-Nabız aracılığı ile kişilerin kendi sağlık durumları ile ilgili bilgi sahibi olmaları, bu bilgiler ışığında sağlıkları ile ilgili kararlara katılmak sureti ile kendi sağlık durumlarını yönetmeleri, tetkik tekrarlarını önlemek suretiyle teşhis ve tedavi sürelerinin kısaltılması ve bütünleşik bir sağlık hizmeti sağlanması hedefi ile T.C. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü 2016/6 sayılı Sağlık. Net Online ve e-Nabız genelgesini yayınlanmıştır (Türkiye Cumhuriyeti Sağlık Bakanlığı, 2016).

4.4. Kişisel Elektronik Sağlık Kayıtları

T.C. Sağlık Bakanlığı, Kişisel Elektronik Sağlık Kayıtları (KESK)'nı, "Elektronik ortamda tutulan, kişilerin geçmiş ve şimdiki sağlık durumlarıyla ilgili bilgileri içeren kayıtlardır. Bu kayıtlarda, sağlık profesyonellerinin gereksinim duyacağı ve görmek isteyeceği tüm bilgiler kronolojik sırada yer alır. KESK, sağlık yönetimindeki gelişmelerin kaçınılmaz ve kritik bir adımını oluşturur. KESK sağlık sorunlarında, tedavi seçeneklerinde, sağlık harcamalarında, kronik hastalıkların yönetiminde, sağlıklı yaşam seçeneklerinin değerlendirilmesinde, koruyucu sağlık hizmetlerinde, sağlık bilgilerinin doğruluğu ve güvenliği konusunda kişinin rolünü güçlendirir. Uygun, güvenilir ve erişilebilir bir şekilde saklanması durumunda kişinin kan grubu, alerjileri, aşıları, geçirmiş olduğu hastalıklar ve ameliyatlar, kullanmış olduğu ilaçlar gibi tüm sağlık bilgileri kişiye hızlı ve doğru teşhis koyabilmeleri ve tedavi uygulayabilmeleri için sağlık profesyonellerine yardımcı olacaktır" diye açıklamaktadır.

Türkiye'de her türlü Kişisel Sağlık Verileri T.C. Sağlık Bakanlığı gözetim ve düzenlemeleri Ulusal Sağlık Bilgi Sistemi (USBS) ile toplanmaktadır. T.C. Sağlık Bakanlığı'nın web sitesinde; USBS'nin, Sağlıkta Dönüşüm Programı'nın temel bileşenlerinden ve uygulamaya koyulan reformların en önemli aşamalarından biri olarak açıklamakta ve USBS'yi şöyle tanımlamaktadır; "USBS tüm vatandaşları kapsayan, her bireyin kendi bilgilerine erişebildiği, bireyin doğumundan önce başlayıp tüm yaşamı boyunca sağlığıyla ilgili verilerden oluşan işlevsel bir veri tabanının, yüksek bant genişlikli ve tüm ülkeyi kapsayan bir iletişim omurgasında 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." (Resmi Gazete, 2019)

Sağlık Bakanlığı, Türkiye'deki e-sağlık uygulamalarının temel bileşenlerinin Merkezi Hastane Randevu Sistemi (MHRS), Tele-Tıp, Ulusal Sağlık Veri Standartları (USVS), Sağlık Kodlama Referans Sözlüğü (SKRS) ve internet üzerinden sunulan çok sayıda servisten oluştuğunu, Sağlık. Net olarak adlandırıldığını açıklamaktadır.

Bakanlık, Sağlık. Net'i;'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 platformu' olarak tanımlamaktadır.

Bakanlık, tüm sağlık kurum ve kuruluşlarında oluşturulan sağlık verilerinin web servisler aracılığıyla online (çevrim içi) toplanmasını, işlenmesini ve veri kalitesinin yükseltilmesini sağlayan sistematik ve işlevsel kayıt sistemi olan e-Nabız uygulaması ile yapmaktadır (Sağlık. Net, 2019).

Türkiye'de Ulusal Sağlık Bilgi Sistemi, dağıtık sağlık bilgi sistemleri arasında birlikte çalışabilirliği sağlamayı amaçlamaktadır. Dağıtık sağlık bilgi sistemlerinde birlikte çalışabilirlik için; bütün sağlık kurumlarına referans olan ve terminoloji bakımından büyük katkı sağlayan Ulusal Sağlık Veri Sözlüğü (USVS) kullanılmaktadır. USVS, sağlık kurumlarından verilerin belirlenmiş standartlar doğrultusunda toplanmasını, analizini ve değerlendirmesini sağlamayı amaçlamaktadır. USVS ile aynı zamanda, sahadan sağlık verisi toplama konusunda verimi artırmak, tekrarlanan ve hatalı verileri azaltmak ve toplanan verinin amacına daha uygun bir şekilde kullanılmasını sağlamak amaçlanmaktadır. İlk sürümü T.C. Sağlık Bakanlığı Bilgi İşlem Daire Başkanlığı tarafından 2007 yılında oluşturulan USVS, şu anda kullanılmakta olan son sürüm 2.2 2014 yılında güncellemiştir.

USVS'nin son sürümünde ne tür bilgilerinin toplanacağı ayrıntılı olarak yer alırken Çizelge 1'de gösterilen toplam 66 kapsamı ve amacı farklı veri seti bulunmaktadır.

Çizelge 1. USVS Sürüm 2.2.'de tanımlanmış veri setleri

Veri Seti Adı	**Veri Seti Adı**
15 - 49 Yaş Kadın İzlem Veri Seti	Ağız Ve Diş Sağlığı Veri Seti
Anne Ölümü Veri Seti	Artroplasti Veri Seti
Aşı Veri Seti	Aşı Erteleme / İptal Veri Seti
Aşı Sonrası İstenmeyen Etki (Asıe) Veri Seti	Bebek /Çocuk Beslenme Veri Seti
Bebek / Çocuk İzlem Veri Seti	Bebek/Çocuk Psikososyal İzlem Veri Seti
Bebek Ölümü Veri Seti	Bildirimi Zorunlu Enfeksiyon Etkenleri Veri Seti
Bulaşıcı Hastalık Kesin Vaka Bildirimi Veri Seti	Bulaşıcı Hastalık Olası Vaka Bildirimi Veri Seti
Diyabet Veri Seti	Diyaliz Hastası Bildirim Veri Seti
Diyaliz Hastası İzlem Veri Seti	Doğum Bildirim Veri Seti
Evde Sağlık Hizmeti İlk İzlem Veri Seti	Evde Sağlık Hizmeti İzlem Veri Seti
Gebelik Bildirim Veri Seti	Gebe İzlem Veri Seti
Gebe Psikososyal İzlemi Veri Seti	Gebelik Sonucu Veri Seti
Gençlik Sağlığı İzlem Veri Seti	Gizli Hasta Veri Seti
Gönderim Paketi Genel Veri Seti	Hasta Kabul Veri Seti
Hasta Çıkış Veri Seti	Hasta Özlük Bilgileri Veri Seti
Hıv Tespit Veri Seti	Hıv İzlem Veri Seti
İntihar Girişimi ve Kriz veri Seti	İntihar Girişimi vee Kriz veri Seti
Kadına Yönelik Şiddet Veri Seti	Kanser Veri Seti
Kanser İzlem Veri Seti	Kök Hücre Nakli Bildirim Veri Seti
Kök Hücre Nakli İzlem Veri Seti	Kronik Hastalıklar Veri Seti
Kuduz Şüpheli Temas Bildirim Veri Seti	Kuduz Profilaksi İzlem Veri Seti
Lohusa İzlem Veri Seti	Madde Bağımlılığı Bildirim Veri Seti
Muayene Veri Seti	Obezite Veri Seti
Organ Nakli Bildirim Veri Seti	Organ Nakli İzlem Veri Seti
Ölüm Bildirim Veri Seti	Paraziter Hastalıklar Vaka Bildirim Veri Seti
Reçete Veri Seti	Sıtma Veri Seti
Tetkik Talep Veri Seti	Tetkik Sonucu Veri Seti
Toplum Tabanlı Kanser Tarama Veri Seti	Tütün Kullanımı Veri Seti
Vatandaş Veri Seti	Vatansız Veri Seti
Verem Veri Seti	Verem Tarama Veri Seti
Yabancı Veri Seti	Yatan Hasta Kabul Veri Seti
Yatan Hasta Veri Seti	Yatan Hasta Çıkış Veri Seti
Yenidoğan Veri Seti	Zehirlenme Veri Seti

Bütün sağlık kuruluşlarının, toplayıp Ulusal Sağlık Bilgi Sistemine göndermekle yükümlü tutulduğu bilgiler belirtilen hastalıkların yanı sıra kişisel aşağıda listelenen bilgileride içermektedir.

Kimlik	Adres	İletişim bilgileri
Hamilelik testleri	Sağlık geçmişi	Özürlülük durumu
Medeni hal	Alkol kullanımı	Madde kullanımı
Sigara kullanımı	İş meslek	Öğrenim durumu
Eğitim Durumu	Gelir durumu	Ailesinde intihar girişimi
Partner bilgileri	Kişisel bakım	Kişisel hijyen
Mahkumiyet durumu	Hastalık şikayetleri	Hastanın öyküsü
Bütün tetkik sonuçları	Tetkik istenen kurumlar	Kullanılan aile planlaması
Gebelik tespiti sonuçları	Son adet tarihi	

4.5. Türkiye'de Sağlık Bilişimi Güvenliği

Türkiye'de sağlık bilişim sistemlerinin doğuşu ve uygulanmaya başlamasıyla beraber ve dünyada örnekleri çokça bulunan siber saldırıları engellemek için Sağlık Bakanlığı sağlık bilişimi uygulamarında ve yazılımlarında bulunması gereken güvenlik gereksinimlerinin ve müdahale süreçlerinin tanımlandığı Bilgi Güvenliği Politikaları Kılavuzu'nu yayımlamıştır. Bu kılavuza göre bakanlık temel olarak bilgi gizliliği ve siber güvenlik hakkında ilgili temel prensipleri yerine getirmek, elde tutulan bilgilere yönelik olası tehditleri öngörmek ve önlem almak, yasalara uymak, BGYS (Bilgi Güvenliği Yönetim Sistemleri)'yi sürekli güncel tutmak ve bu konuya ilişkin eğitimler düzenlemek gibi görevleri üstlenmektedir. Sağlık Bakanlığı bilgi güvenliği kapsamında Sağlık Bilişim Sistemlerine erişebilen çalışanlardan birtakım sorumluluklar istemiştir. Personelin sisteme erişimi için tahsis edilen kullanıcı adı, parola gibi bilgileri üçüncü kişilerle paylaşması yasaktır ve oluşabilecek tehlikelerden, güvenlik zaafiyetine sebep olan personel sorumlu kılınmıştır. Erişebildiği bilgileri yalnızca

işi kapsamında kullanmak ve bu bilgileri yalnızca yetkisi olan kişilerle paylaşmak tanımlanmış yükümlülüklerdendir. Bu yükümlülükler personel iş ile bağını koparsa bile devam etmektedir (Türkiye Cumhuriyeti Sağlık Bakanlığı, 2018). Bilgi güvenliğinin sağlanmasının temel kıstaslarından olan erişim yetkileri için erişim yetkisi ve kontrol matrisleri oluşturulur ve hangi bilgiye kimlerin erişip kimlerin erişemeyeceği belirlenir (Türkiye Cumhuriyeti Sağlık Bakanlığı, 2018). Veri güvenliği verinin korunması için Sağlık Bakanlığı üstlenici firmaları, nesne ve referans bütünlüklerini sağlamak, VTYS (Veri tabanı Yönetim Sistemi)'ye erişim için kullanıcı adı ve parola gereksinimi, VTYS verilerini otomatik olarak yedeklemek ve istenildiği zaman yedekten geri yükleme özelliğine sahip olmalıdır. Kişisel bilgilerin korunması ile ilgili veri tabanında SELECT yetkisi sadece belirlenmiş kişilere verilmeli ve harici kullanıcılara bilgi erişimi kapatılmadır (Türkiye Cumhuriyeti Sağlık Bakanlığı, 2018).

Kullanıcı erişimi ve parola güvenliği konusunda kurumların bilgi güvenliği yetkilileri tarafından parola standartları oluşturulmak zorundadır. Parola standartları belirlenirken kullanıcılar asgari düzeyde, en az 8 karakter, en az 1 küçük 1 büyük harf, en az 1 rakam ve en az 1 sembolden oluşan bir parola oluşturmalıdır. Aynı harf ve rakamların ardarda sıralandığı kombinasyonlar engellenmelidir. Doğum tarihi, isim gibi tahmin edilebilecek bilgilerden oluşan şifreler engellenmeli ve periyodik aralıklarla şifreler sıfırlanarak yenileri ile değiştirilmesi zorunlu olmalıdır. Sisteme erişimine ihtiyaç duyulmayan, işten ayrılan personellerin kullanıcı adlarının kapatılması ve bu personellerin sisteme girmesi engellenmelidir. Sağlık hizmetlerinden yararlanan gerçek kişilerin kimlik bilgilerinin kullanıldığı KPS (Kimlik Paylaşım Sistemi)'ye erişebilen sistemlerin kişilerin bilgi güvenliği için gerekli önlemleri alması ve sistem aracılığıyla KPS'ye erişen kullanıcıların bilgileri üçüncü kişiler ile paylaşmaması gerekmektedir (Türkiye Cumhuriyeti Sağlık Bakanlığı, 2018). Sağlık bilişim sistemlerine uzaktan erişim genel olarak yüklenici firmalar

tarafından gerçekleştirilmektedir. Bakanlık uzaktan erişimin güvenlik zaafiyetine yol açan en büyük tehditlerden biri olmasından kaynaklı; uzaktan erişimi VPN gibi kullanıcı adı ve şifre ile girilebilen domain adreslerine herkesin kolayca ulaşamayacağı uzaktan erişim standartları ile gerçekleştirerek riski en aza indirmeyi zorunlu kılmaktadır. Belirlenen standartlara göre VPN kullanıcılarının kullanıcı adı ve şifreleri yükleniciler tarafından formla başvuru şeklinde oluşturulmalı, VPN kullanıcı şifreleri de parola standartlarına uymalı ve uzun süre kullanılmayan hesaplar askıya alınıp bağlantı sırasında belirli bir süre AFK (Away From Keyboard) kalan kullanıcılar sistemden düşmek zorunda kalmalıdır (Türkiye Cumhuriyeti Sağlık Bakanlığı, 2018). Veri düzeyine kadar indirgenen güvenlik tedbirlerinin en etkililerinden biri olan kriptografik kontroller ise bilgi gizliliğini sağlamak, bütünlüğü korumak, alıcı ve gönderici kimliklerini doğrulamak ve gönderici-alıcı arasında yapılan işlemlerin kayıt altına alınmasını sağlar. Kriptografik kontrolleri sağlamak için şifreleme uygulaması, bilgilerin şifrelenip art niyetli kullanıcıların eline geçse dahi erişilemeyeceği bir koruma sağlar. Kriptografik kontrol yöntemlerinden biri olan veri özeti, bilginin bütünlüğünün korunması için geliştirilen bir stratejidir. Bütünlüğü korunacak olan bilgiden bir harf bile eksildiği takdirde farklı bir özet oluşacağı için, bilgi korunması en üst düzeye çıkmış olacaktır. Kriptografik kontrolleri sağlamak için ise asimetrik şifreleme yöntemleri RSA (Ron Rivest, Adi Shamir ve Leonard Adleman) veya eliptik eğri kriptolojisi (ECC: Elliptic Curve Cryptography) yöntemlerinden en az birisi kullanılır. Anahtar değişimi ve doğrulama (authentication) fonksiyonlarında, Diffie-Hellman (DH), internet anahtar değişim (IKE: İnternet Key Exchange) veya eliptik eğri kullanan DH (ECDH: Elliptic Curve Diffie-Hellman) algoritmalarından birisi seçilip uygulanır. Sağlık Bilişim Sistemlerinde ortaya çıkabilecek güvenlik hatalarından korunmak ve sistemlerin karşı karşıya kalabileceği durdurucu hataların önüne geçilebilmesi için geliştirme, test ve canlı ortamların birbirinden ayrılması ve oluşabilecek bir sorunun canlı ortamda karşılaşılmadan test veya geliştirme

ortamında fark edilmesi amaçlanır. Sağlık Bilişim Sistemlerine erişimi sağlayan sunucu ve sistemlerin güvenliği için, iş güvenliği ve devamlılığı için prosedürler oluşturularak acil durumlarda ulaşılabilecek personel ve yetkililer belirlenir, sunuculara erişebilecek kişilerin yetki tanımlaması için erişim matrisleri oluşturur. Sunuculara yapılan erişimlerin gerçekleştiği saat ve erişimi gerçekleştiren kişilerin sunucuda yaptığı işlemler raporlanmak zorundadır. Sunucularda açılacak oturumlar için kurallar tanımlanır ve kullanıcı parolaları parola güvenliği standartlarına uymalıdır. Sunucularda maksimum 10 dakika AFK (Away From Keyboard) olarak kalan kullanıcılar otomatik olarak sistemden atılmalıdır. Sistemlere karşı oluşan tehditler ve olası saldırı durumlarında iz kayıtları (log) yönetimi devreye girmeli ve saldırı veya tehdit durumunda oluşan durumlar ve işlemler kayıt altına alınmalıdır (Türkiye Cumhuriyeti Sağlık Bakanlığı, 2018). Sağlık Bakanlığı kişisel ve kurumsal bilginin gizliliği ile art niyetli kişilerin eline geçmemesi için geçmişte dünyada ve ülkemizde yaşanan olaylardan veriler toplayarak güvenli bilişim sistemleri oluşturmak amacıyla; ülkemizde Sağlık Bilişim Sistemleri yazılım ve donanım hizmeti sunan firmaların uygulaması adına belli prosedürler oluşturmuş ve Sağlık Bilişim Sistemleri sektöründe faaliyet gösteren firmaları yukarıda belirtilen gereksinimleri uyma konusunda zorunlu tutmuştur.

5. ARAŞTIRMA

5.1. Araştırmanın Amacı ve Önemi

Araştırmada, dijital veri güvenliği perspektifinden Türkiye Cumhuriyeti vatandaşlarının dijital sağlık kayıtlarının güvenliğine yönelik farkındalık ve beklentilerini değerlendirilmesi amaçlanmıştır. Bu kapsamda elektronik sağlık kayıtları farkındalık ve beklentileri ölçeği ifadelerinden oluşan anket formu Google Forms üzerinden elektronik anket formu şeklinde oluşturularak, yaşları 18-70 arasında değişen farklı illerde yaşayan ve sektörlerde çalışan, çalışmayan 444 katılımcıya uygulanmıştır.

5.2. Araştırma Yöntemi ve Soruları

Anket soruları literatür taraması yapılarak hazırlanmıştır. Anket soruları iki bölümden oluşmaktadır. Birinci bölümde katılımcılara ait demografik değişkenlere yer verilmiş olup; ikinci bölümde ise ESK ile ilgili sorular sorulmuştur. Araştırmada 1932 yılında sosyal psikolog Rensis Likert tarafından geliştirilen insanların görüşleri bütüncül bir şekilde görülebilmesini sağlayan 5'li Likert tipi ölçek kullanılmıştır. Seçenekler, "Kesinlikle Katılıyorum"dan "Kesinlikle Katılmıyorum"a kadar değişmektedir, böylece anket insanların görüşleri bütüncül bir şekilde görülebilmektedir. Ölçek, aynı zamanda, konu hakkında bilgisiz ya da tarafsız olanlar için ne katılıyorum ne de katılmıyorum gibi bir orta noktalar içermektedir.

5.3. Araştırmanın Evreni ve Örneklem

Araştırmanın evrenini, Türkiye Cumhuriyeti'nde yaşayan bireyler oluşturmaktadır. Türkiye Cumhuriyeti'nde yaşayan tüm bireylere ulaşmanın mümkün olmamasından dolayı farklı sektörlerde çalışan bireyler ile anket linki paylaşarak farklı çevrelere yayılması sağlanmıştır.

Araştırmanın saha uygulaması 8 Aralık 2020 tarihinde başlayıp, 05 Ocak 2021 tarihinde sonlandırılmıştır. Araştırmaya Türkiye'nin 7 bölgesinden toplamda 444 kişi katılmıştır.

5.4. Araştırma Sınırlılıkları

Araştırma kapsamında yapılan anket çalışmasının yönteminin dijital anket yöntemi olarak belirlenmesi araştırmacı ve katılımcının yüz yüze görüşme yaparak elde edilebilecek verilere ulaşılamamasının yanında teknoloji okur yazarı olamayan bireylere ulaşılamaması da bir sınırlılık olarak kabul edilmiştir.

5.5. Araştırma Verilerinin Değerlendirilmesi

Çalışmada Öğütçü tarafından 2011 yılında yapılan Elektronik Sağlık Kayıtlarının İçeriği, Hassasiyeti ve Erişim Kontrollerine Yönelik Farkındalık ve Beklentilerin Değerlendirilmesi çalışmasında kullanılan anket soruları günümüze uyarlanarak kullanılmıştır.

Araştırmada uygulanan anket formu yedi bölümden oluşmaktadır. Birinci bölümde katılımcıların Sosyo demografik özelliklerine yönelik sorular sorulmuştur. İkinci bölümde katılımcıların elektronik ortamlarda kayıt altına alınan verilerini ne derece kişisel bulduklarını ölçmeye yönelik sorular sorulmuştur. Üçüncü bölümde katılımcılara elektronik ortamlarda kayıt altına alınan bilgilerinin dijital ortam ve uygulamarda kayıt altına alındığının farkındalığına yönelik sorular sorulmuştur. Dördüncü bölümde katılımcılara sağlık bilgilerinin gizliliği ile ilgili görüşlerini ölçmeye yönelik sorular sorulmuştur. Beşinci bölümde katılımcılara sağlık bilgilerinin dijital ortamlarda saklanması ile ilgili gizlilik ve güvenlik ile ilgili farkındalık ve beklentilerini ölçmeye yönelik sorular sorulmuştur. Altıncı bölümde katılımcılara dijital ortamda saklanan sağlık bilgilerinin kullanımı ile ilgili farkındalık ve beklentilerini ölçmeye yönelik sorular sorulmuştur. Son bölümde ise

katılımcılara, dijital ortamda saklanan sağlık bilgilerinin güvenlik sorumlulukları ile ilgili farkındalık ve beklentilerini ölçmeye yönelik sorular sorulmuştur.

Anket formunda, ilk bölümde 8 soru, ikinci bölümde ise 11 soru, üçüncü bölümde 11 soru, dördüncü bölümde 8 soru, beşinci bölümde 6,altıncı bölümde 8 son bölümde ise 8 soru olmak üzere toplam 60 sorudan oluşmaktadır. İlk 8 soru katılımcıların, yaş, yaşanılan şehir vs. gibi sosyo-demografik özelliklerine yönelik sorulardan oluşmakta olup çoktan seçmeli ve açık uçlu sorulardan oluşmaktadır. Sonraki 11 soru katılımcıların elektronik sağlık kayıtları hakkında farkındalık ve beklentilerini ölçmeye yönelik 3'lü Likert (1.Evet 2.Hayır 3.Fikrim Yok) 41 soru ise katılımcıların elektronik sağlık kayıtları hakkında farkındalık ve beklentilerini ölçmeye yönelik 5'li Likert (1: kesinlikle katılmıyorum, 2: katılmıyorum, 3: orta derecede katılıyorum, 4: katılıyorum, 5: kesinlikle katılıyorum) ile ölçeklendirilmiştir.

5.6. Araştırmada Kullanılan Analizler

Araştırma sonucunda elde edilen verilerin analizi için Statistical Package for the Social Sciences (SPSS) 22.0 kullanılmıştır. Katılımcıların demografik bilgileri (yaş, eğitim) tablolar ile düzenlenmiştir.

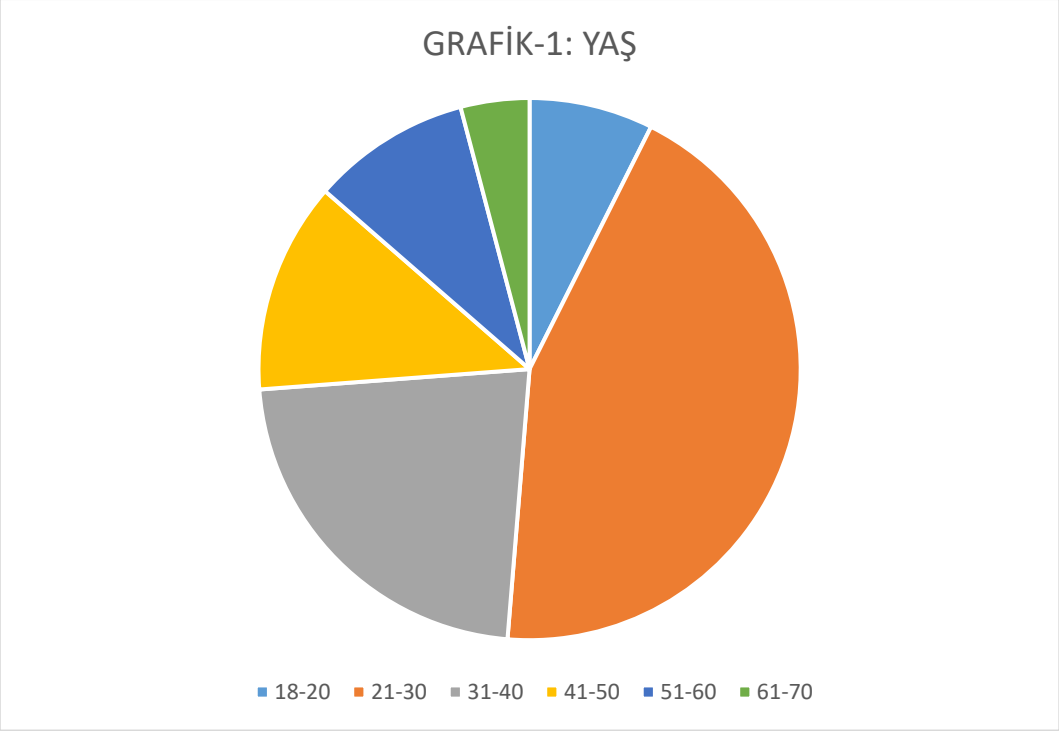
Araştırmada veriler, 'n' ve '%' olarak verilmiştir. Verilerin sonuçlarını aktarmak için yüzde, standart sapma, güven derecesi, sayı gibi istatistik verileri kullanılmıştır. Araştırmada elde edilen verilerin istatiksel anlamlılık düzeyi $p<0,5$ olarak kabul edilmiştir. Araştırmada ölçeğin güvenilirliği için Cronbach's Alpha değeri saptanmıştır. Cronbach's Alpha değeri >0,70 güvenilir olarak kabul edilmiştir ve çalışmada, Cronbach's Alpha değeri 0,900, Cronbach's Alpha Based on Standardized Items değeri (Güvenirlik katsayısı) ise 0,911 olarak bulunmuştur (Tablo 1).

Tablo 1. Güvenilirlik Analizi

Cronbach’s Alpha	Standartlaştırılmış Maddelere Dayalı Cronbach's Alpha	Madde Numarası
0,900	0,911	52

6. ANALİZ VE BULGULAR

Araştırmaya katılan katılımcıların yaşları, %43,9'u 21-30 yaş arası, %22,5'i 31-40 yaş arası, %12,6 sı 41-50 yaş arası, %9,5'i 51-60 yaş arası, %7,4'ü 18-20 yaş arası %4,1'i 18-20 yaş arası bireylerden oluşmaktadır. Araştırmaya katılan katılımcıların %66'sı 21-40 yaş arasındadır (Grafik-1) (Tablo-2).

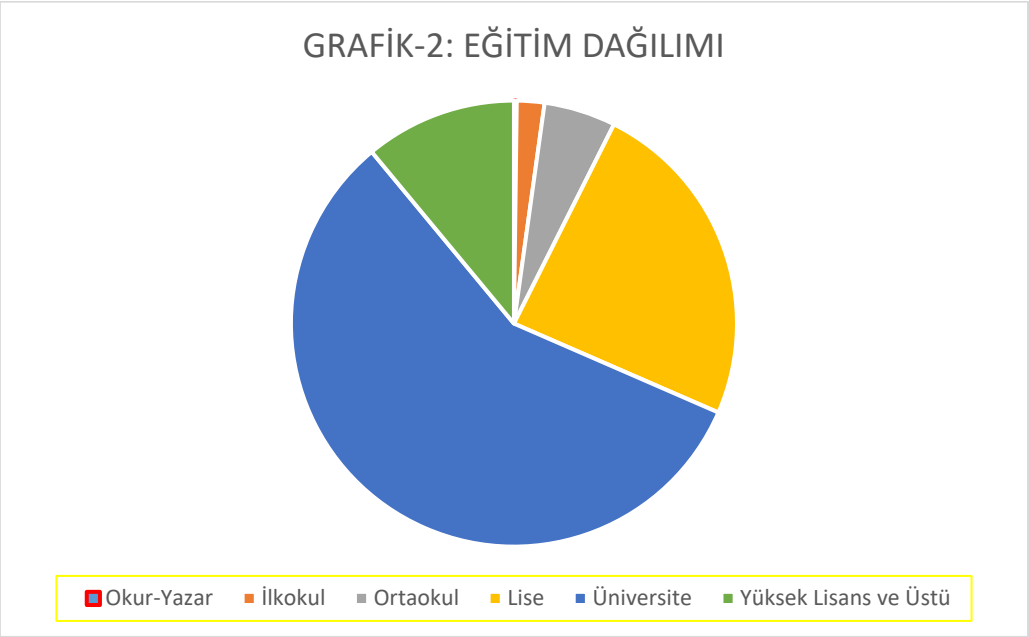


Grafik 1. Yaş

Tablo 2. Yaş Dağılımı

Yaş Aralığı	**Kişi Sayısı (n)**	**Yüzde (%)**
18-20	33	7,4
21-30	195	43,9
31-40	100	22,5
41-50	56	12,6
51-60	42	9,5
61-70	18	4,1
Toplam	444	100,0

Eğitim düzeyleri, %57,4'ü üniversite mezunu, %24,1'i, lise mezunu, %11,0'ı yüksek lisans ve üstü mezunu, %5,2'si ortaokul mezunu, %2,0'ı ilkokul mezunu, %0,2'si ise okur-yazar bireylerden oluşmaktadır. Katılımcıların %92'si lise ve daha yüksek eğitim düzeyine sahiptir (Grafik-2) (Tablo-3).



Grafik 2. Eğitim Dağılımı

Tablo 3. Eğitim Düzeyi Dağılımı

Eğitim Durumu	**Kişi Sayısı (n)**	**Yüzde (%)**
Okur-Yazar	1	0,2
İlkokul	9	2,0
Ortaokul	23	5,2
Lise	107	24,1
Üniversite	255	57,4
Yüksek Lisans ve Üstü	49	11,0
Toplam	444	100,0

Katılımcıların, güncel sağlık durumları katılımcıların verdikleri cevaplara göre, %79,3'ünün herhangi bir bilinen rahatsızlığı bulunmamaktadır. %20'sinin bilinen bir rahatsızlığı bulunmaktadır. %0.7 katılımcı ise bu soruya iki yanıtı seçerek cevap vermişlerdir ve değerlendirmede verdikleri cevaplar geçersiz sayılmıştır

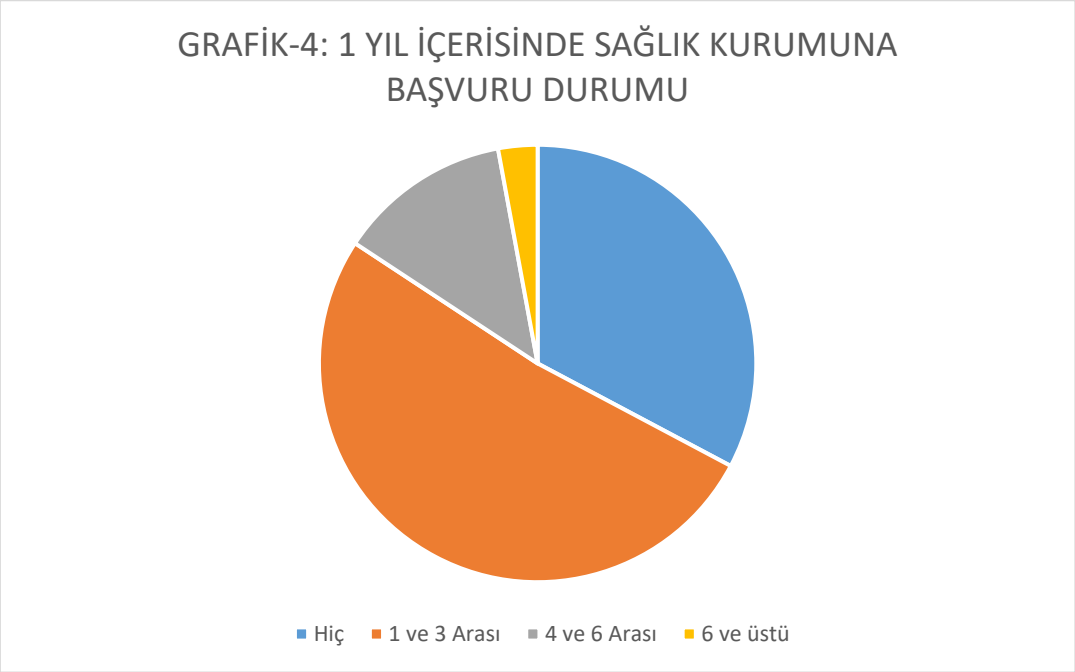
(Grafik-3) (Tablo-4).

Grafik 3. Güncel Sağlık Durumu

Tablo 4. Güncel Sağlık Durumu

Rahatsızlık Durumu	Kişi Sayısı (n)	Yüzde (%)
Bilinen herhangi bir rahatsızlığım yoktur.	352	79,3
Geçersiz	3	0,7
Rahatsızlığım var.	89	20,0
Toplam	444	100,0

Katılımcıların, %51,4'ü son 1 yıl içerisinde 1-3 arası kez sağlık kurumuna başvururken, %12,8'i 4-6 arası kez sağlık kurumuna başvurmuştur. %2,9 katılımcı ise son 1 yıl içerisinde 6 ve üzeri defa sağlık kurumuna başvururken, %32,7 katılımcı hiç sağlık kurumuna başvurmamıştır. Katılımcıların %66'sı son 1 yıl içerisinde en az bir kez sağlık kurumuna başvurmuştur (Grafik-4) (Tablo-5).

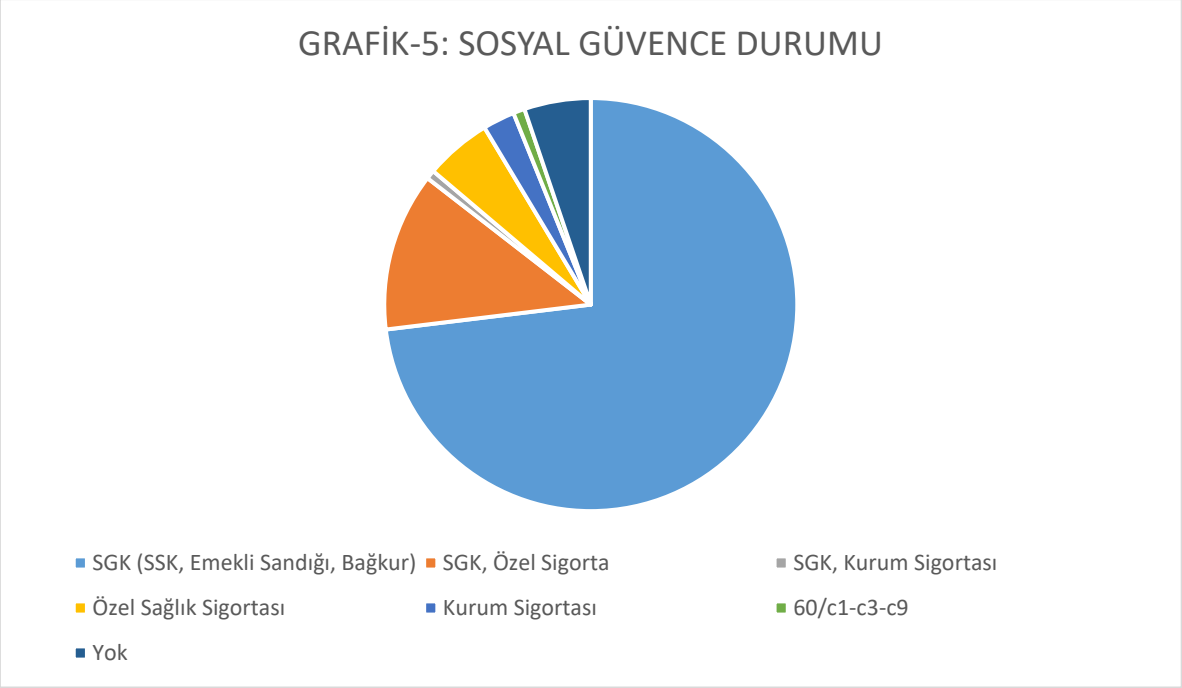


Grafik 4. 1 Yıl İçerisinde Sağlık Kurumuna Başvuru Durumu

Tablo 5. 1 Yıl İçerisinde Sağlık Kurumuna Başvuru

Başvuru Sayısı	**Kişi Sayısı (n)**	**Yüzde (%)**
Geçersiz	1	0,2
Hiç	145	32,7
1-3	228	51,4
4-6	57	12,8
6 ve üstü	13	2,9
Toplam	444	100,0

Katılımcıların sosyal güvenceleri %73'ü SGK (SSK, Emekli Sandığı, Bağkur) gibi devlet tarafından sağlanan sosyal güvenceye sahip bireylerden oluşmaktadır. %12,4 'ünü oluşturan katılımcı ise SGK güvencesinin yanına ek olarak özel sağlık sigortası yaptırmış bireylerdir. %5,2 katılımcının ise sadece özel sağlık sigortası vardır. Katılımcıların, %2.5'i ise kurum sigortası ile sosyal güvencelerini sağlamaktadırlar. Katılımcıların %0,9'u ise Türkiye Cumhuriyeti tarafından engelli vatandaşlara sağlanan 60/c1-c3-c9 kapsamında sosyal güvenceye sahipken. %5,3 katılımcı herhangi bir sosyal güvenceye sahip değillerdir (Grafik-5) (Tablo-6).

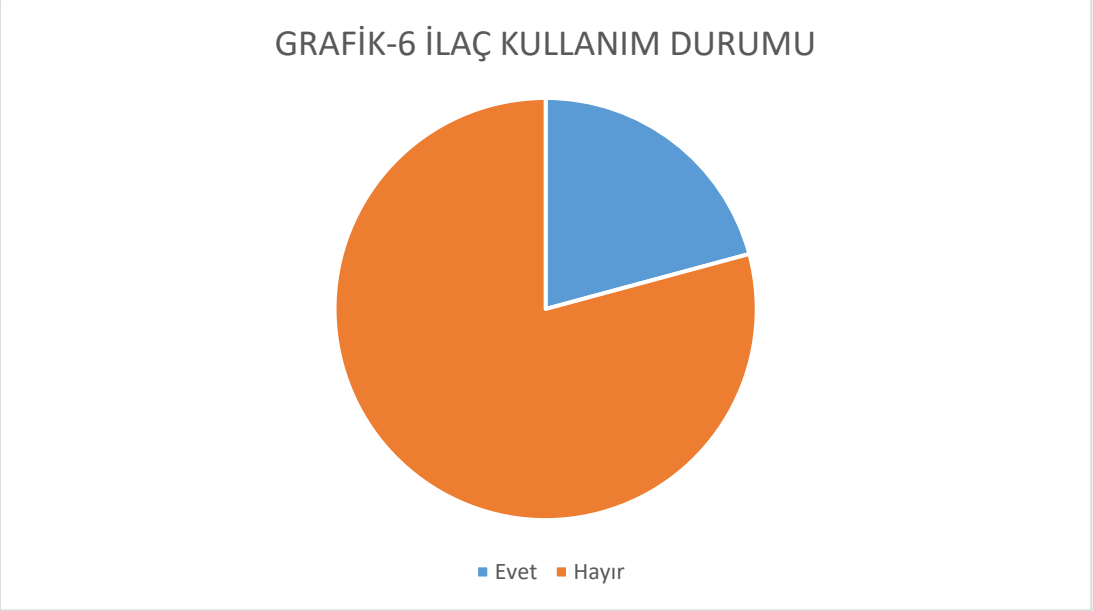


Grafik 5. Sosyal Güvence Durumu

Tablo 6. Sosyal Güvence Durumu

Güvence Türü	Kişi Sayısı (n)	Yüzde (%)
Geçersiz	1	0,2
SGK (SSK, Emekli Sandığı, Bağkur)	324	73,0
SGK, Özel Sigorta	55	12,4
SGK, Kurum Sigortası	3	0,7
Özel Sağlık Sigortası	23	5,2
Kurum Sigortası	11	2,5
60/c1-c3-c9	4	0,9
Yok	23	5,2
Toplam	444	100,0

Katılımcıların, %78,6'sı sürekli ilaç kullanmazken, %20,5'i sürekli ilaç kullanan bireylerden oluşmaktadır. %0,9 katılımcı ise bu soruya cevap vermemiştir (Grafik-6) (Tablo-7).

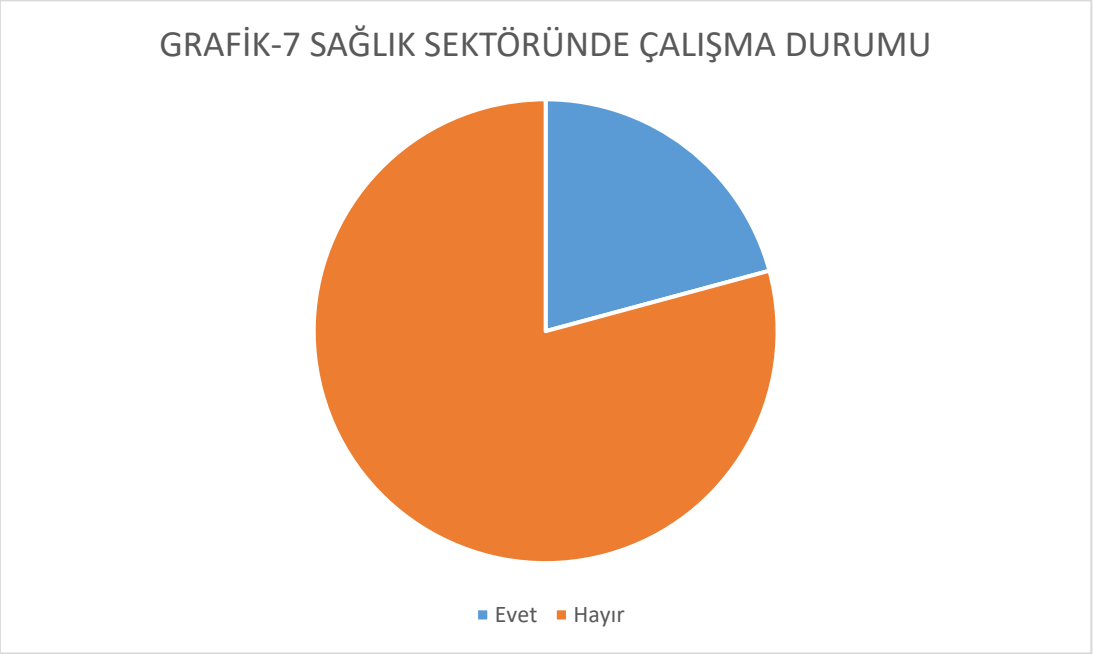


Grafik 6. İlaç Kullanım Durumu

Tablo 7. İlaç Kullanım Durumu

İlaç Kullanımı	Kişi Sayısı (n)	Yüzde (%)
Evet	91	20,5
Hayır	349	78,6
Geçersiz	4	0,9
Toplam	444	100,0

Katılımcıların, %82,9 farklı sektörlerde çalışırken, %16,9'u sağlık sektöründe çalışmaktadır (Grafik-7) (Tablo-8).

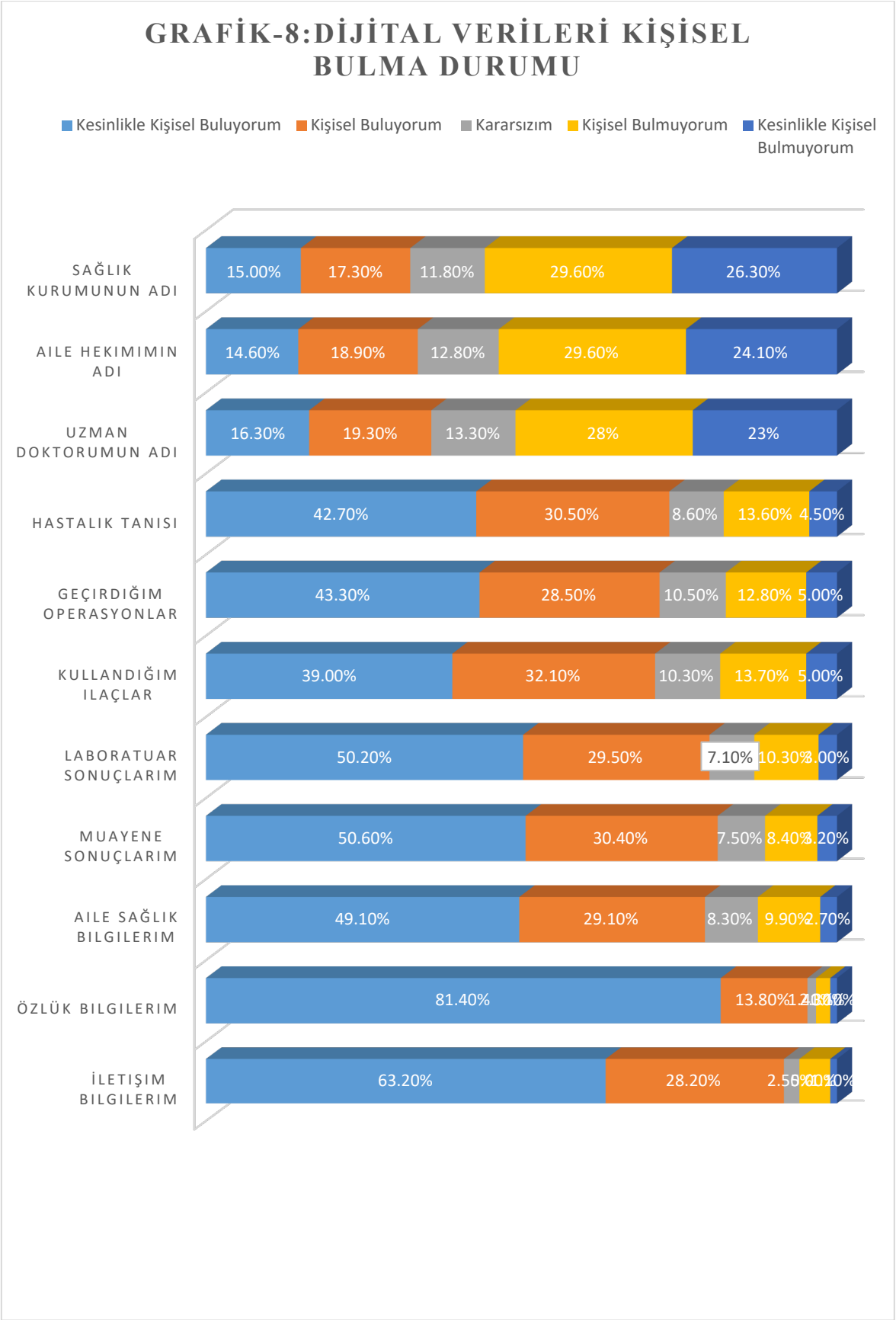


Grafik 7. Sağlık Sektöründe Çalışma Durumu

Tablo 8. Sağlık Sektöründe Çalışma Durumu

Sektör Bilgisi	**Kişi Sayısı (n)**	**Yüzde (%)**
Evet	91	20,5
Hayır	349	78,6
Geçersiz	4	0,9
Toplam	444	100,0

Çalışmaya katılan, katılımcılara kayıt altına alınan dijital sağlık verilerini kişisel bulup bulmadıkları ile ilgili sorular yöneltilmiştir. Bu veriler, iletişim bilgileri (Adres, telefon, vb.), özlük bilgileri (TC kimlik no, doğum tarihi, vb.), aile sağlık bilgileri (Kalıtsal hastalıklar, genetik bilgiler, vb.), muayene sonuçları (şikayetler, doktor bulguları, vb.), laboratuar sonuçları (kan/idrar tahlilleri, röntgen, MR sonuçları, vb.), kullandığı ilaçlar, geçirdiği operasyonlar, hastalık tanıları, uzman doktorlarının adı, aile hekimlerinin adı, başvurdukları sağlık kurumunun adı (Hastane, Eczane, vb.) gibi elektronik ortamlarda kayıt altına alınan bilgilerdir. Katılımcıların %90,5'i iletişim bilgilerini kişisel bulurken), geri kalan kısım ise kararsız ve kişisel bulmadıklarını belirtmişlerdir. Özlük bilgilerini ise katılımcıların, %94,8'i kişisel bulurken kalan kısım kararsız ve kişisel bulmadıklarını belirtmişlerdir. Aile sağlık bilgilerinde ise katılımcıların %78,2 kişisel bulduklarını ifade ederken kalan kısım kararsız ve kişisel bulmadıklarını belirtmişlerdir. Muayene sonuçlarını kişisel bulan katılımcı oranı %80,4 iken kalan kısım kişisel bulmayan ve kararsız kalan katılımcılardan oluşmaktadır. Laboratuar sonuçlarını kişisel bulan katılımcı oranı %78,6'dır. Kullandığı ilaçları kişisel bulan katılımcı oranı ise %70,3'dür. Geçirdiği operasyonları kişisel bulan katılımcı oranı %71'dir. Hastalık tanılarını ise kişisel bulan katılımcı oranı %72,5'dir. Katılımcıların %34,9'u doktorlarının adını kişisel bulduklarını belirtmişlerdir. Aile hekiminin adlarını kişisel bulan katılımcıların oranı %33,1' Sağlık kurumlarının adlarını kişisel bulan katılımcı oranı %31,5dir (Grafik-8) (Tablo-9).

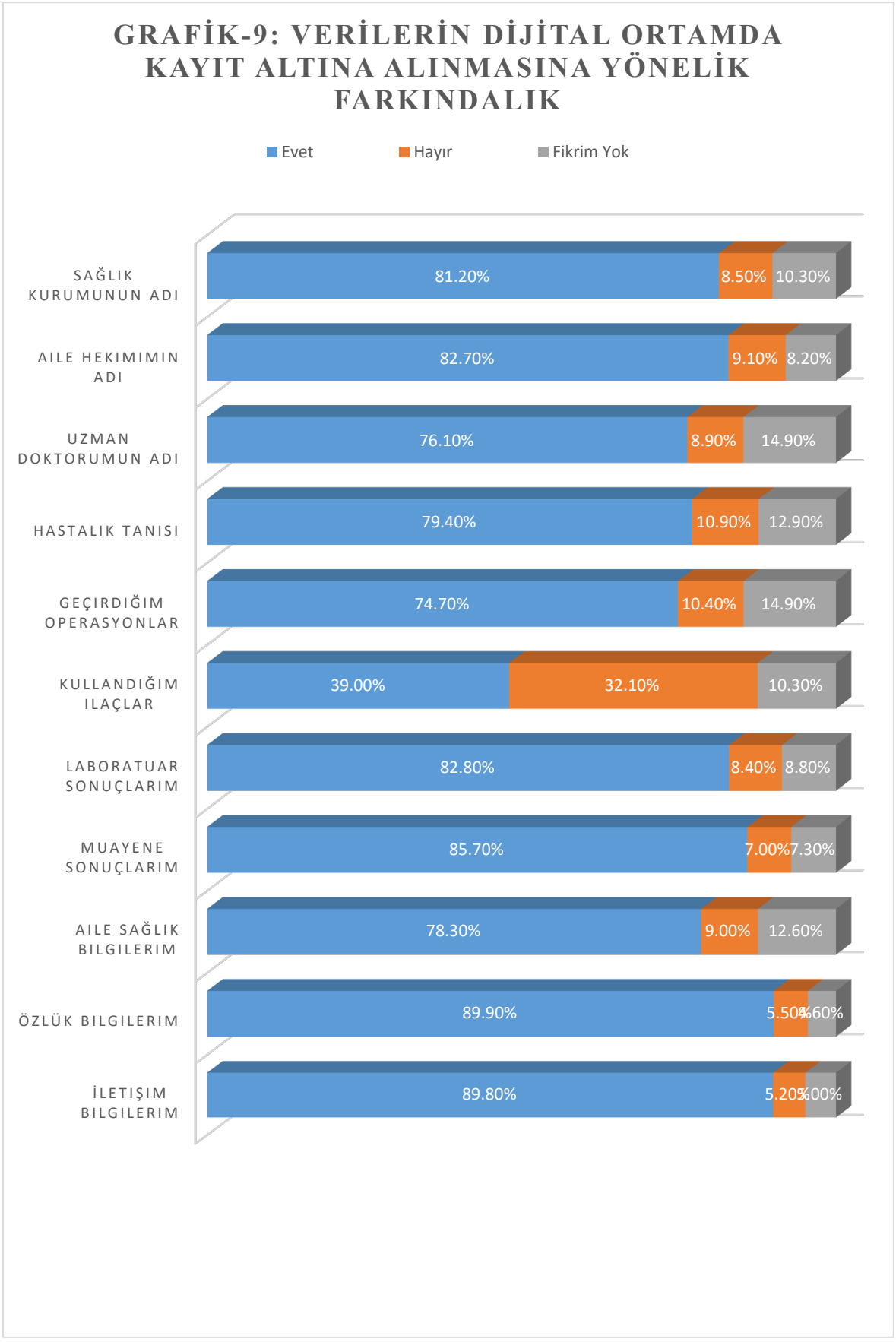


Grafik 8. Dijital Verileri Kişisel Bulma Durumu

Tablo 9. Dijital Verileri Kişisel Bulma Durumu

Sorular	Kesinlikle Kişisel Buluyorum	Kişisel Buluyorum	Kararsızım	Kişisel Bulmuyorum	Kesinlikle Kişisel Bulmuyorum
İletişim bilgilerim	%63,2	%28,2	%2,5	%5,0	%1,1
Özlük bilgilerim	%81,4	%13,8	%1,4	%2,3	%1,1
Aile sağlık bilgilerim	%49,1	%29,1	%8,3	%9,9	%2,7
Muayene sonuçlarım	%50,6	%30,4	%7,5	%8,4	%3,2
Laboratuar sonuçlarım	%50,2	%29,5	%7,1	%10,3	%3,0
Kullandığım ilaçlar	%39,0	%32,1	%10,3	%13,7	%5,0
Geçirdiğim operasyonlar	%43,3	%28,5	%10,5	%12,8	%5,0
Hastalık tanısı	%42,7	%30,5	%8,6	%13,6	%4,5
Uzman doktorumun adı	%16,3	%19,3	%13,3	%28	%23
Aile hekimimin adı	%14,6	%18,9	%12,8	%29,6	%24,1
Sağlık kurumunun adı	%15,0	%17,3	%11,8	%29,6	%26,3

Çalışmaya katılanlara, sağlık verilerinin, dijital ortamlarda kayıt altına alındığının ve saklandığının farkındalığını ölçmek için sorular yönetilmiştir. Araştırmaya katılan 444 katılımcıdan, iletişim bilgilerinin dijital ortamda kayıt altına alındığını bilenlerin oranı %89,8'dir. Özlük bilgilerinin kayıt altına alınıp, saklandığının farkında olan katılımcı oranı ise 89,9'dur. Katılımcıların, Aile sağlık bilgilerinin dijital ortamlarda saklandığının farkında olanlarının oranı ise %78,3'dür. Muayene sonuçlarının dijital ortamlarda saklandığının farkında olan katılımcı oranı ise %85,7'dir. Katılımcıların %82,8'i laboratuar sonuçlarının dijital ortamlarda saklandığını bilmektedir. Kullandığı ilaçların dijital ortamlarda saklandığını bilen katılımcı oranı ise %74,7'dir. Geçirdiği operasyonların dijital ortamlarda saklandığını bilen katılımcı oranı %76,2'dir. Hastalık tanılarının dijital ortamlarda kayıt edildiğini bilen katılımcı oranı ise %79,4'dür. Uzman doktorunun adlarının dijital ortamlarda kayıt altına alındığını ise katılımcıların %76,1'i bilmektedir. Aile hekiminin adının dijital ortamlarda kayıt altına alınığ, saklandığını bilen katılımcı oranı %82,7'dir. Sağlık kurmunun adının dijital ortamlarda kayıt altına alındığını bilen katılımcı oranı ise %81,2'dir (Grafik-9) (Tablo-10).

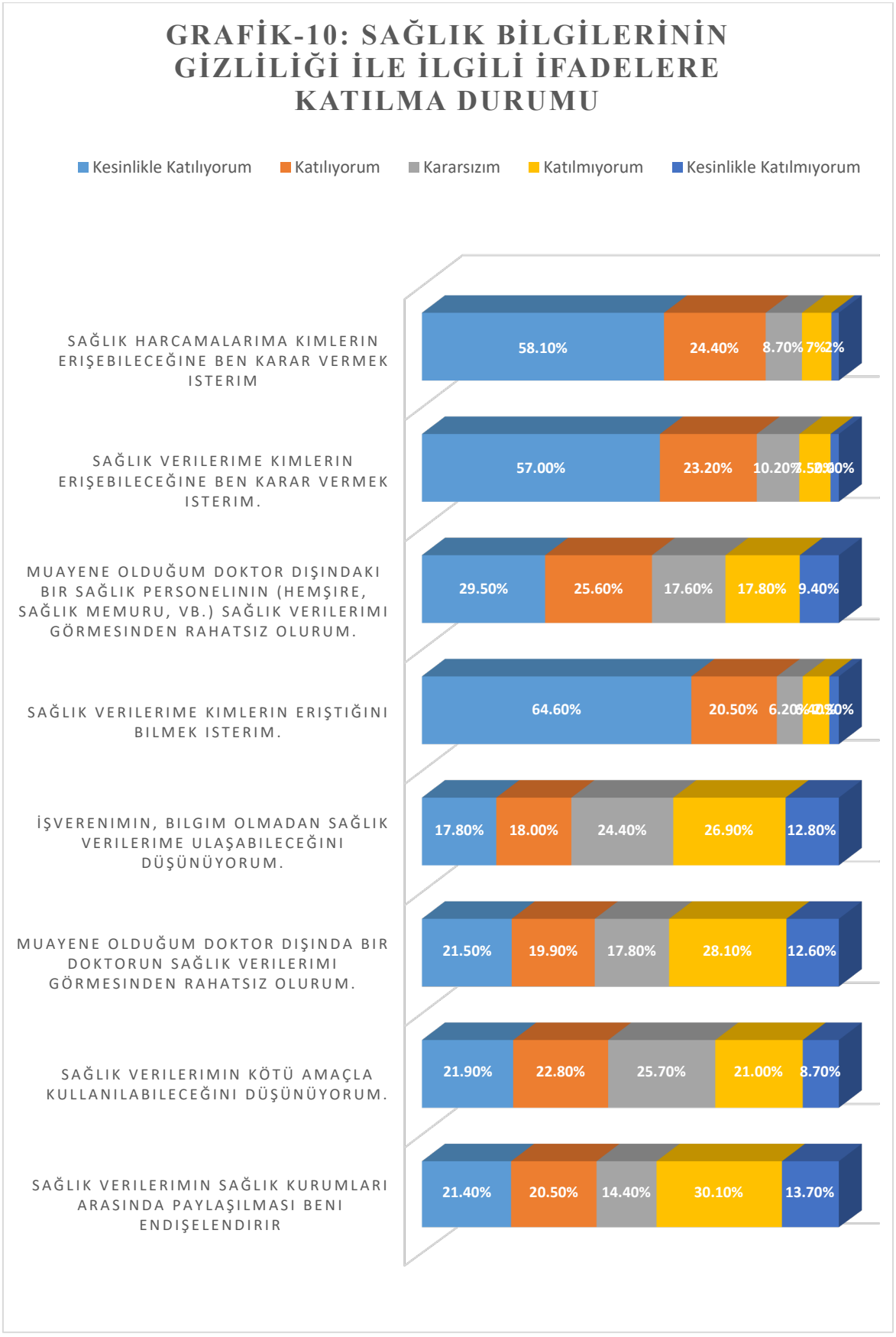


Grafik 9. Verilerin Dijital Ortamda Kayıt Altına Alınmasına Yönelik Farkındalık

Tablo 10. Verilerin Dijital Ortamda Kayıt Altına Alınmasına Yönelik Farkındalık

Tablo 11. Verilerin Dijital Ortamda Kayıt Altına Alınmasına Yönelik Farkındalık **Sorular**	**Evet**	**Hayır**	**Fikrim Yok**
İletişim bilgilerim	%89,8	%5,2	%5,0
Özlük bilgilerim	%89,9	%5,5	%4,6
Aile sağlık bilgilerim	%78,3	%9,0	%12,6
Muayene sonuçlarım	%85,7	%7,0	%7,3
Laboratuar sonuçlarım	%82,8	%8,4	%8,8
Kullandığım ilaçlar	%39,0	%32,1	%10,3
Geçirdiğim operasyonlar	%74,7	%10,4	%14,9
Hastalık tanısı	%79,4	%10,9	%12,9
Uzman doktorumun adı	%76,1	%8,9	%14,9
Aile hekimimin adı	%82,7	%9,1	%8,2
Sağlık kurumunun adı	%81,2	%8,5	%10,3

Katılımcılara sağlık bilgilerinin gizliliği ile ilgili bir takım ifadelere katılma derecelerini belirleyen sorular sorulmuştur. Katılımcıların %41,9'u kayıt altına alınan sağlık verilerinin sağlık kurumları arasında paylaşılmasından endişe duyacaklarını belirtmiştir. Katılımcıların %44,7'si mevcut sağlık verilerinin kötü amaçla kullanılabileceğini düşünmektedir. Muayene olduğu doktor dışında başka bir doktorun sağlık verilerini görmesinden rahatsız olacağını ifade eden katılımcı yüzdesi ise %41,4'dür. İşverenlerinin sağlık verilerine izinsiz bir şekilde ulaşabileceklerini düşünen katılımcı oranı ise %35,8'dir. Sağlık verilerini kimlerin erişeceğini bilmek isteyen katılımcı oranı %85,1'dir. Muayene olduğu doktor dışında herhangi bir sağlık personelinin sağlık verilerini görmesinden rahatsız olacağını belirten katılımcı oranı ise %55,1'dir. Sağlık verilerine kimlerin erişeceğinin yetkilendirmesini yapmak isteyen katılımcı oranı ise %80,2'dir. Sağlık harcamalarına kimlerin erişebileceğini kendisinin karar vermesini isteyen katılımcı oranı %82,5'dir (Grafik-10) (Tablo-11).

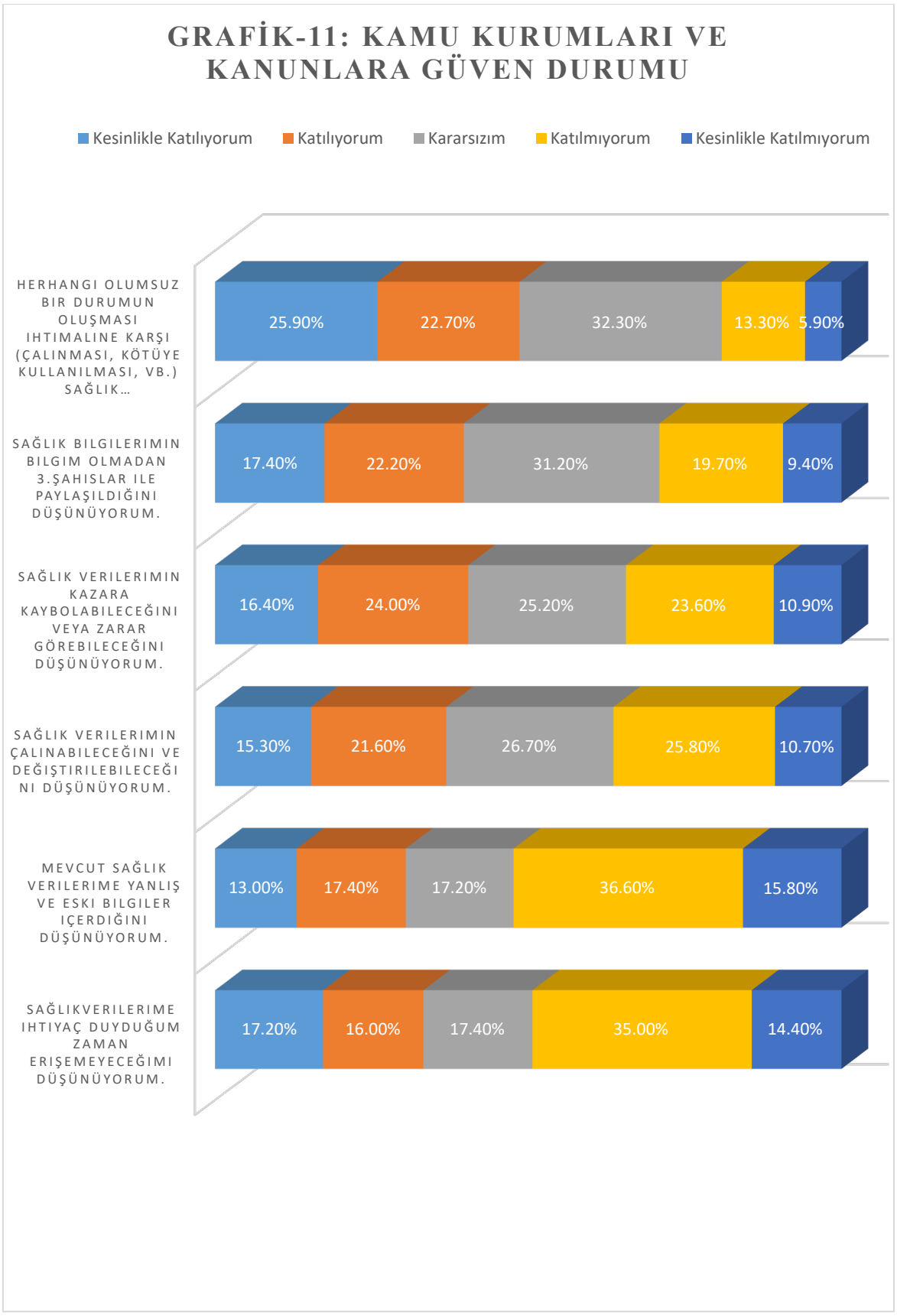


Grafik 10. Sağlık Bilgilerinin Gizliliği ile İlgili İfadelere Katılma Durumu

Tablo 12. Sağlık Bilgilerinin Gizliliği ile İlgili İfadelere Katılma Durumu

Sorular	Kesinlikle Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle Katılmıyorum
Sağlık verilerimin sağlık kurumları arasında paylaşılması beni endişelendirir	%21,4	%20,5	%14,4	%30,1	%13,7
Sağlık verilerimin kötü amaçla kullanılabileceğini düşünüyorum.	%21,9	%22,8	%25,7	%21,0	%8,7
Muayene olduğum doktor dışında bir doktorun sağlık verilerimi görmesinden rahatsız olurum.	%21,5	%19,9	%17,8	%28,1	%12,6
İşverenimin, bilgim olmadan sağlık verilerime ulaşabileceğini düşünüyorum.	%17,8	%18,0	%24,4	%26,9	%12,8
Sağlık verilerime kimlerin eriştiğini bilmek isterim.	%64,6	%20,5	%6,2	%6,4	%2,3
Muayene olduğum doktor dışındaki bir sağlık personelinin (hemşire, sağlık memuru, vb.) sağlık verilerimi görmesinden rahatsız olurum.	%29,5	%25,6	%17,6	%17,8	%9,4
Sağlık verilerime kimlerin erişebileceğine ben karar vermek isterim.	%57,0	%23,2	%10,2	%7,5	%2,0
Sağlık harcamalarıma kimlerin erişebileceğine ben karar vermek isterim	%58,1	%24,4	%8,7	%7,1	%1,8

Katılımcılara, Sağlık bilgilerinin dijital ortamda saklanmasıyla ilgili verilen ifadelere katılma derecelerini ölçmek amacıyla bazı sorular sorulmuştur. Katılımcıların verdikleri cevaplar neticesinde, sağlık verilerine ihtiyaç duydukları anda erişemeyeceğini düşünen katılımcı oranı %33,2'dir. Katılımcıların %30,4'ü mevcut sağlık verilerinin yanlış ve eski bilgiler içerdiğini, %36,9 sağlık verilerinin çalınabilip, değiştirilebileceğini düşünmektedir. Sağlık verilerinin kazara kaybolabileceğini düşünen katılımcı oranı ise %40,4'dür. Sağlık bilgilerinin, bilgileri dahili olmadan üçümcü şahıslar ile paylaşıldığını düşünen katılımcı oranı %39,7'dir. Sağlık verilerinin çalınması, kötüye kullanılması gibi durumlarda kamu kurum, kuruluş ve kanunlarla korunduğunu düşünen katılımcı oranı ise %48,6'dır (Grafik-11) (Tablo-12).

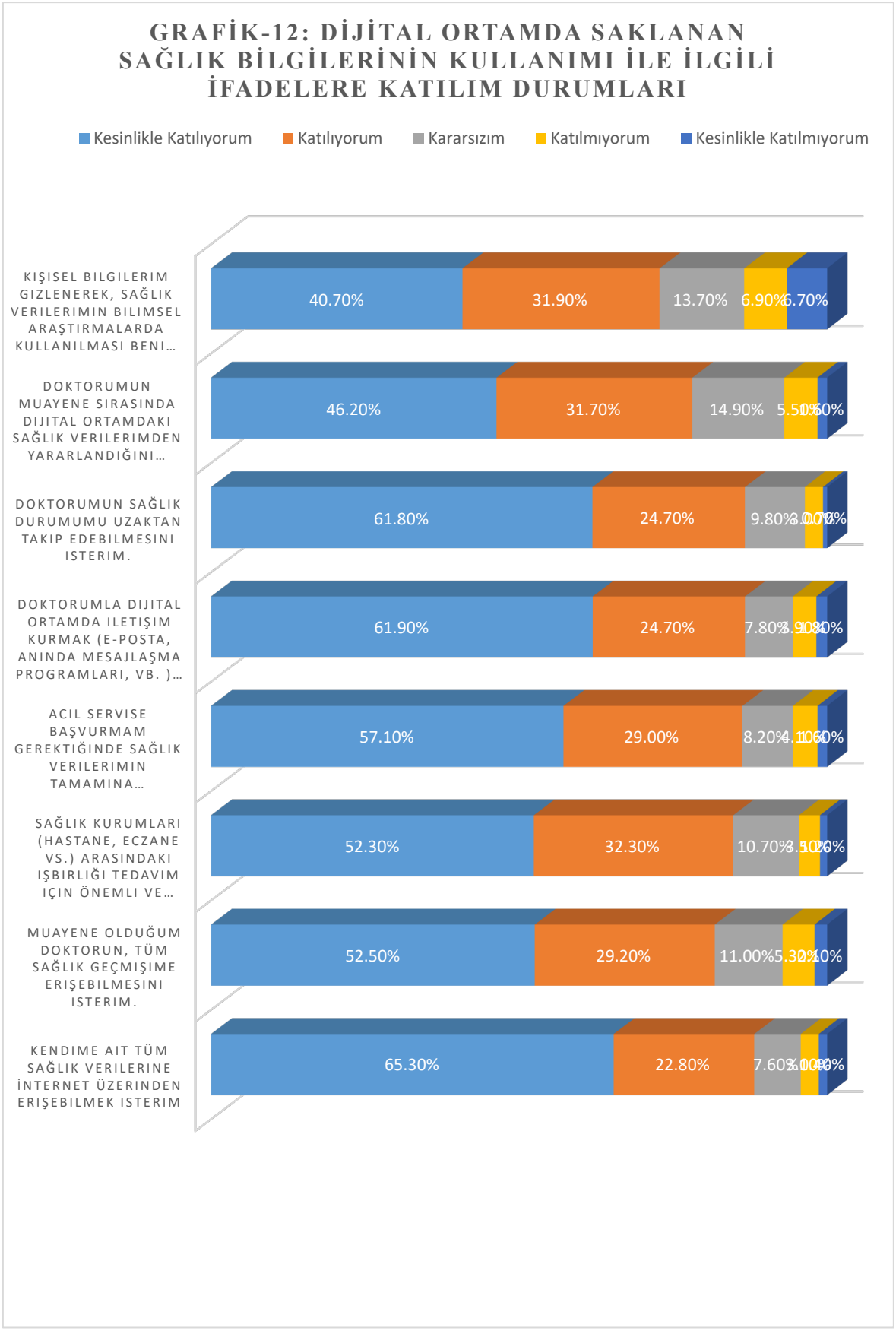


Grafik 11. Kamu Kurumları ve Kanunlara Güven Durumu

Tablo 13. Kamu Kurumları ve Kanunlara Güven Durumu

Sorular	Kesinlikle Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle Katılmıyorum
Sağlık verilerime ihtiyaç duyduğum zaman erişemeyeceğimi düşünüyorum.	%17,2	%16,0	%17,4	%35,0	%14,4
Mevcut sağlık verilerime yanlış ve eski bilgiler içerdiğini düşünüyorum.	%13,0	%17,4	%17,2	%36,6	%15,8
Sağlık verilerimin çalınabileceğini ve değiştirilebileceğini düşünüyorum.	%15,3	%21,6	%26,7	%25,8	%10,7
Sağlık verilerimin kazara kaybolabileceğini veya zarar görebileceğini düşünüyorum.	%16,4	%24,0	%25,2	%23,6	%10,9
Sağlık bilgilerimin bilgim olmadan 3.şahıslar ile paylaşıldığını düşünüyorum.	%17,4	%22,2	%31,2	%19,7	%9,4
Herhangi olumsuz bir durumun oluşması ihtimaline karşı (çalınması, kötüye kullanılması, vb.) sağlık verilerimin kurum, kuruluş ve kanunlarla korunduğuna inanıyorum.	%25,9	%22,7	%32,3	%13,3	%5,9

Dijital ortamlarda saklanan sağlık bilgilerinin kullanımı ile ilgili katılımcılara belirtilen ifadelere katılım derecelerini belirlemek için sorular sorulmuştur, katılımcıların verdikleri yanıtlara göre, Tüm sağlık verilerine internet üzerinden ulaşmak isteyen katılımcıların oranı %88,1'dir. Katılımcıların %81,7'si muayene oldukları doktorlarının, sağlık geçmişlerine erişebilmelerini istediklerini belirtmişlerdir. Katılımcıların, %84,6'sı ise sağlık kurumları (hastane, eczane vs) arasındaki işbirliğinin tedavileri için önemli ve yararlı olduklarını düşünmektedirler. Katılımcıların %86,1'i acil servise başvurmaları gerektiğinde başvurdukları acil servislerin sağlık verilerinin tamamına ulaşabilmelerini istemektedirler. Doktoru ile dijital ortamda (e-posta, anında mesajlaşma programları, vb.) iletişim kurmak isteyen katılımcı oranı ise %86,6'dır. Katılımcıların, %86,5ì ise doktorlarının, sağlık durumlarını uzaktan takip etmesini istemektedir. Muayene oldukları doktorlarının dijital ortamdaki sağlık verilerinden yararlandığını düşünen katılımcı oranı ise 77,9'dur. Kişisel sağlık bilgilerinin anonimleştirilerek, bilimsel araştırmalarda kullanılmasından rahatsız olmayacak katılımcı oranı ise %72,6'dır (Grafik-12) (Tablo-13).

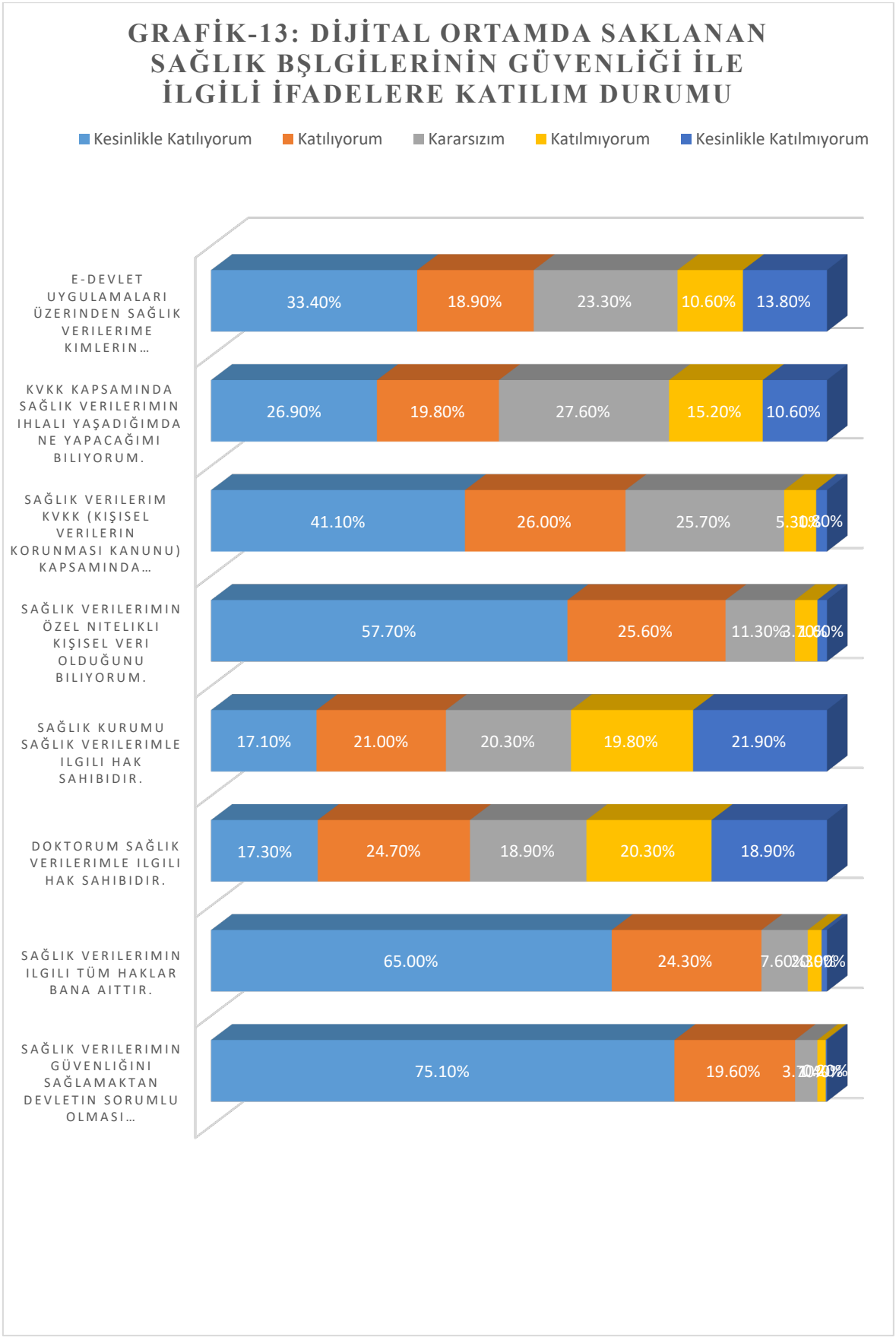


Grafik 12. Dijital Ortamda Saklanan Sağlık Bilgilerinin Kullanımı İle İlgili İfadelere Katılım Durumları

Tablo 14. Dijital Ortamda Saklanan Sağlık Bilgilerinin Kullanımı İle İlgili İfadelere Katılım Durumları

Sorular	Kesinlikle Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle Katılmıyorum
Kendime ait tüm sağlık verilerine İnternet üzerinden erişebilmek isterim.	%65,3	%22,8	%7,6	%3,0	%1,4
Muayene olduğum doktorun, tüm sağlık geçmişime erişebilmesini isterim.	%52,5	%29,2	%11,0	%5,3	%2,1
Sağlık kurumları (hastane, eczane vs.) arasındaki işbirliği tedavim için önemli ve yararlı olabilir.	%52,3	%32,3	%10,7	%3,5	%1,2
Acil servise başvurmam gerektiğinde sağlık verilerimin tamamına ulaşılabilmesini isterim.	%57,1	%29,0	%8,2	%4,1	%1,6
Doktorumla dijital ortamda iletişim kurmak (e-posta, anında mesajlaşma programları, vb.) isterim.	%61,9	%24,7	%7,8	%3,9	%1,8
Doktorumun sağlık durumumu uzaktan takip edebilmesini isterim.	%61,8	%24,7	%9,8	%3,0	%0,7
Doktorumun muayene sırasında dijital ortamdaki sağlık verilerimden yararlandığını düşünüyorum.	%46,2	%31,7	%14,9	%5,5	%1,6
Kişisel bilgilerim gizlenerek, sağlık verilerimin bilimsel araştırmalarda kullanılması beni rahatsız etmez.	%40,7	%31,9	%13,7	%6,9	%6,7

Dijital ortamlarda saklanan sağlık bilgilerinin güvenlik sorumlulukları ile ilgili bazı sorular yöneltilmiştir. Katılımcıların %94,7'si sağlık verilerinin güvenliğini sağlamaktan devletin sorumlu olması gerektiğini düşünmektedir. Kişisel sağlık verileri ile ilgili tüm hakların kendisine ait olduğunu düşünen katılımcı oranı %89,3'dür. Doktorlarının, sağlık verileri ilgili hak sahibi olduğunu düşünen katılımcıları oranı %42'dir. Başvurdukları sağlık kurumlarının sağlık verileri ile ilgili hak sahibi olduğunu düşünen katılımcıların oranı ise %38,1'dir. Sağlık verilerinin özel nitelikli kişisel veri olduğunun farkında olan katılımcı oranı %83,3'dür. Katılımcıların %67,1'i sağlık verilerinin Kişisel Verilerin Korunması Kanunu (KVKK) kapsamından korunduğunun farkında olduklarını belirtmişlerdir. Kişisel Verilerin Korunması Kanunu (KVKK) kapsamında, sağlık verileri ihlale uğradığında ne yapmaları gerektiğini bildiklerini belirten katılımcıların oranı %46,7'dir. E-devlet üzerinden sağlık verilerine kimlerin erişebileceği konusunda yetkilendirme yapabileceğini bilen kullanıcıların oranı ise %52,3'dür (Grafik-13) (Tablo-14).

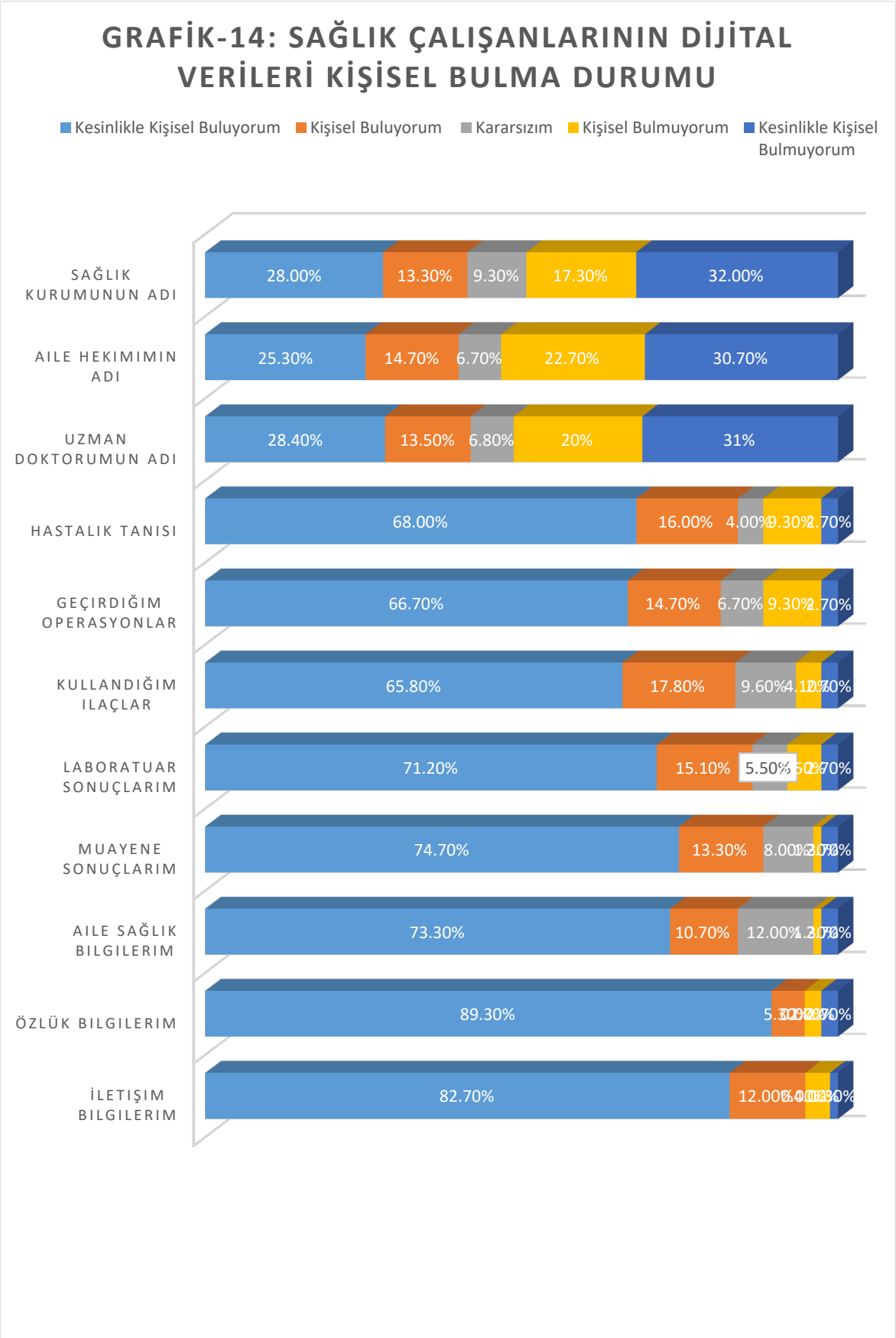


Grafik 13. Dijital Ortamda Saklanan Sağlık Bilgilerinin Güvenliği İle İlgili İfadelere Katılım Durumu

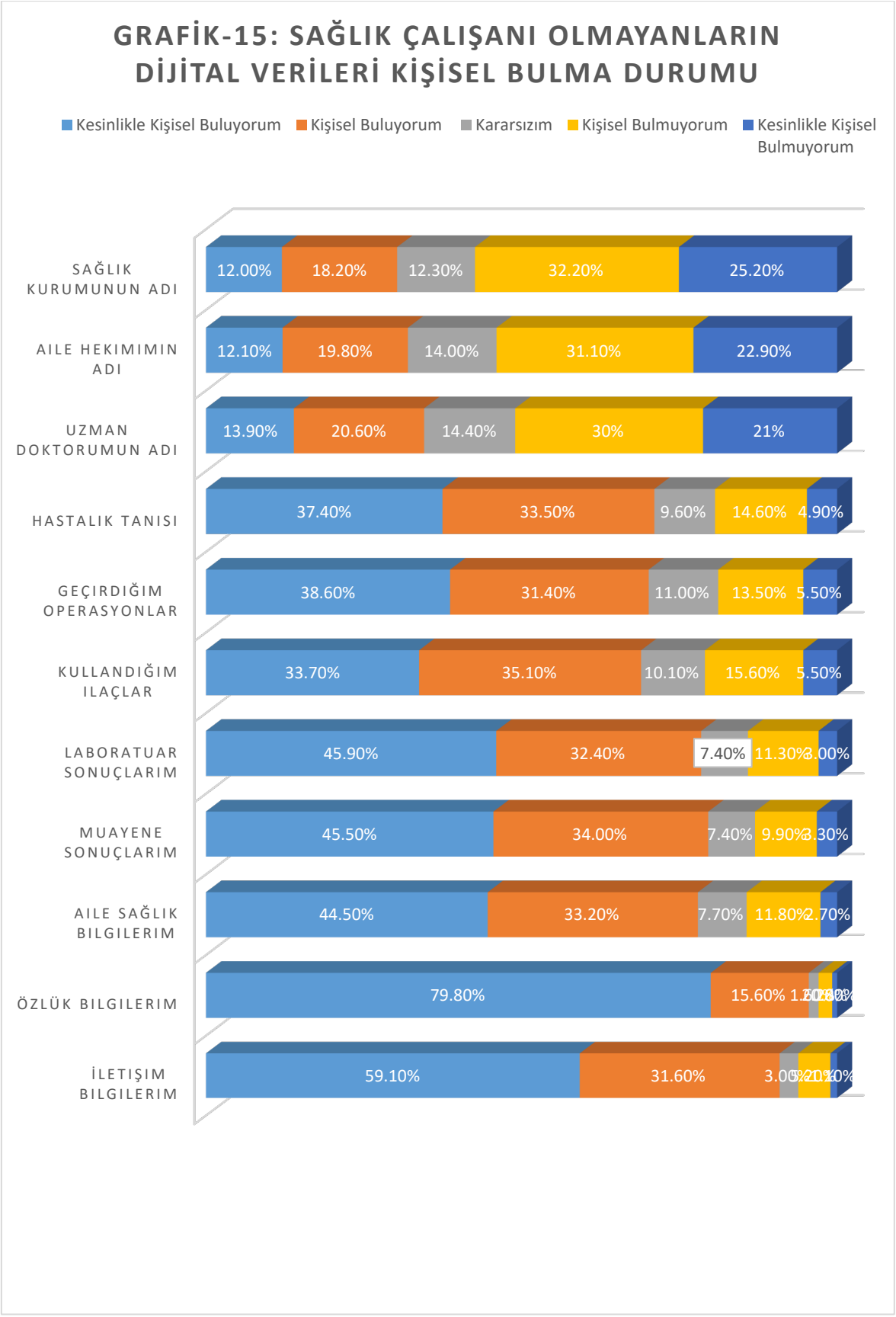
Tablo 15. Dijital Ortamda Saklanan Sağlık Bilgilerinin Güvenliği İle İlgili İfadelere Katılım Durumu

Sorular	Kesinlikle Katılıyorum	Katılıyorum	Kararsızım	Katılmıyorum	Kesinlikle Katılmıyorum
Sağlık verilerimin güvenliğini sağlamaktan devletin sorumlu olması gerektiğini düşünüyorum.	%75,1	%19,6	%3,7	%1,4	%0,2
Sağlık verilerimin ilgili tüm haklar bana aittir.	%65	%24,3	%7,6	%2,3	%0,9
Doktorum sağlık verilerimle ilgili hak sahibidir.	%17,3	%24,7	%18,9	%20,3	%18,9
Sağlık kurumu sağlık verilerimle ilgili hak sahibidir.	%17,1	%21	%20,3	%19,8	%21,9
Sağlık verilerimin özel nitelikli kişisel veri olduğunu biliyorum.	%57,7	%25,6	%11,3	%3,7	%1,6
Sağlık verilerim KVKK (Kişisel Verilerin Korunması Kanunu) kapsamında korunduğunu biliyorum.	%41,1	%26,0	%25,7	%5,3	%1,8
KVKK kapsamında sağlık verilerimin ihlali yaşadığımda ne yapacağımı biliyorum.	%26,9	%19,8	%27,6	%15,2	%10,6
E-devlet uygulamaları üzerinden sağlık verilerime kimlerin erişebileceği ile ilgili yetkilendirmeyi kendimin yapabileceğini biliyorum.	%33,4	%18,9	%23,3	%10,6	%13,8

Çalışmaya katılanlar, sağlık çalışanları ve sağlık sektöründe çalışmayanlar olarak iki farklı gruba ayrılarak kayıt altına alınan dijital sağlık verilerini kişisel bulup bulmadıkları ile ilgili sorulara verdikleri cevaplar değerlendirilmiştir. Verilen cevaplar doğrultusunda iletişim bilgileri (Adres, telefon, vb.), özlük bilgileri (TC kimlik no, doğum tarihi, vb.), aile sağlık bilgileri (Kalıtsal hastalıklar, genetik bilgiler, vb.), muayene sonuçları (şikayetler, doktor bulguları, vb.), laboratuar sonuçları (kan/idrar tahlilleri, röntgen, MR sonuçları, vb.), kullandığı ilaçlar, geçirdiği operasyonlar, hastalık tanıları, uzman doktorlarının adı, aile hekimlerinin adı, başvurdukları sağlık kurumunun adı (Hastane, Eczane, vb.) gibi elektronik ortamlarda kayıt altına alınan bilgilerdir. Sağlık çalışanlarının, %94,7'si iletişim bilgilerini kişisel bulurken sağlık sektöründe çalışmayan katılımcıların kişisel bulma oranı %90,7'dir. Özlük bilgilerini ise sağlık çalışanlarının, %94,6 sı kişisel bulurken sağlık sektöründe çalışmayan katılımcıların %95,4'ü kişisel bulduklarını belirtmişlerdir. Aile sağlık bilgilerinde ise sağlık çalışanlarının %84'ü kişisel bulurken sağlık sektöründe çalışmayan katılımcıların kişisel bulma oranları %77,7'dir. Muayene sonuçlarını kişisel bulan sağlık çalışanı katılımcı oranı %88 farklı sektör çalışanlarındaki kişisel bulma oranı ise %79'dur. Laboratuar sonuçlarını kişisel bulan sağlık çalışanı oranı %86,30,farklı sektör çalışanlarındaki kişisel bulma oranı ise %78,3'dür. Kullandığı ilaçları kişisel bulan sağlık çalışanlarının oranı %83,6,farklı sektör çalışanlarındaki oran ise %68,80'dir. Geçirdiği operasyonları kişisel bulan sağlık çalışanı oranı%81,40,farklı sektör çalışanlarındaki oran ise %70'dir. Hastalık tanılarını kişisel bulan sağlık çalışanı oranı %84,0,farklı sektör çalışanlarının oranı ise %70'dir. Sağlık çalışanlarının %41,9'u uzman doktorlarının adlarını kişisel bulurken farklı sektör çalışanlarında bu oran %34,50'dir. Benzer durumda sağlık çalışanlarının %40'ı aile hekimlerinin ismini kişisel bulurken farklı sektör çalışanlarında bu oran %31,9'dur. Sağlık çalışanlarının %41,30'u başvurdukları sağlık kurumlarının adını kişisel bulurken farklı sektör katılımcılarında bu oran %30,20'dir (Grafik-14) (Grafik-15).

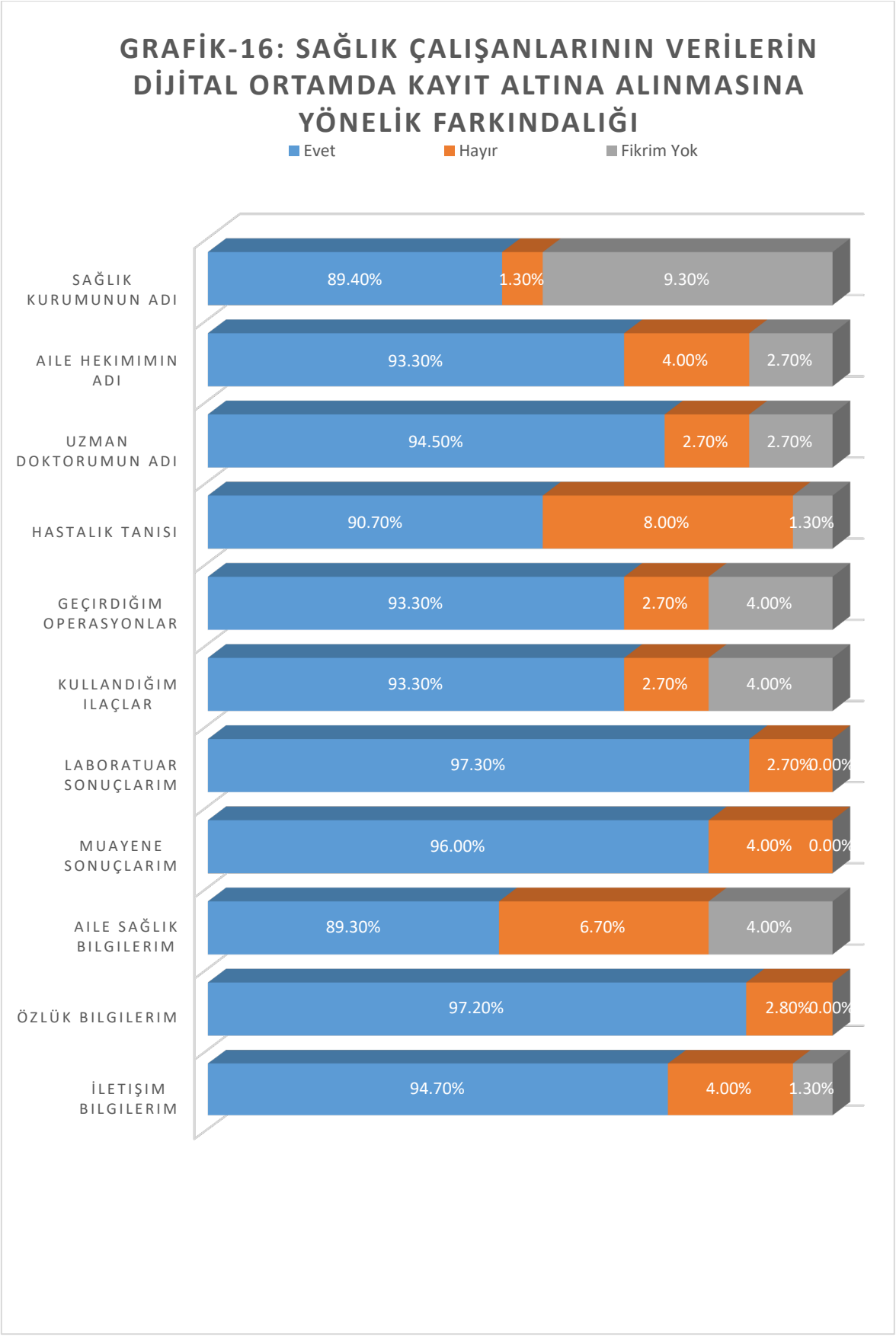


Grafik 14. Sağlık Çalışanlarının Dijital Verileri Kişisel Bulma Durumu

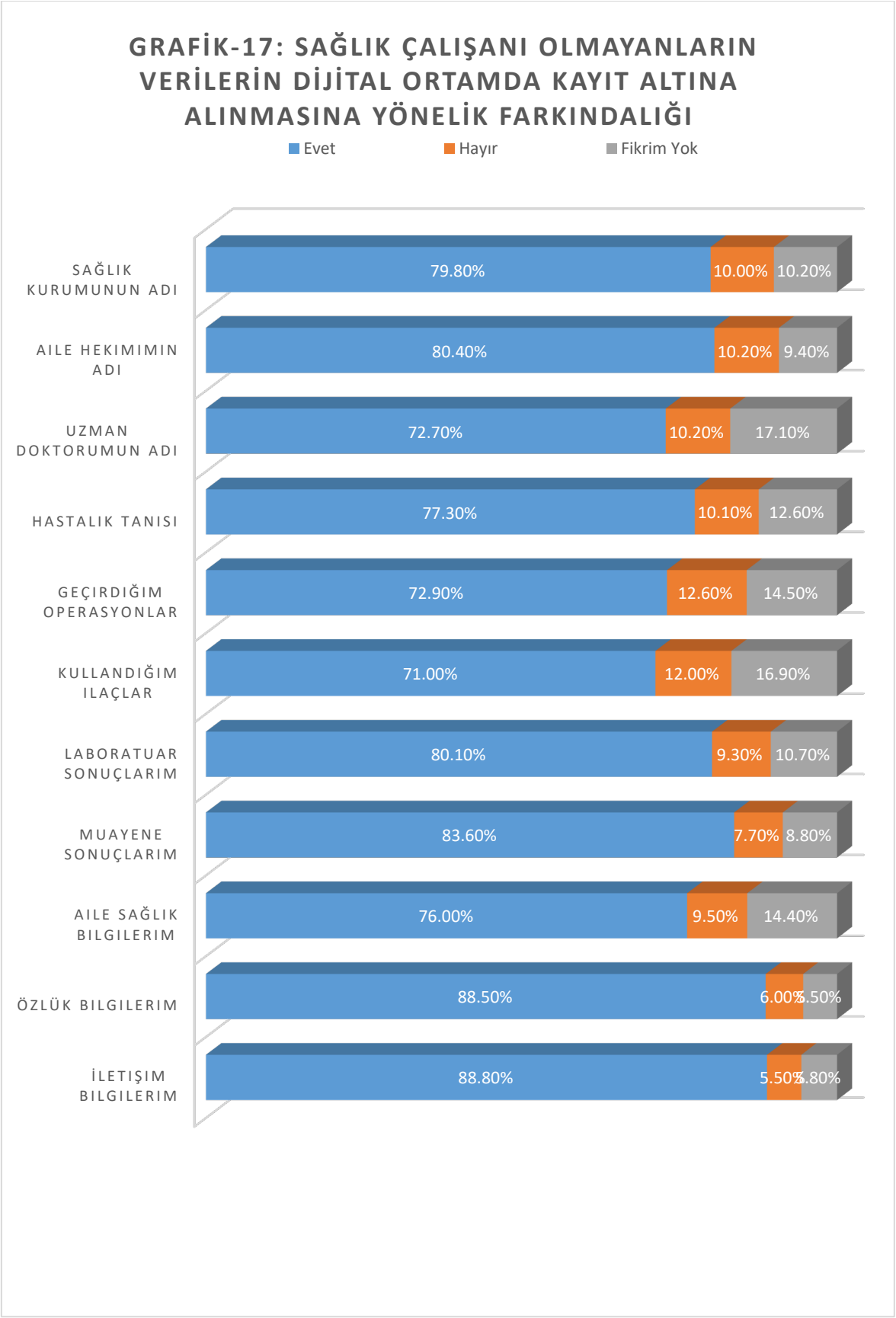


Grafik 15. Sağlık Çalışanı Olmayanların Dijital Verileri Kişisel Bulma Durumu

Çalışmaya katılanlar, sağlık çalışanları ve sağlık sektöründe çalışmayanlar olarak iki farklı gruba ayrılarak, sağlık verilerinin, dijital ortamlarda kayıt altına alındığının ve saklandığının farkındalığını ölçmek için sorular yönetilmiştir. İletişim bilgilerinin dijital ortamda kayıt altına alındığını bilen sağlık çalışanı oranı %94,7 iken farklı sektör çalışanlarında bu oran %88,8'dir. Özlük bilgilerinin kayıt altına alınıp, saklandığının farkında olan sağlık çalışanı oranı ise %97,2 farklı sektör çalışanlarının oranı ise %88,5'dir. Aile sağlık bilgilerinin dijital ortamlarda saklandığının farkında olan sağlık çalışanı %89,3 farklı sektör çalışanlarda ise bu oran %76'dır. Muayene sonuçlarının dijital ortamlarda saklandığının farkında olan sağlık çalışanı oranı %96,0 farklı sektör çalışanlarının oranı %83,6'dır. Sağlık çalışanlarının %97'3'ü laboratuar sonuçlarının dijital ortamlarda saklandığını bilmekteyken farklı sektör çalışanlarında bu oran %80,10'dur. Kullandığı ilaçların dijital ortamlarda saklandığını bilen sağlık çalışanı oranı ise %93,3 farklı sektör çalışanlarında ise bu oran %71,0'dır. Geçirdiği operasyonların dijital ortamlarda saklandığını bilen sağlık çalışanı oranı %93,3'dür. Farklı sektör çalışanlarında ise bu oran %72,9'dur. Hastalık tanılarının dijital ortamlarda kayıt edildiğini bilen sağık çalışanı oranı %90,7 farklı sektörde .çalışanlarda ise %77,3'dür. Uzman doktorunun adlarının dijital ortamlarda kayıt altına alındığını bilen sağlık çalışanı oranı %94,5 farklı sektör çalışanlarında bu oran %72'7'dir. Aile hekiminin adının dijital ortamlarda saklandığını bilen sağlık çalışanı oranı %93,3'dür. Farklı sektör çalışanlarında bu oran %80,4'dür. Sağlık kurmunun adının dijital ortamlarda kayıt altına alındığını bilen sağlık çalışanı oranı ise %89,4 iken farklı sektör çalışanlarında bu oran %79,8'dir (Grafik-16) (Grafik-17).

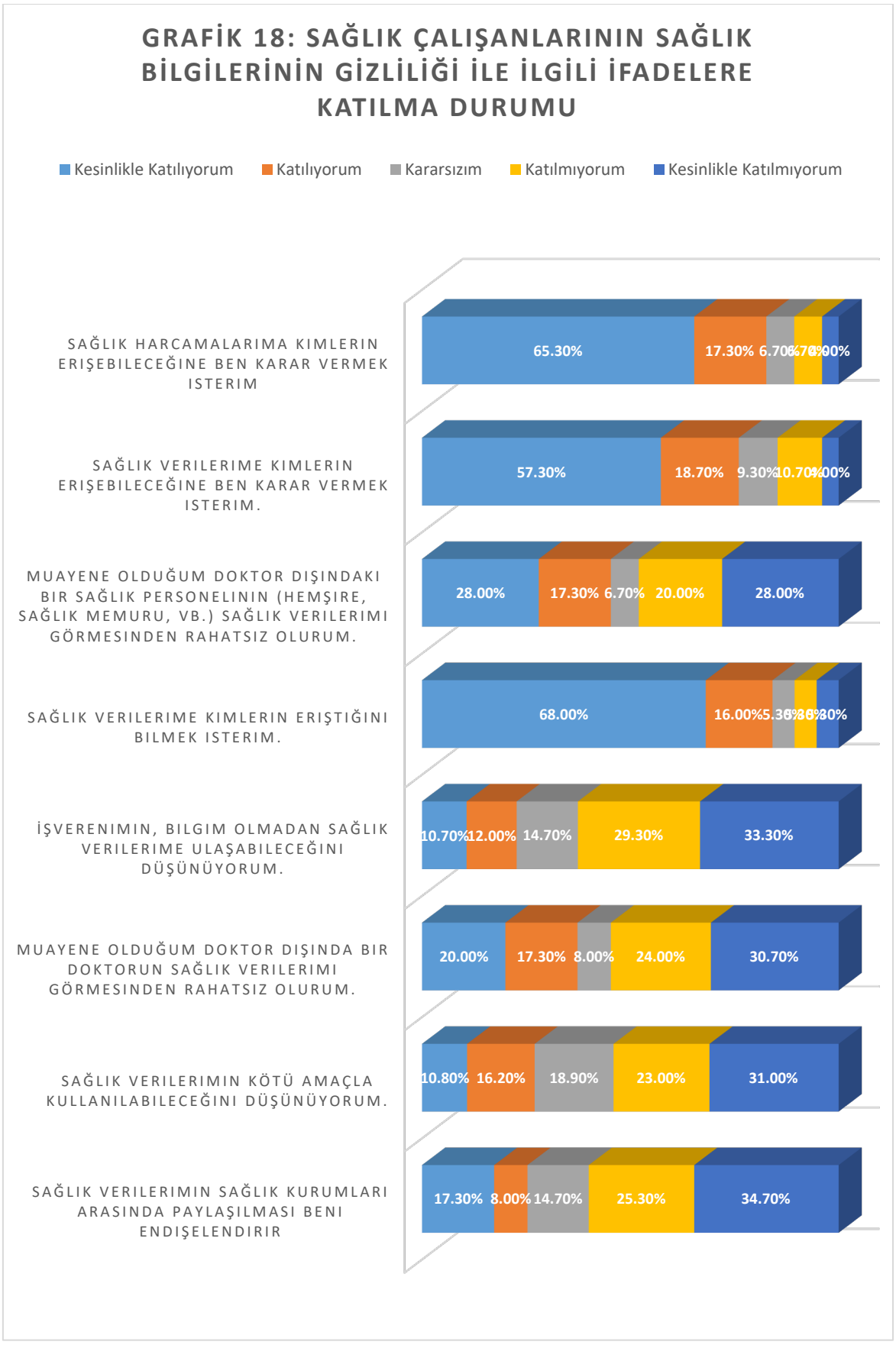


Grafik 16. Sağlık Çalışanlarının Verilerin Dijital Ortamda Kayıt Alınmasına Yönelik Farkındalığı

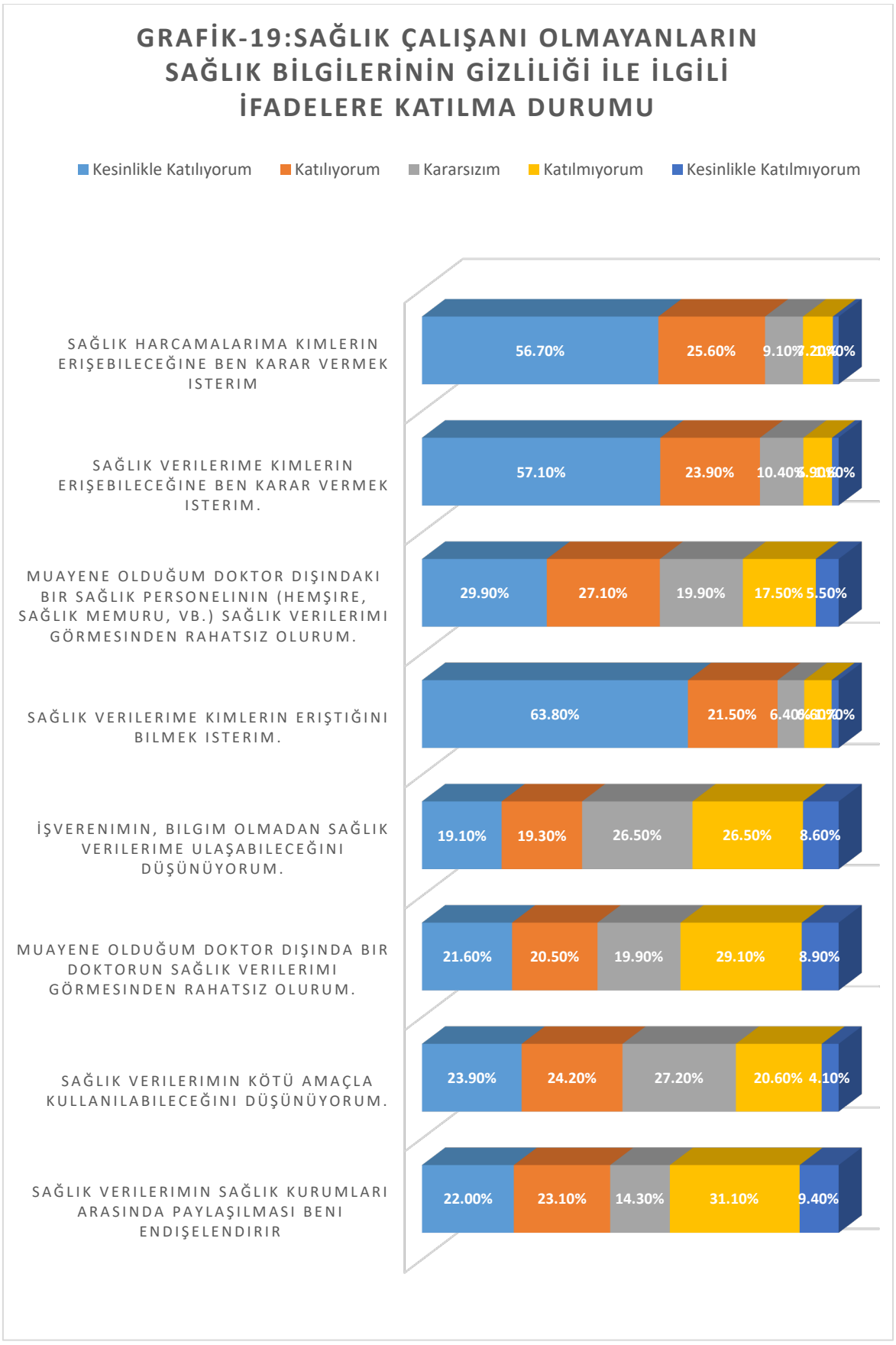


Grafik 17. Sağlık Çalışanı Olmayanların Verilerin Dijital Ortamda Kayıt Alınmasına Yönelik Farkındalığı

Çalışmaya katılanlar, sağlık çalışanları ve sağlık sektöründe çalışmayanlar olarak iki farklı gruba ayrılarak, sağlık bilgilerinin gizliliği ile ilgili bir takım ifadelere katılma derecelerini belirleyen sorular sorulmuştur. Sağlık çalışanlarının %25,3'ü kayıt altına alınan sağlık verilerinin sağlık kurumları arasında paylaşılmasından endişe duyacaklarını belirtirken farklı sektör çalışanlarında bu oran %45,1'dir. Sağlık çalışanlarının %27,0'ı mevcut sağlık verilerinin kötü amaçla kullanılabileceğini düşünmekteyken farklı sektör çalışanlarında bu oran %48,1'dir. Sağlık çalışanlarının muayene olduğu doktor dışında başka bir doktorun sağlık verilerini görmesinden rahatsız olacağını ifade edenlerin yüzdesi %37,3'dür. Farklı sektör çalışanlarında ise %42,1'dir. Sağlık çalışanlarından işverenlerinin sağlık verilerine izinsiz bir şekilde ulaşabileceklerini düşünenlerin oranı ise %22,7 iken farklı sektör çalışanlarında bu oran %38,4'dür. Sağlık verilerini kimlerin erişeceğini bilmek isteyen sağlık çalışanı oranı %84 farklı sektör çalışanlarında ise bu oran %85,3'dür. Muayene olduğu doktor dışında herhangi bir sağlık personelinin sağlık verilerini görmesinden rahatsız olacağını belirten sağlık çalışanı oranı ise %45,3'dür. Farklı sektör çalışanlarında oran %57'dir. Sağlık verilerine kimlerin erişeceğinin yetkilendirmesini yapmak isteyen sağlık çalışanı oranı ise %76 iken farklı sektör çalışanlarında oran %81'dir. Sağlık harcamalarına kimlerin erişebileceğini kendisinin karar vermesini isteyen sağlık çalışanı oranı %82,5 farklı sektör çalışan oranı ise %82,3'dür.(Grafik-18) (Grafik-19).

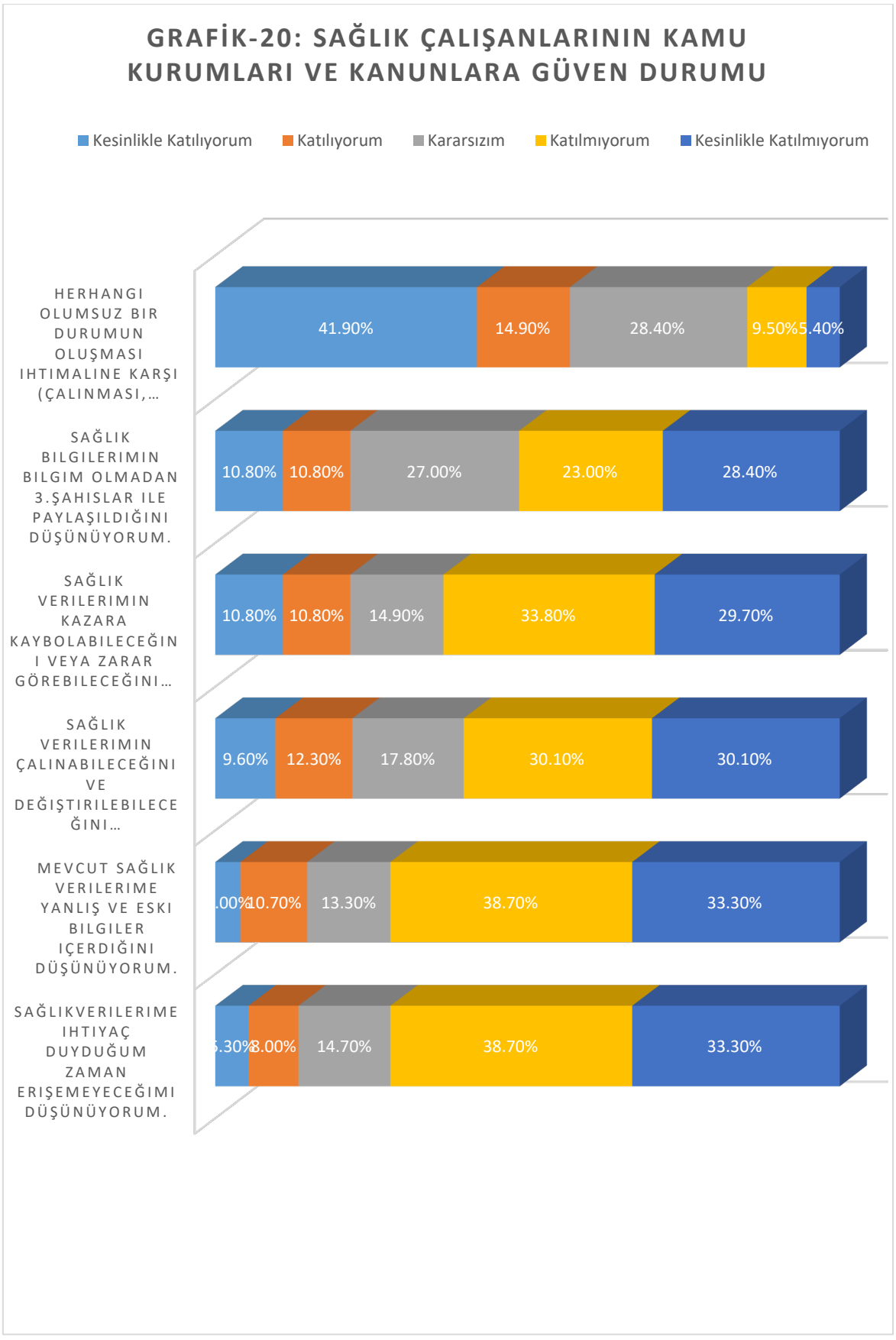


Grafik 18. Sağlık Çalışanlarının Sağlık Bilgilerinin Gizliliği ile İlgili İfadelere Katılma Durumu

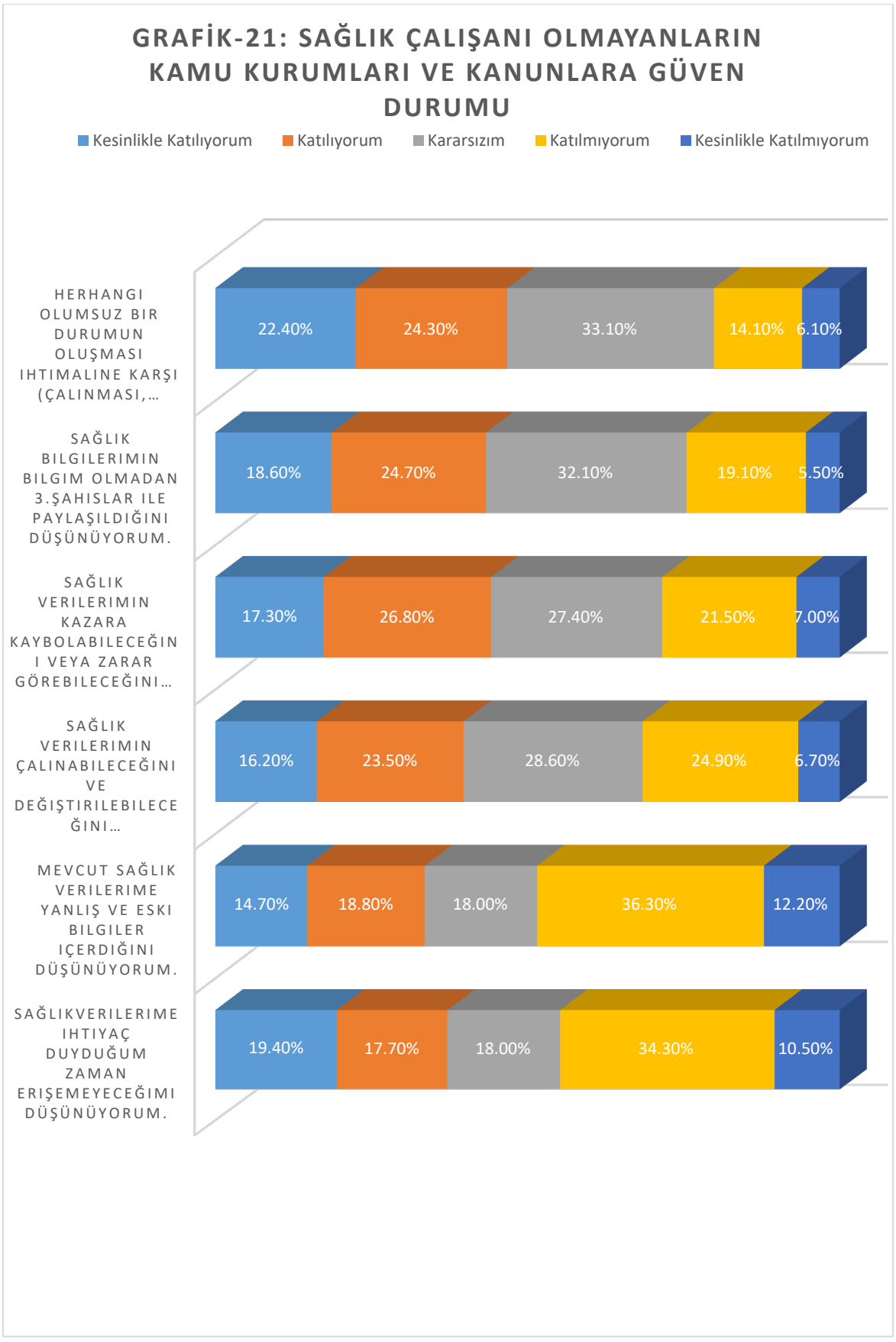


Grafik 19. Sağlık Çalışanı Olmayanların Sağlık Bilgilerinin Gizliliği ile İlgili İfadelere Katılma Durumu

Çalışmaya katılanlar, sağlık çalışanları ve sağlık sektöründe çalışmayanlar olarak iki farklı gruba ayrılarak, sağlık bilgilerinin dijital ortamda saklanmasıyla ilgili verilen ifadelere katılma derecelerini ölçmek amacıyla bazı sorular sorulmuştur. Katılımcıların verdikleri cevaplar neticesinde, sağlık verilerine ihtiyaç duydukları anda erişemeyeceğini düşünen sağlık çalışanı oranı %13,8'dir. Farklı sektör çalışanlarında bu oran %37,1'dir. Sağlık çalışanlarının %14,70'i mevcut sağlık verilerinin yanlış ve eski bilgiler içerdiğini düşünürken farklı sektör çalışanlarında bu oran %33,5'dir. Sağlık çalışanlarının %21,9'u sağlık verilerinin çalınabilip, değiştirilebileceğini düşünürken farklı sektör çalışanlarının %39,7'si sağlık verilerinin çalınabilip, değiştirilebileceğini düşünmektedir. Sağlık verilerinin kazara kaybolabileceğini düşünen sağlık çalışanı oranı %21,6'dır. Farklı sektör çalışanlarında bu oran %44,1'dir. Sağlık bilgilerinin, bilgileri dahili olmadan üçümcü şahıslar ile paylaşıldığını düşünen sağlık çalışanı oranı %21,6'dır. Farklı sektör çalışanlarında bu oran %43,6'dır. Sağlık verilerinin çalınması, kötüye kullanılması gibi durumlarda kamu kurum, kuruluş ve kanunlarla korunduğunu düşünen sağlık çalışanı oranı ise %56,8'dir. Farklı sektör çalışanlarının ise %46,7'si sağlık verilerinin çalınması, kötüye kullanılması gibi durumlarda kamu kurum, kuruluş ve kanunlarla korunduğunu düşünmektedir.(Grafik-20) (Grafik-21).

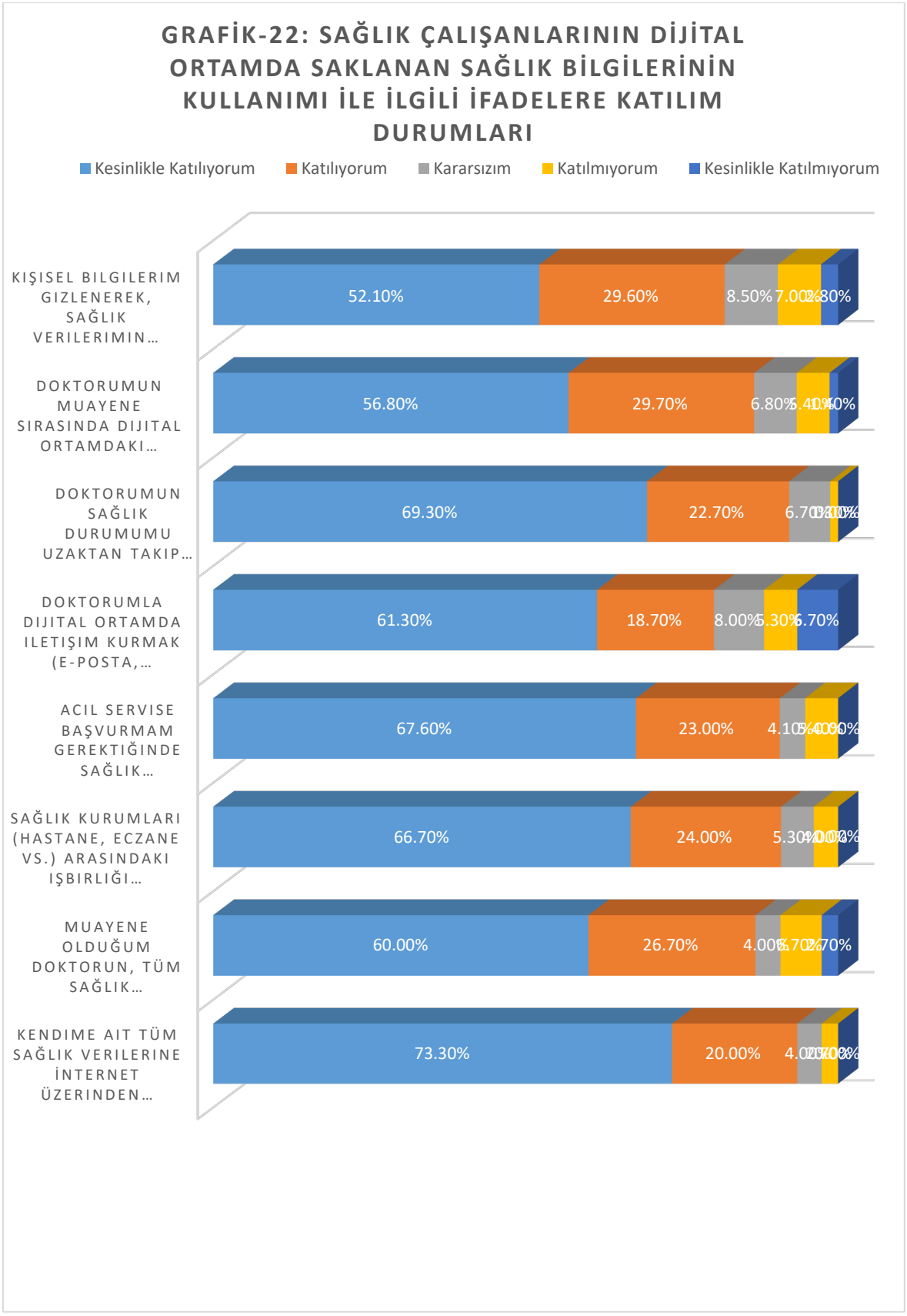


Grafik 20. Sağlık Çalışanlarının Kamu Kurumları ve Kanunlara Güven Durumları

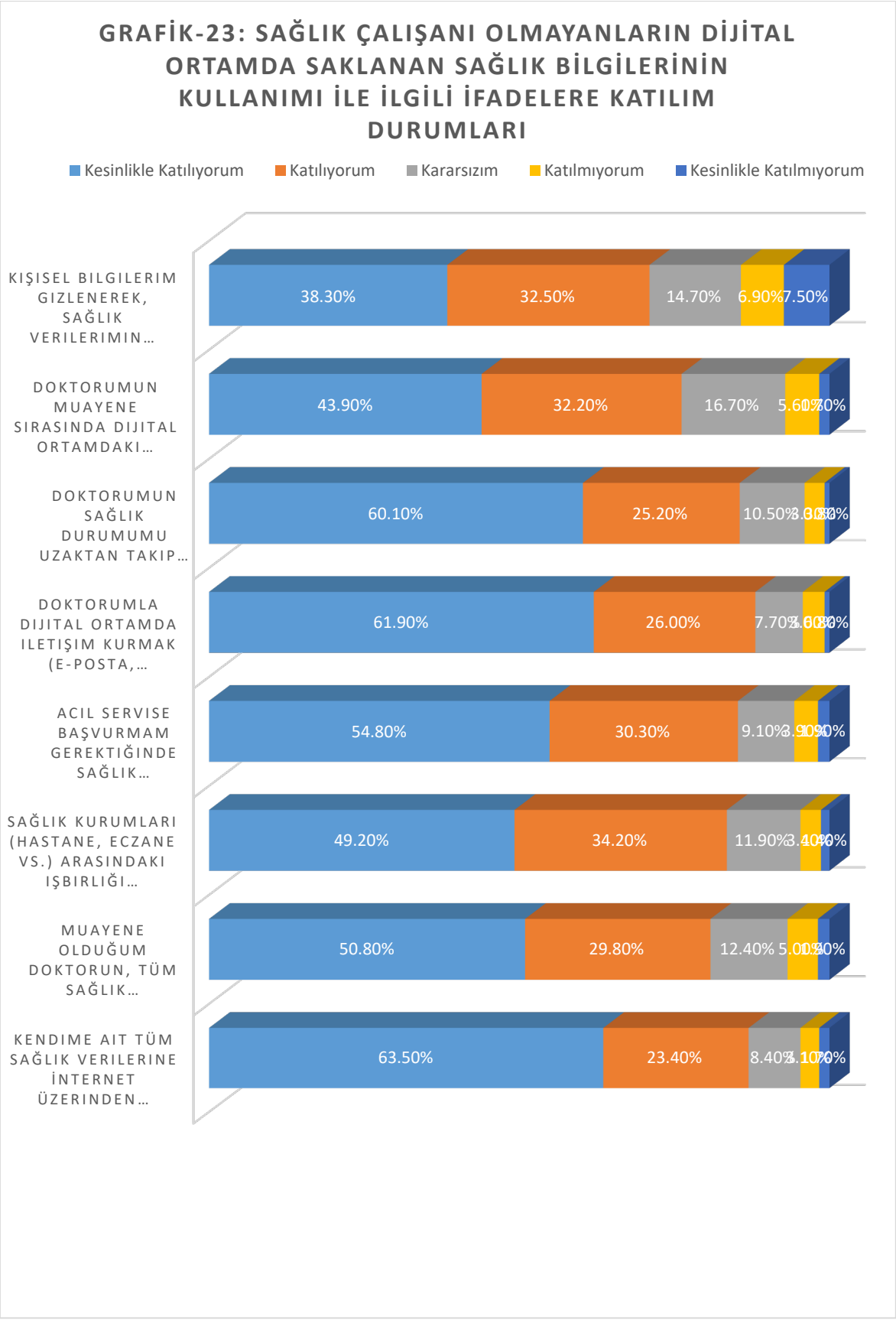


Grafik 21. Sağlık Çalışanı Olmayanların Kamu Kurumları ve Kanunlara Güven Durumları

Çalışmaya katılanlar, sağlık çalışanları ve sağlık sektöründe çalışmayanlar olarak iki farklı gruba ayrılarak, dijital ortamlarda saklanan sağlık bilgilerinin kullanımı ile ilgili belirtilen ifadelere katılım derecelerini belirlemek için sorular sorulmuştur, Katılımcıların verdikleri yanıtlara göre, Tüm sağlık verilerine internet üzerinden ulaşmak isteyen sağlık çalışanı oranı %93,1 iken farklı sektör çalışanlarında bu oran %86,9'dur. Sağlık çalışanlarının %86,7'si muayene oldukları doktorlarının, sağlık geçmişlerine erişebilmelerini istediklerini belirtirken farklı sektör çalışanlarının %80,6'sı muayene oldukları doktorlarının, sağlık geçmişlerine erişebilmelerini istediklerini belirtmişlerdir. Sağlık çalışanlarının, %90,7'si sağlık kurumları (hastane, eczane vs) arasındaki işbirliğinin tedavileri için önemli ve yararlı olduklarını düşünmektedirler. Farklı sektör çalışanlarında bu oran %83,4'dür. Sağlık çalışanlarının %90,6'sı acil servise başvurmaları gerektiğinde başvurdukları acil servislerin sağlık verilerinin tamamına ulaşabilmelerini isterken farklı sektör çalışanlarında bu oran %85,1'dir. Doktoru ile dijital ortamda (e-posta, anında mesajlaşma programları, vb.) iletişim kurmak isteyen sağlık çalışanı oranı ise %78'dir. Farklı sektör çalışanlarında bu oran %87,9'dur. Sağlık çalışanlarının, %92'si farklı sektör çalışanlarının ise %85,3'ü doktorlarının, sağlık durumlarını uzaktan takip etmesini istemektedir. Muayene oldukları doktorlarının dijital ortamdaki sağlık verilerinden yararlandığını düşünen sağlık çalışanı oranı ise 86,5'dir. Farklı sektör çalışanlarında bu oran %76,1'dir. Kişisel sağlık bilgilerinin anonimleştirilerek, bilimsel araştırmalarda kullanılmasından rahatsız olmayacak sağlık çalışanı oranı ise %81,7 iken farklı sektör çalışanlarında bu oran 70,8'dir (Grafik-22) (Grafik-23).

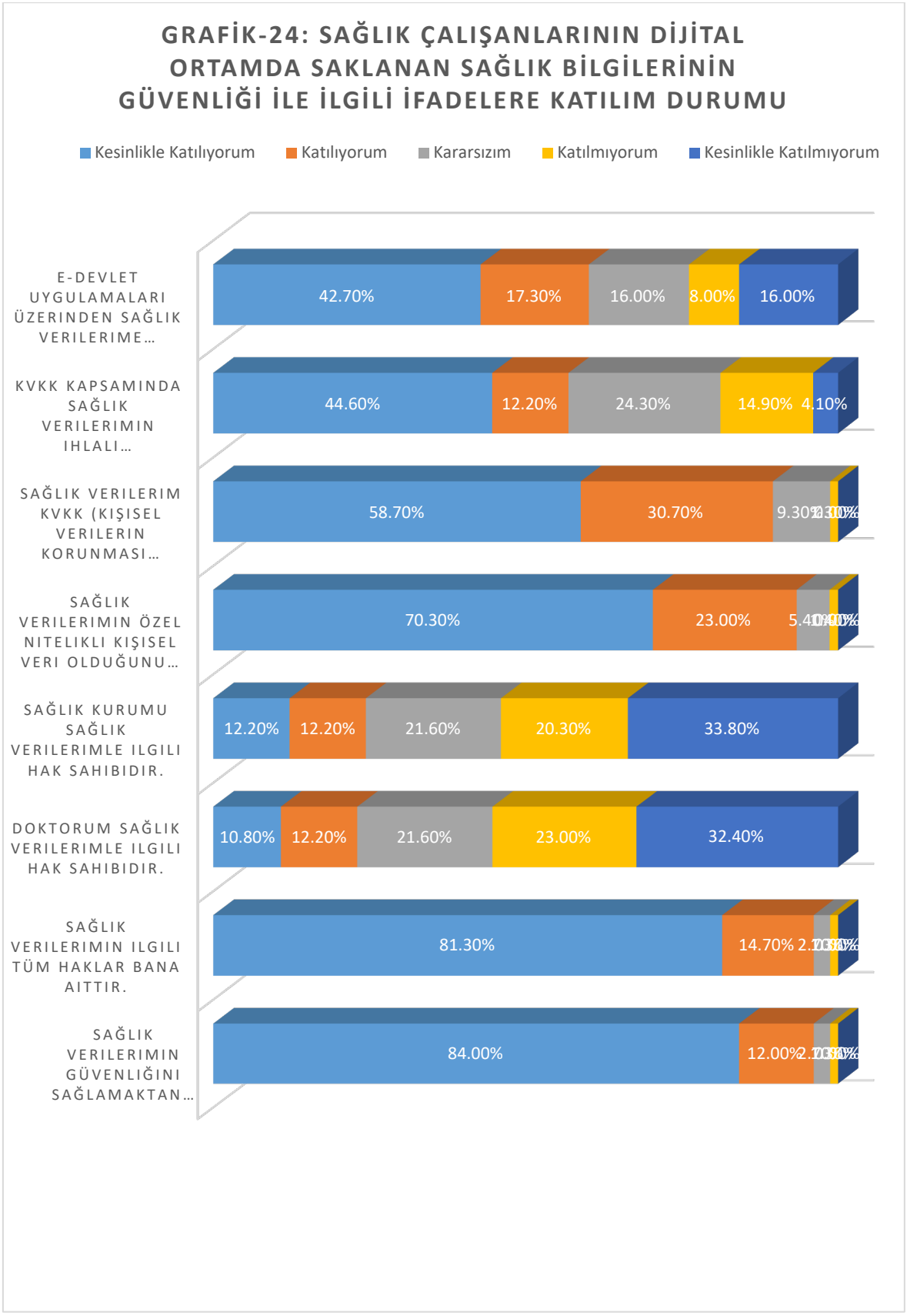


Grafik 22. Sağlık Çalışanlarının Dijital Ortamlarda Saklanan Sağlık Bilgilerinin Kullanımı İle İlgili İfadelere Katılım Durumları

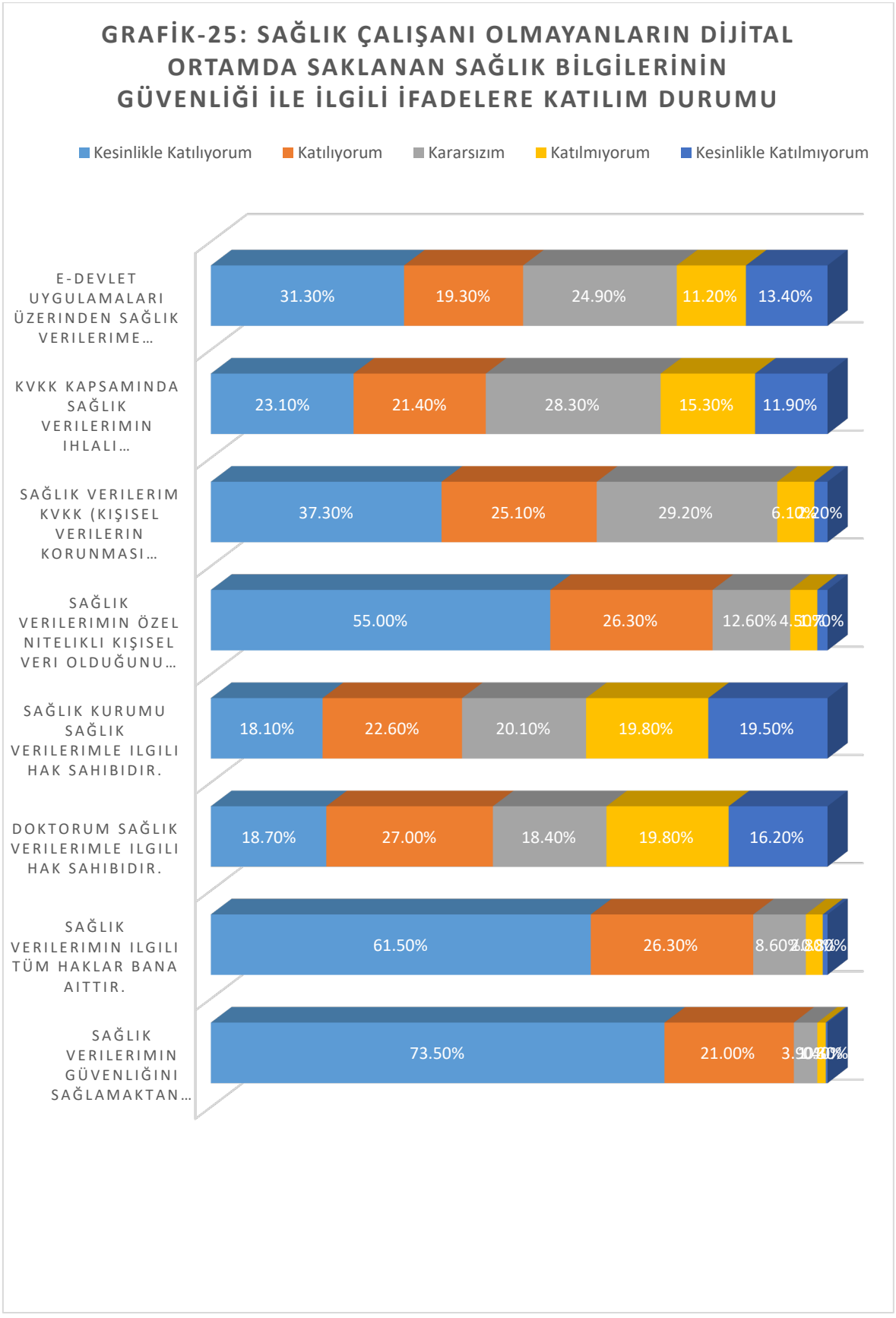


Grafik 23. Sağlık Çalışanı Olmayanların Dijital Ortamlarda Saklanan Sağlık Bilgilerinin Kullanımı İle İlgili İfadelere Katılım Durumları

Çalışmaya katılanlar, sağlık çalışanları ve sağlık sektöründe çalışmayanlar olarak iki farklı gruba ayrılarak, dijital ortamlarda saklanan sağlık bilgilerinin güvenlik sorumlulukları ile ilgili bazı sorular yöneltilmiştir. Sağlık çalışanlarının %96'sı sağlık verilerinin güvenliğini sağlamaktan devletin sorumlu olması gerektiğini düşünürken farklı sektör çalışanlarının %94,5'i düşünmektedir. Kişisel sağlık verileri ile ilgili tüm hakların kendisine ait olduğunu düşünen sağlık çalışanı oranı %96'dır. Bu oran farklı sektör çalışanlarında %87,8'dir. Doktorlarının, sağlık verileri ilgili hak sahibi olduğunu düşünen sağlık çalışanı oranı %23 iken farklı sektör çalışanlarında bu oran %45,7'dir. Başvurdukları sağlık kurumlarının sağlık verileri ile ilgili hak sahibi olduğunu düşünen sağlık çalışanı oranı %24,4'dür. Farklı sektör çalışanlarında bu oran %40,7'dir. Sağlık verilerinin özel nitelikli kişisel veri olduğunun farkında olan sağlık çalışanı oranı %93,3'dür. Bu oran farklı sektör çalışanlarında %81,3'dür. Sağlık çalışanlarının %89,4'ü sağlık verilerinin Kişisel Verilerin Korunması Kanunu (KVKK) kapsamından korunduğunun farkında olduklarını belirtirken bu oran farklı sektör çalışanlarında %62,4'dür. Kişisel Verilerin Korunması Kanunu (KVKK) kapsamında, sağlık verileri ihlale uğradığında ne yapmaları gerektiğini bildiklerini belirten sağlık çalışanı oranı %56,8 iken farklı sektör çalışanlarında bu oran %44,5'dir. E-devlet üzerinden sağlık verilerine kimlerin erişebileceği konusunda yetkilendirme yapabileceğini bilen katılımcı oranı ise %60'dır. Bu oran farklı sektör çalışanlarında %50,6'dır (Grafik-24) (Grafik-25).



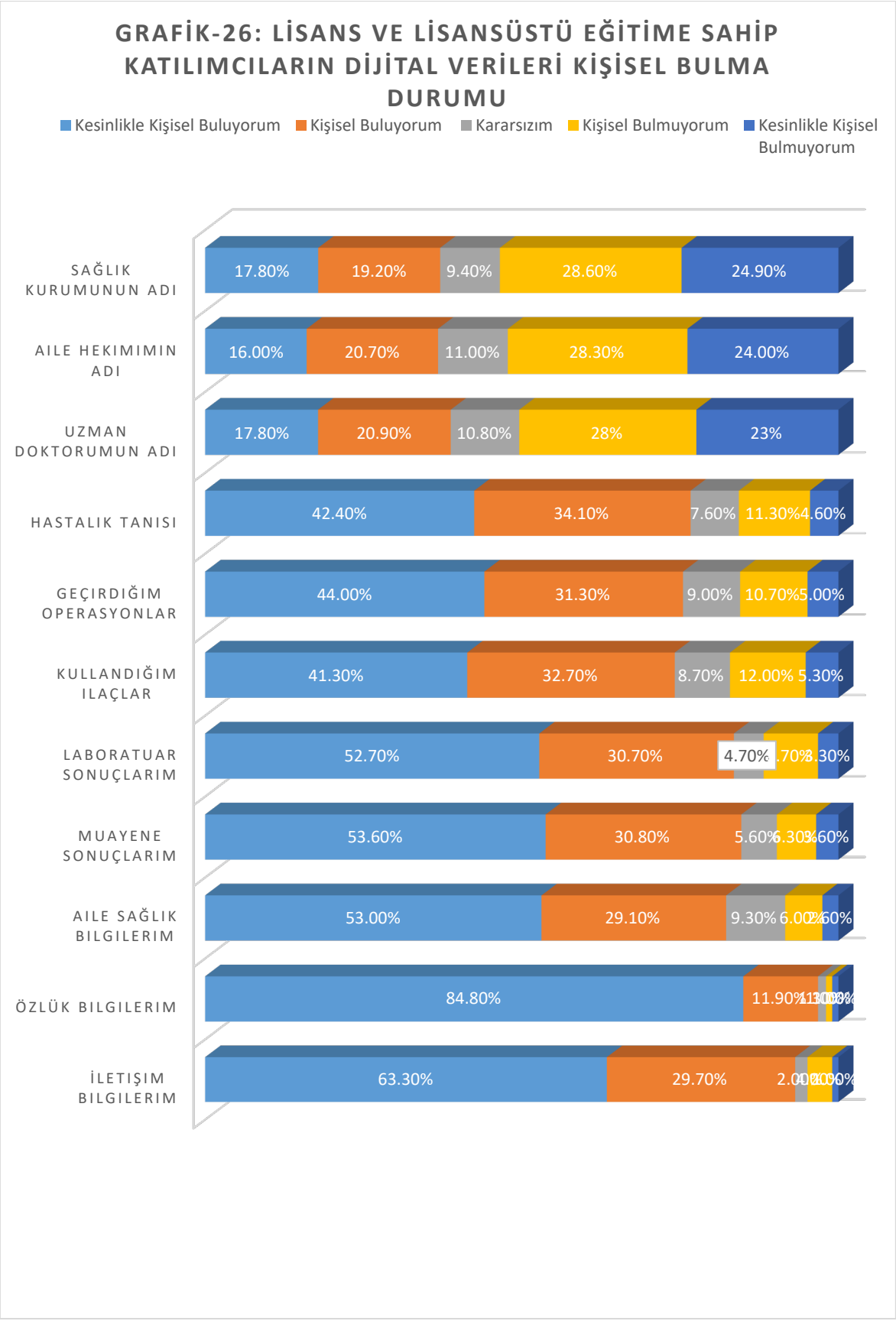
Grafik 24. Sağlık Çalışanlarının Dijital Ortamda Saklanan Sağlık Bilgilerinin Güvenliği ile İlgili İfadele Katılım Durumu



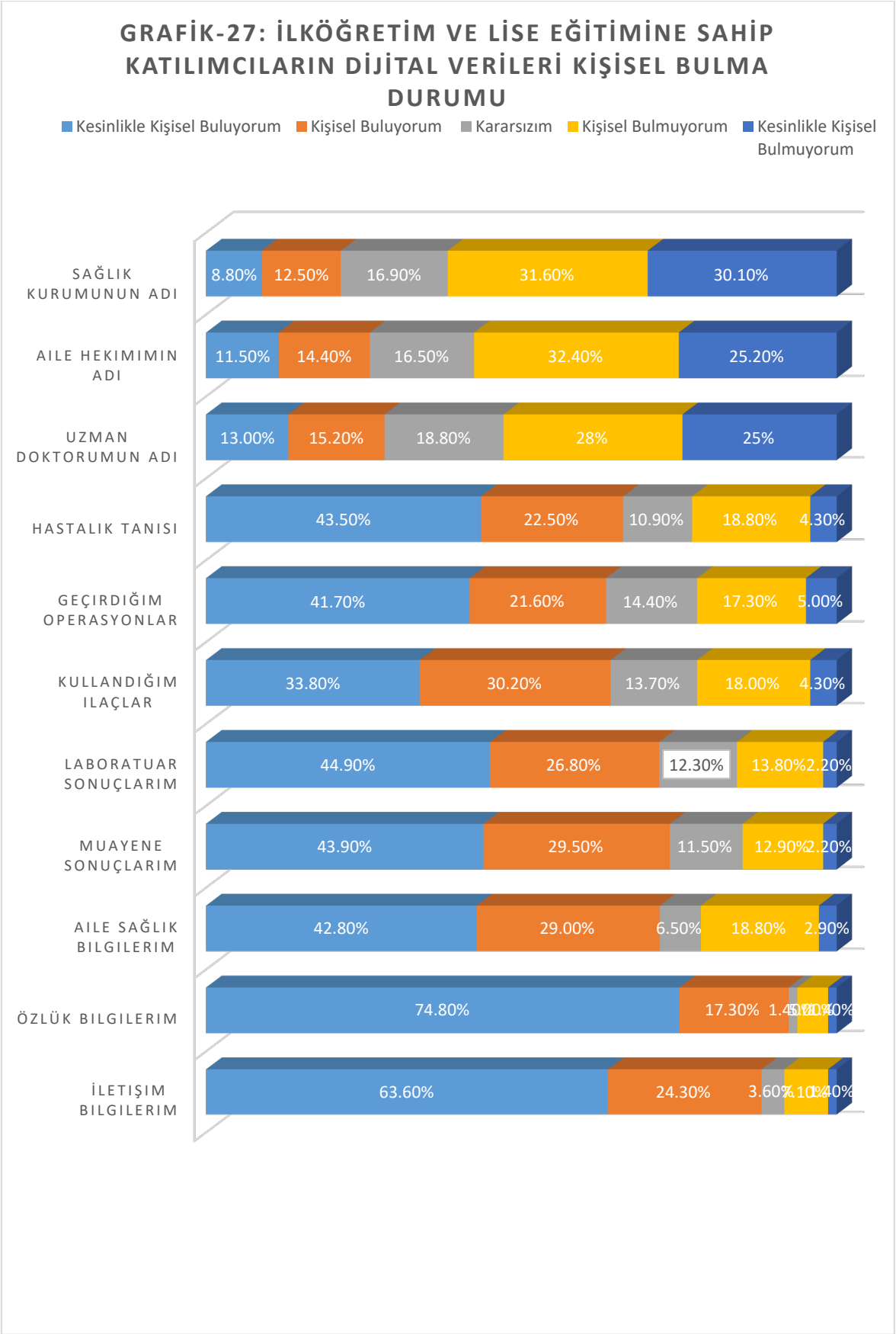
Grafik 25. Sağlık Çalışanı Olmayanların Dijital Ortamda Saklanan Sağlık Bilgilerinin Güvenliği ile İlgili İfadele Katılım Durumu

Çalışmaya katılanlar, lisans-lisansüstü ve ilköğretim-lise eğitimine sahip katılımcılar olarak iki farklı gruba ayrılarak kayıt altına alınan dijital sağlık verilerini kişisel bulup bulmadıkları ile ilgili sorulara verdikleri cevaplar değerlendirilmiştir. Verilen cevaplar doğrultusunda iletişim bilgileri (Adres, telefon, vb.), özlük bilgileri (TC kimlik no, doğum tarihi, vb.), aile sağlık bilgileri (Kalıtsal hastalıklar, genetik bilgiler, vb.), muayene sonuçları (şikayetler, doktor bulguları, vb.), laboratuar sonuçları (kan/idrar tahlilleri, röntgen, MR sonuçları, vb.), kullandığı ilaçlar, geçirdiği operasyonlar, hastalık tanıları, uzman doktorlarının adı, aile hekimlerinin adı, başvurdukları sağlık kurumunun adı (Hastane, Eczane, vb.) gibi elektronik ortamlarda kayıt altına alınan bilgilerdir. Lisans ve lisansüstü eğitime sahip katılımcıların, %91'i iletişim bilgilerini kişisel bulurken ilköğretim ve lise eğitimine sahip katılımcıların kişisel bulma oranı %87,9'dur. Özlük bilgilerini ise lisans ve lisansüstü eğitime sahip katılımcıların, %96,7'si kişisel bulurken ilköğretim ve lise eğitimine sahip katılımcıların %92,1'i kişisel bulduklarını belirtmişlerdir. Aile sağlık bilgilerinde ise lisans ve lisansüstü eğitime sahip katılımcıların %81,1'i kişisel bulurken ilköğretim ve lise eğitimine sahip katılımcıların kişisel bulma oranları %71,8'dir. Muayene sonuçlarını kişisel bulan lisans ve lisansüstü eğitime sahip katılımcıların oranı %84,4 iken ilköğretim ve lise eğitimine sahip katılımcıların kişisel bulma oranı ise %73,4'dür. Laboratuar sonuçlarını kişisel bulan lisans ve lisansüstü eğitime sahip katılımcıların oranı %83,4 ilköğretim ve lise eğitimine sahip katılımcıların kişisel bulma oranı ise %71,7'dir. Kullandığı ilaçları kişisel bulan lisans ve lisansüstü eğitime sahip katılımcıların oranı %74,ilköğretim ve lise eğitimine sahip katılımcılarının oranı ise %64'dür. Geçirdiği operasyonları kişisel bulan . Lisans ve lisansüstü eğitime sahip katılımcıların oranı %75,3 ilköğretim ve lise eğitimine sahip katılımcıların oranı ise %63,3'dür. Hastalık tanılarını kişisel bulan . Lisans ve lisansüstü eğitime sahip katılımcıların oranı %76,5 ilköğretim ve lise eğitimine sahip katılımcıların oranı ise %66'dır. Lisans ve lisansüstü eğitime sahip katılımcıların %38,7'si uzman

doktorlarının adlarını kişisel bulurken Lisans ve lisansüstü eğitime sahip katılımcılarda bu oran %28,20'dir. Benzer durumda Lisans ve lisansüstü eğitime sahip katılımcıların %36,7'si aile hekimlerinin ismini kişisel bulurken ilköğretim ve lise eğitimine sahip katılımcılarda bu oran %25,9'dur. Lisans ve lisansüstü eğitime sahip katılımcıların %37'si başvurdukları sağlık kurumlarının adını kişisel bulurken ilköğretim ve lise eğitimine sahip katılımcılarda bu oran %21,3'dür (Grafik-26) (Grafik-27).



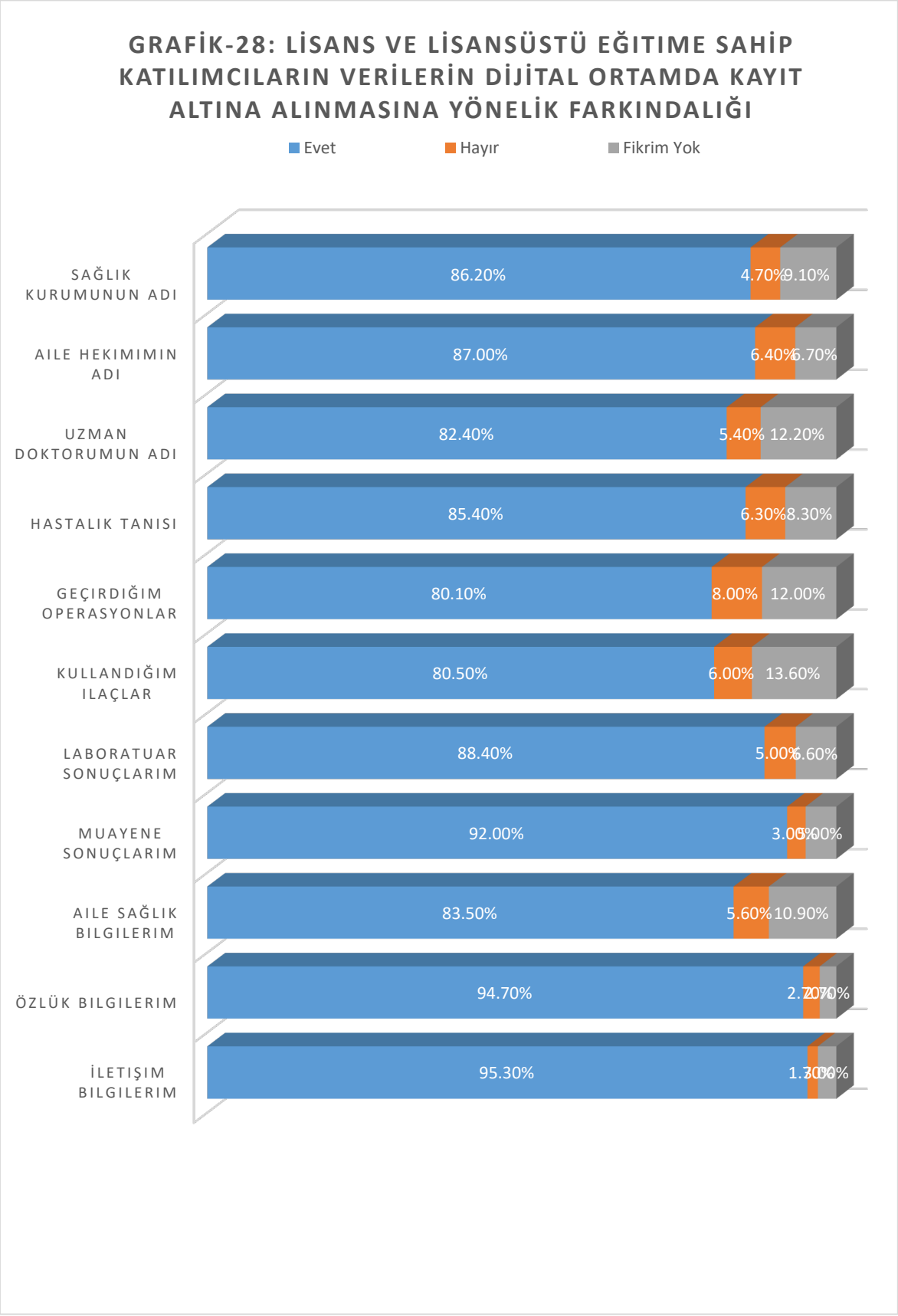
Grafik 26. Lisans ve Lisansüstü Eğitime Sahip Katılımcıların Dijital Verileri Kişisel Bulma Durumu



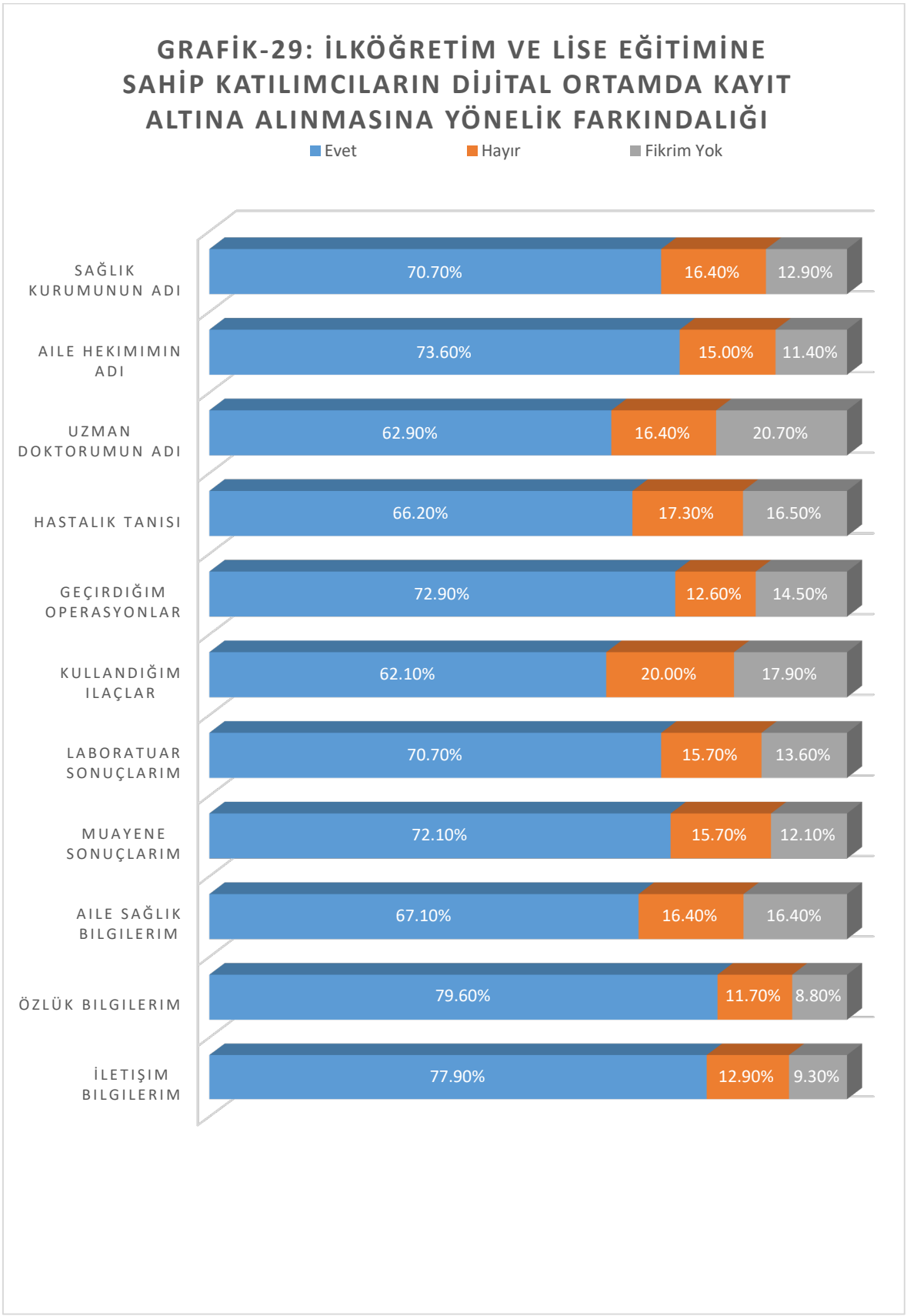
Grafik 27. İlk Öğretim ve Lise Eğitimine Sahip Katılımcıların Dijital Verileri Kişisel Bulma Durumu

Çalışmaya katılanlar, lisans-lisansüstü ve ilköğretim-lise eğitimine sahip katılımcılar olarak iki farklı gruba ayrılarak, sağlık verilerinin, dijital ortamlarda kayıt altına alındığının ve saklandığının farkındalığını ölçmek için sorular yönetilmiştir. İletişim bilgilerinin dijital ortamda kayıt altına alındığını bilen . Lisans ve lisansüstü eğitime sahip katılımcıların oranı %95,3 iken ilköğretim ve lise eğitimine sahip katılımcılarda bu oran %77,9'dur. Özlük bilgilerinin kayıt altına alınıp, saklandığının farkında olan . Lisans ve lisansüstü eğitime sahip katılımcıların oranı ise %94,7 ilköğretim ve lise eğitimine sahip katılımcıların oranı ise %79,6'dır. Aile sağlık bilgilerinin dijital ortamlarda saklandığının farkında olan Lisans ve lisansüstü eğitime sahip katılımcıların oranı %83,5 ilköğretim ve lise eğitimine sahip katılımcılarda ise bu oran %67,1'dir. Muayene sonuçlarının dijital ortamlarda saklandığının farkında olan . Lisans ve lisansüstü eğitime sahip katılımcıların oranı %92,0 ilköğretim ve lise eğitimine sahip katılımcıların oranı %72,1'dir. Lisans ve lisansüstü eğitime sahip katılımcıların %88,4'ü laboratuar sonuçlarının dijital ortamlarda saklandığını bilmekteyken ilköğretim ve lise eğitimine sahip katılımcılarda bu oran %70,7'dir. Kullandığı ilaçların dijital ortamlarda saklandığını bilen . Lisans ve lisansüstü eğitime sahip katılımcıların oranı ise %80,5 ilköğretim ve lise eğitimine sahip katılımcılarda ise bu oran %62,1'dir. Geçirdiği operasyonların dijital ortamlarda saklandığını bilen . Lisans ve lisansüstü eğitime sahip katılımcıların oranı %80,1'dir. Ilköğretim ve lise eğitimine sahip katılımcılarda ise bu oran %72,9'dur. Hastalık tanılarının dijital ortamlarda kayıt edildiğini bilen sağık çalışanı oranı %85,4 Ilköğretim ve lise eğitimine sahip katılımcılarda ise bu oran %66,2'dir. Uzman doktorunun adlarının dijital ortamlarda kayıt altına alındığını bilen . Lisans ve lisansüstü eğitime sahip katılımcıların oranı %82,4 ilköğretim ve lise eğitimine sahip katılımcılarda bu oran %62,9'dur. Aile hekiminin adının dijital ortamlarda saklandığını bilen . Lisans ve lisansüstü eğitime sahip katılımcıların oranı %87'dir. Ilköğretim ve lise eğitimine sahip katılımcılarda bu oran %73,6'dır. Sağlık kurmunun adının dijital ortamlarda kayıt altına

alındığını bilen . Lisans ve lisansüstü eğitime sahip katılımcıların oranı ise %86,2 iken ilköğretim ve lise eğitimine sahip katılımcılardabu oran %70,7'dir (Grafik-28) (Grafik-29)



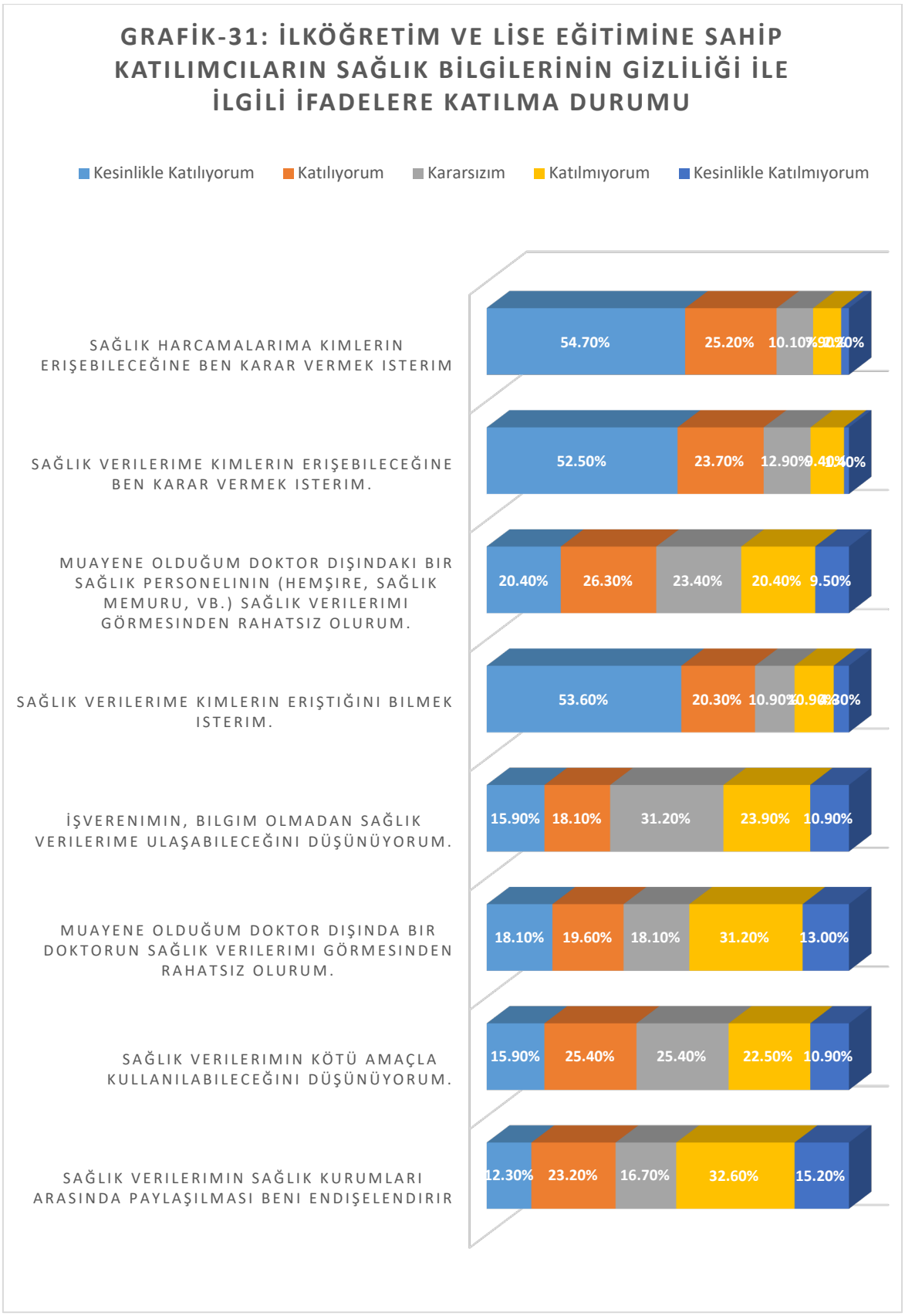
Grafik 28. Lisans ve Lisansüstü Eğitime Sahip Katılımcıların Verilerin Dijital Ortamda Kayıt Altına Alınmasına Yönelik Farkındalığı



Grafik 29. İlköğretim ve Lise Eğitimine Sahip Katılımcıların Verilerin Dijital Ortamda Kayıt Altına Alınmasına Yönelik Farkındalığı

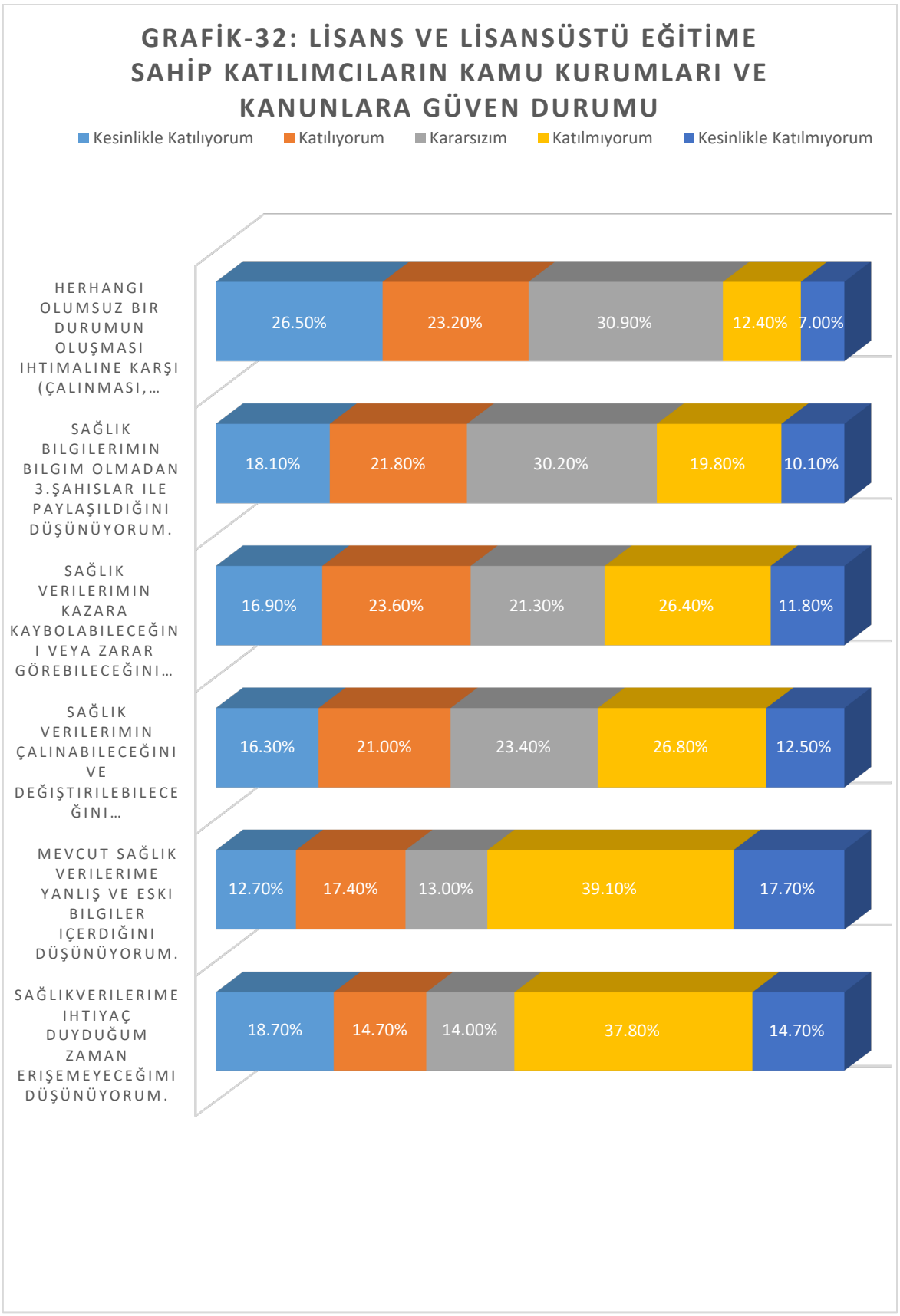
Çalışmaya katılanlar, lisans-lisansüstü ve ilköğretim-lise eğitimine sahip katılımcılar olarak iki farklı gruba ayrılarak, sağlık bilgilerinin gizliliği ile ilgili bir takım ifadelere katılma derecelerini belirleyen sorular sorulmuştur. Lisans ve lisansüstü eğitime sahip katılımcıların %44,9'u kayıt altına alınan sağlık verilerinin sağlık kurumları arasında paylaşılmasından endişe duyacaklarını belirtirken ilköğretim ve lise eğitimine sahip katılımcılarda bu oran %35,6'dır. Lisans ve lisansüstü eğitime sahip katılımcıların %46,2'ı mevcut sağlık verilerinin kötü amaçla kullanılabileceğini düşünmekteyken ilköğretim ve lise eğitimine sahip katılımcılarda bu oran %41,3'dür. Lisans ve lisansüstü eğitime sahip katılımcıların muayene olduğu doktor dışında başka bir doktorun sağlık verilerini görmesinden rahatsız olacağını ifade edenlerin yüzdesi %43,1'dir. Ilköğretim ve lise eğitimine sahip katılımcılarda ise %37,7'dir. . Lisans ve lisansüstü eğitime sahip katılımcılardan iş verenlerinin sağlık verilerine izinsiz bir şekilde ulaşabileceklerini düşünenlerin oranı ise %36,7 iken ilköğretim ve lise eğitimine sahip katılımcılarda bu oran %34'dür. Sağlık verilerini kimlerin erişeceğini bilmek isteyen lisans ve lisansüstü eğitime sahip katılımcıların oranı %90,3 ilköğretim ve lise eğitimine sahip katılımcılarda ise bu oran %70,9'dur. Muayene olduğu doktor dışında herhangi bir sağlık personelinin sağlık verilerini görmesinden rahatsız olacağını belirten . lisans ve lisansüstü eğitime sahip katılımcıların oranı ise %59'dur. Ilköğretim ve lise eğitimine sahip katılımcılardaoran %46,7'dir. Sağlık verilerine kimlerin erişeceğinin yetkilendirmesini yapmak isteyen lisans ve lisansüstü eğitime sahip katılımcıların oranı ise %82 iken ilköğretim ve lise eğitimine sahip katılımcılarda oran %76,2'dir. Sağlık harcamalarına kimlerin erişebileceğini kendisinin karar vermesini isteyen . lisans ve lisansüstü eğitime sahip katılımcıların oranı %83,7 ilköğretim ve lise eğitimine sahip katılımcıların oranı ise %79,9'dur (Grafik-30) (Grafik-31).

Grafik 30. Lisans ve Lisansüstü Eğitime Sahip Katılımcıların Sağlık Bilgilerinin Gizliliği ile İlgili İfadelere Katılma Durumu

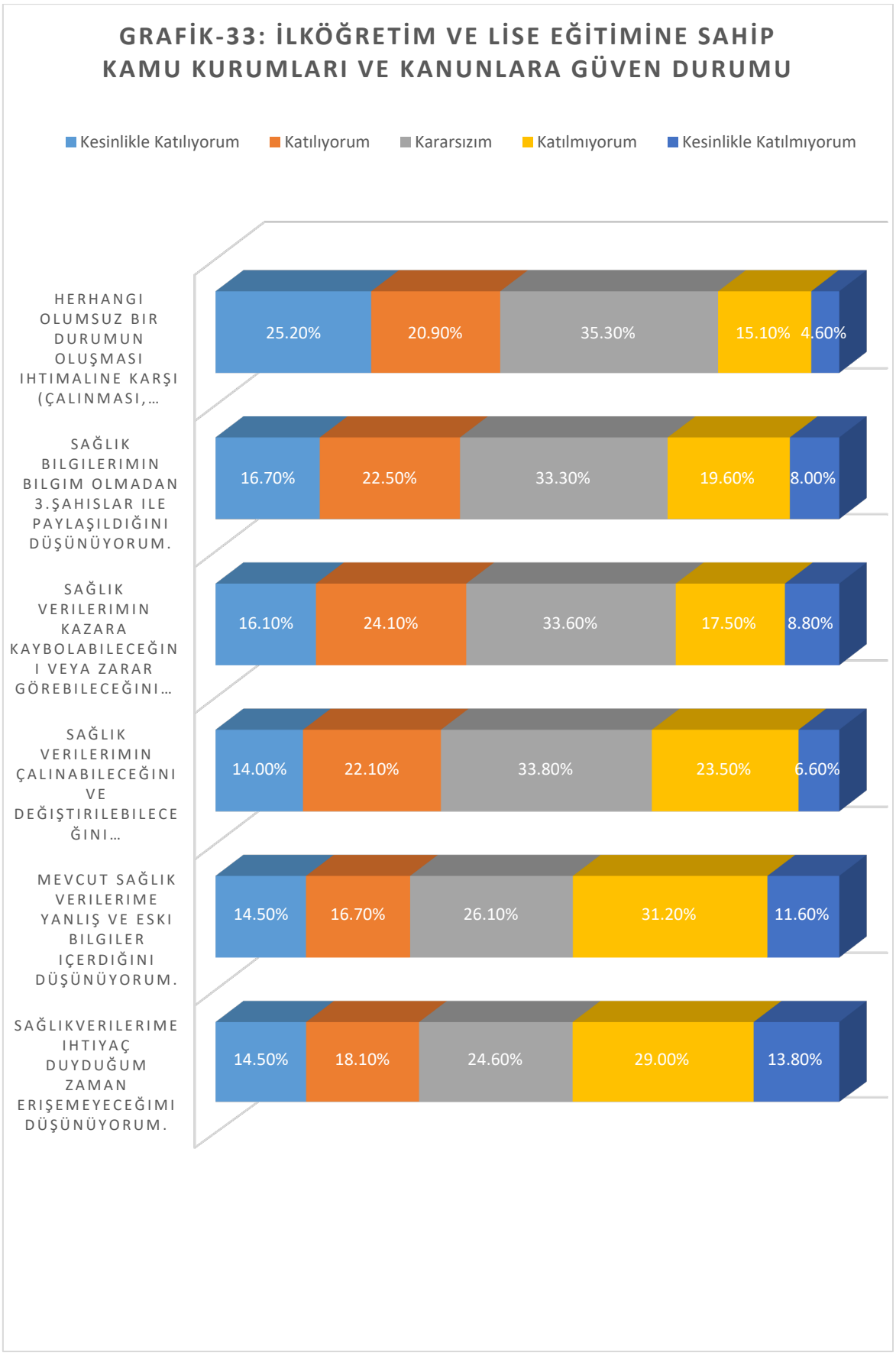


Grafik 31. İlköğretim ve Lise Eğitimine Sahip Katılımcıların Sağlık Bilgilerinin Gizliliği ile İlgili İfadelere Katılma Durumu

Çalışmaya katılanlar, lisans-lisansüstü ve ilköğretim-lise eğitimine sahip katılımcılar olarak iki farklı gruba ayrılarak, sağlık bilgilerinin dijital ortamda saklanmasıyla ilgili verilen ifadelere katılma derecelerini ölçmek amacıyla bazı sorular sorulmuştur. Katılımcıların verdikleri cevaplar neticesinde, sağlık verilerine ihtiyaç duydukları anda erişemeyeceğini düşünen . Lisans ve lisansüstü eğitime sahip katılımcıların oranı %33,4'dür. Ilköğretim ve lise eğitimine sahip katılımcılarda bu oran %32,6'dır. Lisans ve lisansüstü eğitime sahip katılımcıların %30,1'i mevcut sağlık verilerinin yanlış ve eski bilgiler içerdiğini düşünürken ilköğretim ve lise eğitimine sahip katılımcılarda bu oran %31,2'dir. Lisans ve lisansüstü eğitime sahip katılımcıların %37,3'ü sağlık verilerinin çalınabilip, değiştirilebileceğini düşünürken ilköğretim ve lise eğitimine sahip katılımcıların %36,1'i sağlık verilerinin çalınabilip, değiştirilebileceğini düşünmektedir. Sağlık verilerinin kazara kaybolabileceğini düşünen lisans ve lisansüstü eğitime sahip katılımcıların oranı %40,5'dir. Ilköğretim ve lise eğitimine sahip katılımcılarda bu oran %40,2'dir. Sağlık bilgilerinin, bilgileri dahili olmadan üçümcü şahıslar ile paylaşıldığını düşünen lisans ve lisansüstü eğitime sahip katılımcıların oranı %39,9'dur. Ilköğretim ve lise eğitimine sahip katılımcılarda bu oran %39,2'dir. Sağlık verilerinin çalınması, kötüye kullanılması gibi durumlarda kamu kurum, kuruluş ve kanunlarla korunduğunu düşünen . Lisans ve lisansüstü eğitime sahip katılımcıların oranı ise %49,7'dir. Ilköğretim ve lise eğitimine sahip katılımcılarda ise %46,1'i sağlık verilerinin çalınması, kötüye kullanılması gibi durumlarda kamu kurum, kuruluş ve kanunlarla korunduğunu düşünmektedir.(Grafik-32) (Grafik-33).

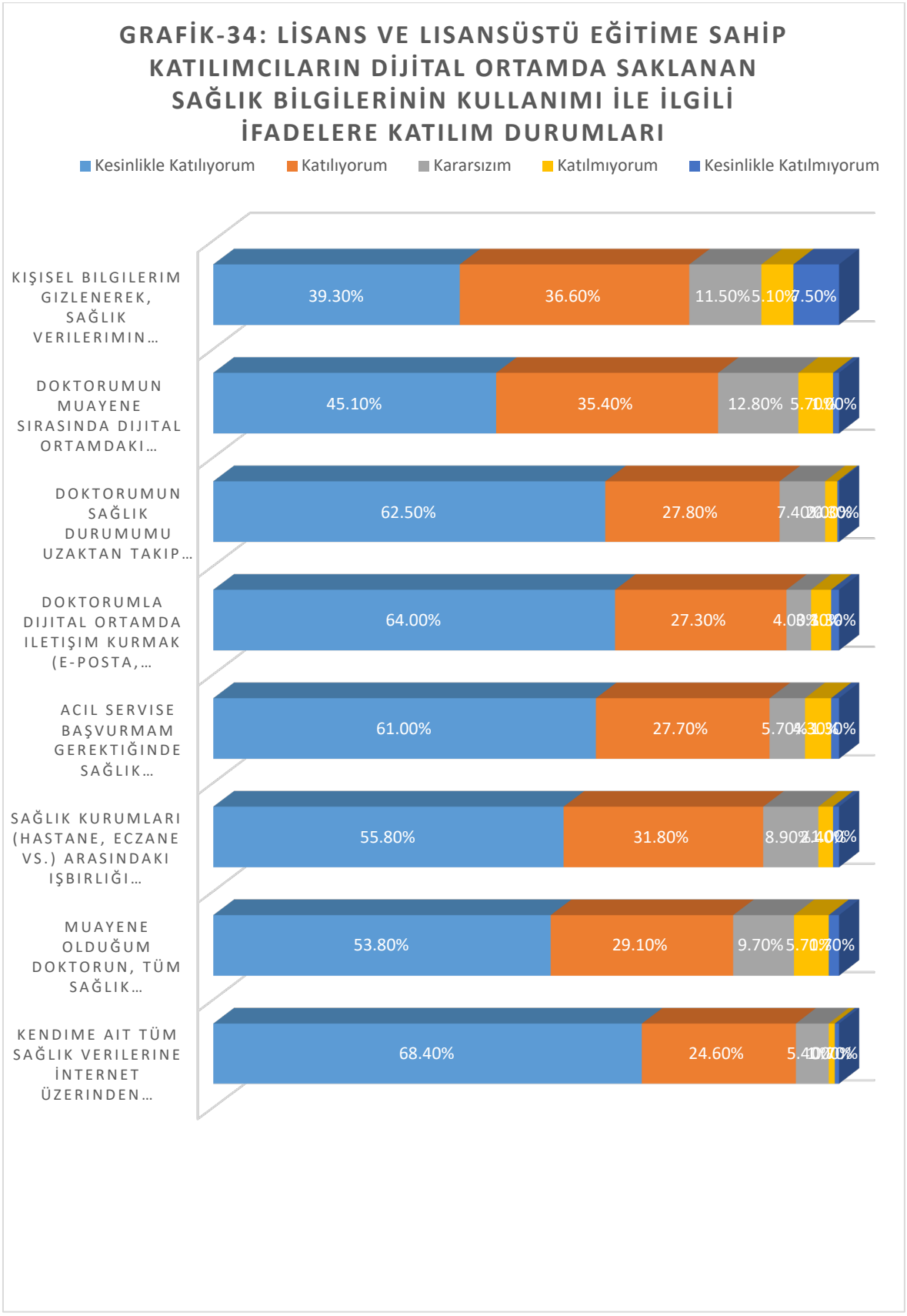


Grafik 32. Lisans ve Lisansüstü Eğitime Sahip Katılımcıların Kamu Kurumları ve Kanunlara Güven Durumu

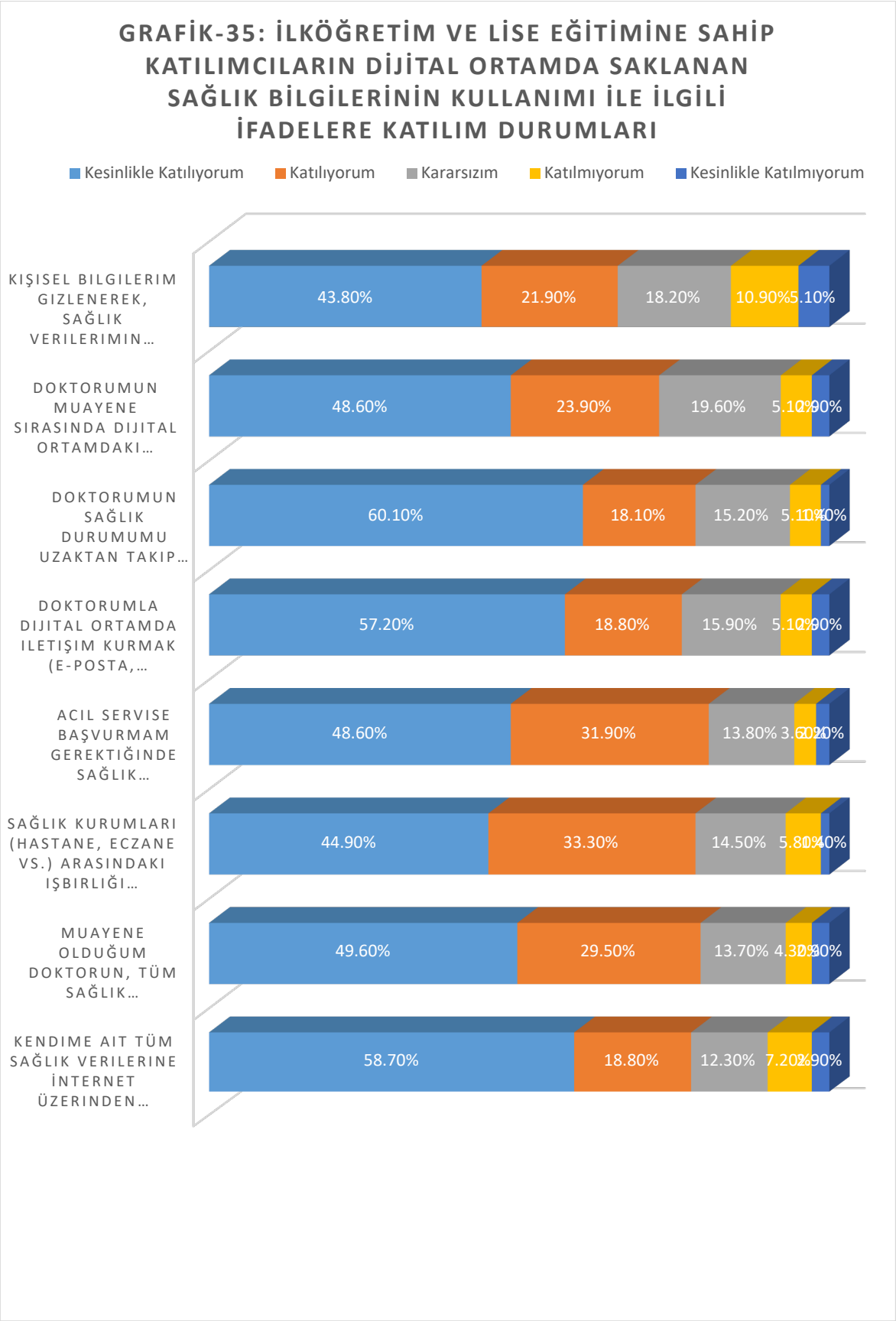


Grafik 33. İlköğretim ve Lise Eğitimine Sahip Katılımcıların Kamu Kurumları ve Kanunlara Güven Durumu

Katılımcılar, lisans-lisansüstü ve ilköğretim-lise eğitimine sahip olarak iki farklı gruba ayrılarak, dijital ortamlarda saklanan sağlık bilgilerinin kullanımı ile ilgili belirtilen ifadelere katılım derecelerini belirlemek için sorular sorulmuştur, Katılımcıların verdikleri yanıtlara göre, Tüm sağlık verilerine internet üzerinden ulaşmak isteyen lisans ve lisansüstü eğitime sahip katılımcıların oranı %93 iken ilköğretim ve lise eğitimine sahip katılımcılarda bu oran %77,5'dir. Lisans ve lisansüstü eğitime sahip katılımcıların %82,9'u muayene oldukları doktorlarının, sağlık geçmişlerine erişebilmelerini istediklerini belirtirken ilköğretim ve lise eğitimine sahip katılımcıların %79,1'i muayene oldukları doktorlarının, sağlık geçmişlerine erişebilmelerini istediklerini belirtmişlerdir. Lisans ve lisansüstü eğitime sahip katılımcıların, %87,6'sı sağlık kurumları (hastane, eczane vs) arasındaki işbirliğinin tedavileri için önemli ve yararlı olduklarını düşünmektedirler. Ilköğretim ve lise eğitimine sahip katılımcılarda bu oran %78,2'dir. Lisans ve lisansüstü eğitime sahip katılımcıların %88,7'si acil servise başvurmaları gerektiğinde başvurdukları acil servislerin sağlık verilerinin tamamına ulaşabilmelerini isterken ilköğretim ve lise eğitimine sahip katılımcılarda bu oran %80,5'dir. Doktoru ile dijital ortamda (e-posta, anında mesajlaşma programları, vb.) iletişim kurmak isteyen . Lisans ve lisansüstü eğitime sahip katılımcıların oranı ise %91,3'dür. İlköğretim ve lise eğitimine sahip katılımcılardabu oran %76'dır. Lisans ve lisansüstü eğitime sahip katılımcıların, %90,3'ü ilköğretim ve lise eğitimine sahip katılımcıların ise %78,2'si doktorlarının, sağlık durumlarını uzaktan takip etmesini istemektedir. Muayene oldukları doktorlarının dijital ortamdaki sağlık verilerinden yararlandığını düşünen . Lisans ve lisansüstü eğitime sahip katılımcıların oranı ise 80,5 İlköğretim ve lise eğitimine sahip katılımcılarda bu oran %72,5'dir. Kişisel sağlık bilgilerinin anonimleştirilerek, bilimsel araştırmalarda kullanılmasından rahatsız olmayacak lisans ve lisansüstü eğitime sahip katılımcıların oranı ise %75,9 iken ilköğretim ve lise eğitimine sahip katılımcılarda bu oran 65,7'dir (Grafik-34) (Grafik-35).

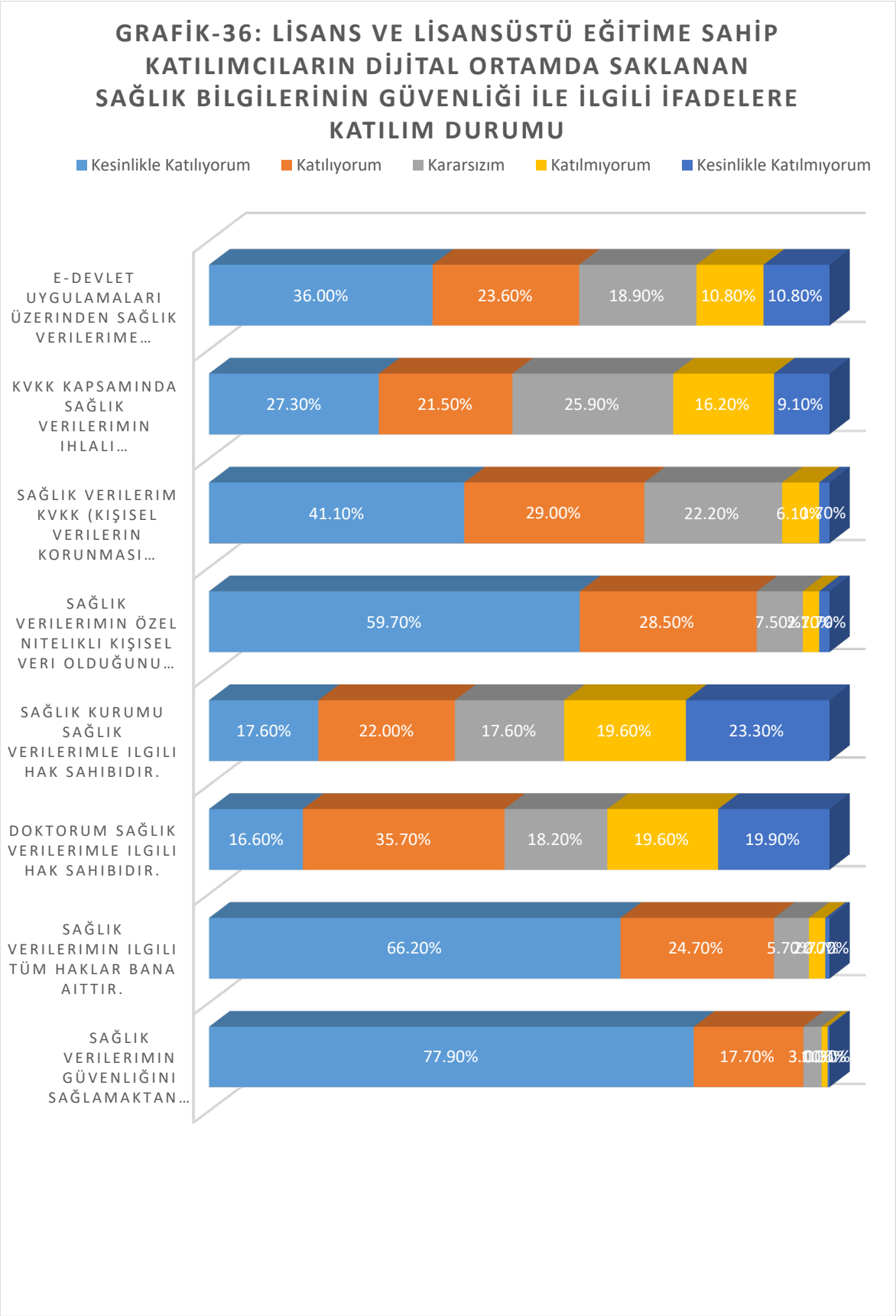


Grafik 34. Lisans ve Lisansüstü Eğitime Sahip Katılımcıların Dijital Ortamda Saklanan Sağlık Bilgilerinin Kullanımı ile İlgili İfadelere Katılım Durumları

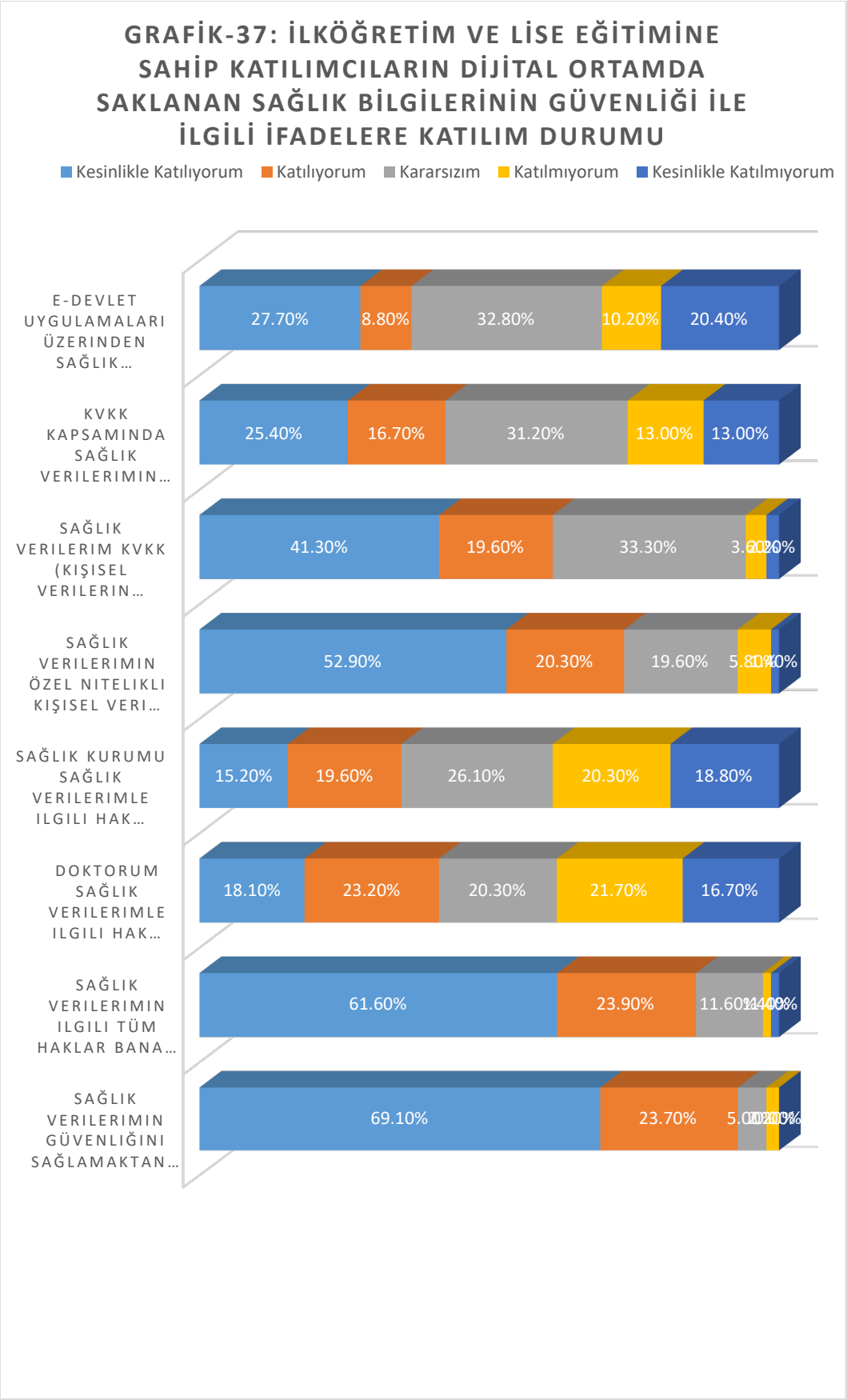


Grafik 35. İlköğretim ve Lise Eğitimine Sahip Katılımcıların Dijital Ortamda Saklanan Sağlık Bilgilerinin Kullanımı ile İlgili İfadelere Katılım Durumları

Çalışmaya katılanlar, lisans-lisansüstü ve ilköğretim-lise eğitimine sahip katılımcılar olarak iki farklı gruba ayrılarak, dijital ortamlarda saklanan sağlık bilgilerinin güvenlik sorumlulukları ile ilgili bazı sorular yöneltilmiştir. Lisans ve lisansüstü eğitime sahip katılımcıların %95,6'sı sağlık verilerinin güvenliğini sağlamaktan devletin sorumlu olması gerektiğini düşünürken ilköğretim ve lise eğitimine sahip katılımcıların %92,8'i sağlık verilerinin güvenliğini sağlamaktan devletin sorumlu olması gerektiğini düşünmektedir. Kişisel sağlık verileri ile ilgili tüm hakların kendisine ait olduğunu düşünen lisans ve lisansüstü eğitime sahip katılımcıların oranı %90,9'dur. Bu oran ilköğretim ve lise eğitimine sahip katılımcılarda %85,5'dir. Doktorlarının, sağlık verileri ilgili hak sahibi olduğunu düşünen . Lisans ve lisansüstü eğitime sahip katılımcıların oranı %52,3 iken ilköğretim ve lise eğitimine sahip katılımcılarda bu oran %41,3'dür. Başvurdukları sağlık kurumlarının sağlık verileri ile ilgili hak sahibi olduğunu düşünen . Lisans ve lisansüstü eğitime sahip katılımcıların oranı %39,6'dır. İlköğretim ve lise eğitimine sahip katılımcılarda bu oran %34,8'dir. Sağlık verilerinin özel nitelikli kişisel veri olduğunun farkında olan lisans ve lisansüstü eğitime sahip katılımcıların oranı %88,2'dir. Bu oran ilköğretim ve lise eğitimine sahip katılımcılarda %73,2'dir. Lisans ve lisansüstü eğitime sahip katılımcıların %70,1'i sağlık verilerinin Kişisel Verilerin Korunması Kanunu (KVKK) kapsamından korunduğunun farkında olduklarını belirtirken bu oran ilköğretim ve lise eğitimine sahip katılımcılarda%60,9'dur. Kişisel Verilerin Korunması Kanunu (KVKK) kapsamında, sağlık verileri ihlale uğradığında ne yapmaları gerektiğini bildiklerini belirten . lisans ve lisansüstü eğitime sahip katılımcıların oranı %48,8 iken ilköğretim ve lise eğitimine sahip katılımcılardabu oran %42,1'dir. E-devlet üzerinden sağlık verilerine kimlerin erişebileceği konusunda yetkilendirme yapabileceğini bilen lisans ve lisansüstü eğitime sahip katılımcıların oranı ise %59,6'dır. Bu oran ilköğretim ve lise eğitimine sahip katılımcılarda%35,7'dir (Grafik-36) (Grafik-37).



Grafik 36. Lisans ve Lisansüstü Eğitime Sahip Katılımcıların Dijital Ortamda Saklanan Sağlık Bilgilerinin Güvenliği ile İlgili İfadelere Katılım Durumu



Grafik 37. İlköğretim ve Lise Eğitimine Sahip Katılımcıların Dijital Ortamda Saklanan Sağlık Bilgilerinin Güvenliği ile İlgili İfadelere Katılım Durumu

7. SONUÇ VE DEĞERLENDİRME

Farklı demografik özelliklere sahip katılımcılar ile gerçekleştirilen dijital sağlık verilerinin güvenliğine yönelik farkındalığı ve beklentilerinin araştırıldığı çalışma sonucunda ortaya çıkan veriler göstermiştir ki katılımcıların büyük çoğunluğu, özlük bilgilerini, iletişim bilgilerini, aile sağlık bilgilerini, kullandığı ilaçları, hastalık tanılarını, laboratuvar sonuçlarını, geçirdikleri operasyonlar gibi kendilerine ait bilgileri kişisel bulduklarını ifade etmişlerdir. Ancak katılımcıların yine büyük bir kısmı aile hekimlerinin isimlerini, sağlık kuruluşlarının ve uzman doktorlarının isimlerini kişisel bulmadıklarını ifade etmişlerdir. Bu durum ortaya çıkarmaktadır ki katılımcılar, doktorlarını ve başvurdukları sağlık kurumlarını kişiye ait özel bir bilgi olarak görmemektedirler. Katılımcıların büyük bir bölümü bu bilgilerinin dijital ortamda kayıt altında olduğunun farkında olduğunu belirtmişlerdir. Bu da dijital ortamlarda kayıt altına alınan kişisel sağlık verilerinin bireyler tarafından farkında olunduğu sonucunu çıkarmaktadır. Katılımcıların azımsanamayacak bir kısmı sağlık verilerinin sağlık kurumları arasında paylaşılmasından, muayene olduğu doktor haricinde bir doktorun veya sağlık çalışanın sağlık verilerini görmesinden, işverenlerinin kendilerinin bilgisi olmadan sağlık verilerine erişebileceği konusunda endişe duyduklarını, belirtirken. Büyük bir kısmı ise sağlık verilerinin kötü amaçla kullanılabileceğini düşünmekte ve sağlık verilerine, sağlık harcamalarına kimlerin erişeceğine kendileri karar vermek istemektedir. Bu sonuçlar göstermiştir ki katılımcılar dijital ortamda kayıt altına alınan sağlık verilerinin güvenliği ve gizliliği konusunda endişelilerdir. Katılımcıların büyük çoğunluğu sağlık verilerinin dijital ortamlarda kayıt altına alındığını bilmelerine rağmen azımsanmayacak bir kısmı sağlık verilerine ihtiyaç duyulduğu takdirde erişemeyeceklerini ve mevcut sağlık verilerinin yanlış ve eksik bilgiler içerdiğini düşünmektedirler. Büyük bir kısmı ise sağlık verilerinin çalınıp, değiştirileceğine, kaybolabileceğine, kendilerinin bilgisi olmadan üçüncü şahıslar ile paylaşılacağına

inanmaktadırlar. Bunun yanı sıra bu olumsuzluklar yaşandığı takdirde katılımcıların %48,6'sı kişisel sağlık verilerinin kamu kurum, kuruluş ve kanunlarla korunduğuna inandıklarını belirtmiş olsalar da kalan kısım kararsız ve kişisel verilerinin kamu kurum ve kuruluşları tarafından korunmadığına inanmadığını belirtmiştir. Bu sonuçlar göstermiştir ki dijital ortamlarda kayıt altına alınan sağlık verilerine güven konusunda endişeyle yaklaşan katılımcıların %48'sı yine de kişisel sağlık verilerinin devlet tarafından kanunlar kapsamında korunduğuna inandıklarını belirtmişlerdir. Dijital ortamlar ile ilgili kaygılı olan bireylere, dijital ortamların güvenliği ve gizlilik ilkeleri hakkında yasal hakları konusunda bilgilendirme yapılarak bu endişelerinin giderilmesi sağlanabilir. Kişisel veri ihlali yaşadıklarında, kamu kurum, kuruluşları ve kanunlar ile korundukları hakkında katılımcılara gerekli bilinçlendirme yapılmalıdır. Dijital sağlık verileri hakkında endişe duysalar da kendilerine ait tüm verilere internet üzerinden kendilerinin ve doktorlarının erişebilmesini istediklerini belirtmişlerdir. Bu sonuca göre katılımcılar, kendilerinin ya da doktorlarının dijital ortamlar sayesinde verilerine ulaştıkları takdirde, zaman kazanacaklarını, tanı ve teşhislerinin erken bir şekilde sonuçlanabileceğinin farkında olduklarını göstermiştir. Katılımcıların büyük bir çoğunluğu sağlık kurumları arasında oluşacak iş birliğinin tedavilerine büyük bir katkı sağlayacağına inandıklarını belirtmiştir. Bu da göstermiştir ki katılımcılar hızlı tedavi ve hızlı tanı için sağlık verilerinin sağlık kurumları arasında paylaşılmasının, büyük bir kolaylık sağlayacağını düşünmektedirler. Yine aynı şekilde acil servise başvurduklarında, başvurulan acil servisin tüm sağlık verilerine ulaşmasının tedavileri için yararlı bulduklarını belirtmişlerdir. Katılımcıların büyük çoğunluğu zaman tasarrufu, ekonomik tasarruf ve hızlı tanı tedavi için ve daha sağlıklı bir yaşam için doktorlarının kendilerini uzaktan takip etmelerinde bir sakınca görmediklerini ve doktorlarıyla dijital ortamlardan iletişim kurmak istediklerini belirtmişlerdir. Doktorlarının muayeneleri sırasında dijital sağlık verilerinden yararlandığını düşünen katılımcı oranı bir

hayli yüksektir. Bu da katılımcıların, kayıt altına alınan sağlık verilerinden, hekimlerin yararlandığının farkında olduğunun göstergesidir. Katılımcılar, kimlikleri gizlenip, verileri anonimleştirildiği takdirde, sağlık verilerinin bilimsel araştırmalar için kullanılmasından rahatsız olmayacağını belirtmişlerdir. Bu sonuç veri anonimleştirmenin bilimsel çalışmalar için önemini bir kere daha göstermektedir. Anonimleştirildiği takdirde kişisel veriler, sahipleri için herhangi bir mahrumiyet ve hayatlarını olumsuz yönde etkileyecek bir sonuç ortaya çıkarmayacaktır. Her ne kadar dijital ortamlarda verilerin kayıt edilmesi hakkında tam güven oluşmasa da katılımcılar dijital sağlık verilerinin her anlamda hayatlarını kolaylaştıracaklarını düşünmektedirler. Dijital sağlık verilerinin ihlal edildiği takdirde kamu kurum, kuruluşları ve kanunlar tarafından korunduğuna inanan katılımcılar. Büyük bir çoğunluk ile kişisel sağlık verilerinin devlet tarafından korunması gerektiğine inandıklarını ve sağlık verileri ile ilgili tüm hakların kendilerine ait olduğunu düşündüklerini belirtmişlerdir. Bu da katılımcıların sağlık verilerinin öneminin farkında olduklarını ve devletin bu verilerden sorumlu olmasının farkında olduklarını göstermiştir. Sağlık verilerinin özel nitelikli kişisel veri olduğunu bildiklerini belirten katılımcılar, sağlık kurumları ve doktorlarının kendi sağlık verileri ile ilgili hak sahibi olmadıklarını belirtmişlerdir. Bu durum katılımcıların kendilerine ait bilgilerin korunması konusunda devleti sorumlu görseler de kendi bilgileri hakkında devlet kurumu olan sağlık kuruluşlarının herhangi bir haklarının olmadığını düşünmektedirler. Bu sonuçta katılımcıların sağlık verilerinin özel nitelikli kişisel veri olduğunun farkında olduklarının bir kanıtıdır. Devlet tarafından sağlık verilerinin korunması gerektiğini düşünen katılımcılar, sağlık verilerinin KVKK tarafından korunduğunu bildiklerini belirtmişlerdir. Ancak büyük bir çoğunluk sağlık veri ihlali yaşadıklarında KVKK kapsamında ne yapacağını bildikleri konusunda kararsız ve bilmediklerini dile getirmişlerdir. Araştırma sonucunda elde edilen bulgular değerlendirildiğinde genel olarak sağlık sektöründe çalışan bireylerin kişisel sağlık verileri

ile ilgili farkındalıklarının yüksek olduğu, diğer katılımcılarda ise eğitim seviyesinin yükselmesi ile birlikte farkındalığın arttığı saptanmıştır.

Bu sonuçlara göre genel olarak sağlık verilerinin kamu kurum, kuruluş ve kanunlar ile korunduğunu bilen, sağlık verilerinin KVKK kapsamından korunduğunu bilen bireylerin, sağlık ihlalleri karşısında KVKK kapsamında yasal olarak neler yapabilecekleri konusunda bilinçlendirilmesi gerekmektedir. Bu bilinçlendirme neticesinde kamu kurum, kuruluş ve kanunlara güvenin daha da artacağı ve dijital ortamlarla ile ilgili gizlilik ve güvenlik endişelerinin giderileceği görülmektedir. Dijital sağlık verilerinin kullanılması konusunda endişesi bulunmayan ve kullanılmasını destekleyen katılımcılara, kişisel hakları ve kanunlar kapsamında neler yapabilecekleri konusunda yeterli bilinçlendirme yapıldığı takdirde kişisel sağlık verilerinin, tedavi, erken tanı gibi sağlık ihtiyaçlarını büyük oranda kolaylaştıracağına inandığı görülen katılımcıların. Sağlık kuruluşlarını ve hekimlerini benimseyerek güven ilişkinin artacağı görülmüştür. Ortaya çıkan sonuçlar bütün olarak incelendiğinde katılımcıların büyük bölümünün kişisel verileri ile ilgili bilgili oldukları ortaya çıkmaktadır. Bu bilinçlenmenin artması olası kişisel verilere yönelik saldırıların ve kişisel verilerin kötüye kullanılmasının büyük bir ölçüde önüne geçecektir. Katılımcılar, dijital ortamlara ve hasta-sağlık kuruluşu ilişkisi içerisine dahil olacak herhangi bir üçüncü şahısa güvenmediklerini dile getirmişlerdir. Günümüzde verilerin artık teknolojiyle entegre olup, dijitalleştirilmeden saklanmasının imkanı olmadığı aşikardır. Dolayısıyla kişisel sağlık verileri ile ilgili bilinç düzeyi yüksek olan ve yapılan çalışmalar neticesinde her geçen gün bilinç düzeyi artan topluma, dijital ortamlara güven duymaları ve bu endişelerinden kurtulmaları için bilinçlendirme yapılması gerekmektedir. Katılımcıların veri ihlali konusunda hangi kurum ve kuruluşlara başvuracakları konusunda bilinçlendirilip, yasal hakları konusunda bilgilendirilmeye ihtiyaçları olduğu açık bir şekilde görülmektedir.

KAYNAKÇA

Ahmadi, H., Nilashi, M. ve Ibrahim, O (2015). Organizational decision to adopt hospital information system: An empirical investigation in the case of Malaysian public hospitals. *International journal of medical informatics, 84* (3), 166-188.

Ak, B (2009). Türkiye'de sağlık bilişimi, bir kişisel değerlendirme ve uluslararası bir başarı öyküsü: CorTTex. *Akademik Bilişim'09-XI. Akademik Bilişim Konferansı Bildirileri,* 11-13.

America, H. N (2018). HIMSS cybersecurity survey. *Retrieved from*.

Archer, N., Fevrier-Thomas, U., Lokker, C., McKibbon, K. A., & Straus, S. E (2011).

ARSLAN, E. T., & DEMİR, H (2017). Sağlik çalişanlarinin hasta mahremiyetine ilişkin tutumu: nitel bir araştirma. *Bolu Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *17* (4), 191-220.

Personal health records: a scoping review. *Journal of the American Medical Informatics Association*, *18* (4), 515-522.

Ayala, L (2016). Cyber-Physical Attack Recovery Procedures: A Step-by-Step Preparation and Response Guide. Apress.

Başalp, N (2015). Avrupa birliği veri koruması genel regülasyonu'nun temel yenilikleri.

Bayardo, R. J., & Agrawal, R (2005,April). Data privacy through optimal k-anonymization. In 21st International conference on data engineering (ICDE'05) (pp. 217-228). IEEE.

Bloomberg, J (2018). Digitization, digitalization, and digital transformation: confuse them at your peril. *Forbes. Retrieved on August*, *28,*2019.

Boneh, D., & Shaw, J (1998). Collusion-secure fingerprinting for digital data. *IEEE Transactions on Information Theory*, *44* (5), 1897-1905.

Calvaresi, D., Schumacher, M., & Calbimonte, J. P (2020,October). Personal Data Privacy Semantics in Multi-Agent Systems Interactions. In *International Conference on Practical Applications of Agents and Multi-Agent Systems* (pp. 55-67). Springer, Cham.

Chik, W. B (2013). The Singapore Personal Data Protection Act and an assessment of future trends in data privacy reform. *Computer Law & Security Review*, *29* (5), 554-575.

Çobanoğlu, N (2010). Tıp Etiği Açısından Tıbbi Bilgilerin Mahremiyeti. *Ankara Barosu Iıı. Sağlık Hukuku Kurultayı*, 7-8.

Dülger, M. V (2015). Sağlık hukukunda kişisel verilerin korunması ve hasta mahremiyeti. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, *1* (2), 43-80.

Elif Küzeci, Kişisel Verilerin Korunması, 3.Baskı,, Seçkin Yayıncılık, Ankara, 2019

Entzeridou, E., Markopoulou, E., & Mollaki, V (2018). Public and physician's expectations and ethical concerns about electronic health record: Benefits outweigh risks except for information security. *International Journal of Medical Informatics*, *110,*98-107.

Eysenbach, G (2001). What is e-health?. *Journal of medical Internet research*, *3* (2), e20.

Gantz, J., & Reinsel, D (2012). The digital universe in 2020: Big data, bigger digital shadows, and biggest growth in the far east. *IDC iView: IDC Analyze the future*, *2007* (2012), 1-16.

Greenstein, S., Lerner, J., & Stern, S (2013). Digitization, innovation, and copyright: What is the agenda?. *Strategic Organization*, *11* (1), 110-121.

Gursel, G., Gul, H. Ve Kuru, K (2016). Sağlık bilgi sistemlerinin zayıf yönlerinin belirlenmesi: Bir deneysel e-sağlık değerlendirme çalışması. *Academic Journal of Information Technology, 7* (23), 17-29.

Häikiö, J., Yli-Kauhaluoma, S., Pikkarainen, M., Iivari, M., & Koivumäki, T (2020). Expectations to data: Perspectives of service providers and users of future health and wellness services. *Health and Technology*, 1-16.

Hakan Hakeri, Tıp Hukuku, 4.Bası, Seçkin Yayıncılık, Ankara, 2012

Hathaway, O. A., Crootof, R., Levitz, P. ve Nix, H (2012). The law of cyber-attack. Calif. L. Rev., 100,817.

Jang-Jaccard, J. ve Nepal, S (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80 (*5), 973-993.

Karaarslan, E., Ergin, A. M., Turğut, N. ve Kılıç, Ö (2015). Elektronik sağlık kayıtlarının gizlilik ve mahremiyeti. *XX. Türkiye'de İnternet Konferansı*, 1-3.

Knight, A (2017). Towards A New Approach To The Legal Definition Of Personal Data And A Jurisdictional Model Of Data Protection Law: Surpassing The Requirement For An Assessment Of Identifiability From Data With An Effects-Based Approach (Doctoral dissertation, University of Southampton).

Kruse, C. S., Frederick, B., Jacobson, T. ve Monticone, D. K (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care, 25* (1), 1-10.

Lasko, T. A., & Vinterbo, S. A (2009). Spectral anonymization of data. *IEEE transactions on knowledge and data engineering*, *22* (3), 437-446.

Maurya, R. N (2012). Digital library and digitization. *International Journal of Information Dissemination and Technology*, *1* (4), 228-231.

Nilgün Başalp, Kişisel Verilerin Korunması ve Saklanması, 1.Baskı, Seçkin Yayıncılık, Ankara, 2004

O'Leary, D. E., Bonorris, S., Klosgen, W., Khaw, Y. T., Lee, H. Y., & Ziarko, W (1995).

Some privacy issues in knowledge discovery: the OECD personal privacy guidelines. *IEEE Expert*, *10* (2), 48-59.

Öğütçü, G., Köybaşı, N. A. G., & Cula, S (2011). Elektronik Sağlık Kayıtlarının İçeriği, Hassasiyeti ve Erişim Kontrollerine Yönelik Farkındalık ve Beklentilerin Değerlendirilmesi. *Tıp Bilişim Derneği*, 88-97.

Özkan, Ö (2011). Attitudes and opinions of people who use medical services about privacy and confidentiality of health information in electronic environment. *Medical Informatics*.

Ritter, T., & Pedersen, C. L (2020). Digitization capability and the digitalization of business models in business-to-business firms: Past, present, and future. *Industrial Marketing Management*, *86,*180-190.

Safran, C., Bloomrosen, M., Hammond, W. E., Labkoff, S., Markel-Fox, S., Tang, P. C., & Detmer, D. E (2007). Toward a national framework for the secondary use of health data: an American Medical Informatics Association White Paper. *Journal of the American Medical Informatics Association*, *14* (1), 1-9.

Schwartz, P. M (2003). Property, privacy, and personal data. *Harv. L. Rev., 117,*2056.

Schwartz, P. M., & Solove, D. J (2014). Reconciling personal information in the United States and European Union. *Calif. L. Rev., 102,*877.

Selwyn, N (2015). Data entry: towards the critical study of digital data and education. *Learning, Media and Technology*, *40* (1), 64-82.

Spencer, K., Sanders, C., Whitley, E. A., Lund, D., Kaye, J., & Dixon, W. G (2016). Patient perspectives on sharing anonymized personal health data using a digital system for dynamic consent and research feedback: a qualitative study. *Journal of medical Internet research*, *18* (4), e66.

T.C. Sağlık Bakanlığı (2018). *Bilgi Güvenliği Politikaları Kılavuzu.* https://bilgiguvenligi. saglik. gov. tr/Home/Mevzuat (26.12.2020 tarihinde erişildi).

Walters, R (2014). Cyber attacks on US companies in 2014.The Heritage Foundation, 4289,

1-5.

https://dosyaism. saglik. gov. tr/Eklenti/50016,erisimkontrolpolitikasipdf. pdf?0 (26.12.2020 tarihinde erişildi).

https://sys. sagliknet. saglik. gov. tr/dokumanonline/ 26.12.2020 tarihinde erişildi).

Walters, R (2014). Cyber attacks on US companies in 2014.The Heritage Foundation, 4289,1-5.

KişiselSağlıkVerileriHakıındaYönetmelik https://www. resmigazete. gov. tr/eskiler/2019/06/201906213.htm (26.12.2020 tarihinde erişildi).

Yaldır, A. ve Taşer, M (2016). Hastane bilgi yönetim sistemleri için olap yöntemleri ile karar destek modülü tasarımı ve uygulaması. *Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 18* (1), 153-171.

Yılmaz, E., Ulus, H. ve Gönen, S (2015). Bilgi toplumuna geçiş ve siber güvenlik. *Bilişim Teknolojileri Dergisi, 8* (3), 133.

EKLER

EK1: ANKET FORMU

DİJİTAL SAĞLIK VERİLERİ FARKINDALIK VE BEKLENTİ ANKETİ

Bu anket çalışması, Başkent Üniversitesi Sosyal Bilimler Enstitüsü Yönetim Bilişim Sistemleri Tezli Yüksek Lisans Programı alanında yüksek lisans eğitimini sürdürmekte olan bir araştırmacı tarafından yürütülmektedir. Anketi cevaplama süresi ortalama 10 dakikadır. Anket cevapları herhangi bir kişisel bilgi ile ilişkilendirilmeyecek ve üçüncü şahıslarla paylaşılmayacaktır. İstatistiksel sonuçlar, kamu yararına olmak üzere yayınlanacak, Bilgi Toplumu ve E-Sağlık Projeleri yapılandırmasına ışık tutması amacıyla kullanılacaktır. Anket sonuçlarını talep eden cevaplayıcıların denizhanyilmaz@yandex. com adresine "ANKET" konulu boş bir e-posta göndermeleri yeterlidir.

Demografik Bilgiler

Yaşınız:

Yaşadığınız şehir:

Eğitim Düzeyiniz:

1.Okur Yazar

2.İlkokul

3.Ortaokul

4.Lise

5.Üniversite

6.YÜksek Lisans ve Üstü

Güncel sağlık durumunuz:

1.Bilinen herhangi bir rahatsızlığım yoktur.

2.Rahatsızlığım var

Son 1 yıl içinde yaklaşık olarak kaç kez sağlık kurumuna/doktora başvurdunuz:

1.Hiç

2.1-3

3.4-6

4.6 ve üstü

Sosyal güvenceniz (Birden fazla seçeneği işaretleyebilirsiniz):

1.SGK (SSK, Emekli Sandığı, Bağkur)

2.Özel Sağlık Sigortası

3.Kurum Sigortası

4.60/c1-c3-c9

5.Yok

6.Diğer:

Sürekli/düzenli ilaç kullanıyor musunuz?

1.Evet

2.Hayır

Aşağıda verilen bilgileri ne derece kişisel bulduğunuzu işaretleyiniz.

İletişim bilgilerim (Adres, telefon, vb.)

1.Kesinlikle kişisel buluyorum

2.Kişisel buluyorum

3.Kararsızım

4.Kişisel bulmuyorum

5.Kesinlikle kişisel bulmuyorum

Özlük bilgilerim (TC kimlik no, doğum tarihi, vb.)

1.Kesinlikle kişisel buluyorum

2.Kişisel buluyorum

3.Kararsızım

4.Kişisel bulmuyorum

5.Kesinlikle kişisel bulmuyorum

Aile sağlık bilgilerim (Kalıtsal hastalıklar, genetik bilgiler, vb.)

1.Kesinlikle kişisel buluyorum

2.Kişisel buluyorum

3.Kararsızım

4.Kişisel bulmuyorum

5.Kesinlikle kişisel bulmuyorum

Muayene sonuçlarım (şikayetler, doktor bulguları, vb.)

1.Kesinlikle kişisel buluyorum

2.Kişisel buluyorum

3.Kararsızım

4.Kişisel bulmuyorum

5.Kesinlikle kişisel bulmuyorum

Laboratuar sonuçlarım (kan/idrar tahlilleri, röntgen, MR sonuçları, vb.)

1.Kesinlikle kişisel buluyorum

2.Kişisel buluyorum

3.Kararsızım

4.Kişisel bulmuyorum

5.Kesinlikle kişisel bulmuyorum

Kullandığım ilaçlar

1.Kesinlikle kişisel buluyorum

2.Kişisel buluyorum

3.Kararsızım

4.Kişisel bulmuyorum

5.Kesinlikle kişisel bulmuyorum

Geçirdiğim operasyonlar

1.Kesinlikle kişisel buluyorum

2.Kişisel buluyorum

3.Kararsızım

4.Kişisel bulmuyorum

5.Kesinlikle kişisel bulmuyorum

Hastalık tanısı

1.Kesinlikle kişisel buluyorum

2.Kişisel buluyorum

3.Kararsızım

4.Kişisel bulmuyorum

5.Kesinlikle kişisel bulmuyorum

Uzman doktorumun adı

1.Kesinlikle kişisel buluyorum

2.Kişisel buluyorum

3.Kararsızım

4.Kişisel bulmuyorum

5.Kesinlikle kişisel bulmuyorum

Aile hekimimin adı

1.Kesinlikle kişisel buluyorum

2.Kişisel buluyorum

3.Kararsızım

4.Kişisel bulmuyorum

5.Kesinlikle kişisel bulmuyorum

Sağlık kurumunun adı (Hastane, Eczane, vb.)

1.Kesinlikle kişisel buluyorum

2.Kişisel buluyorum

3.Kararsızım

4.Kişisel bulmuyorum

5.Kesinlikle kişisel bulmuyorum

Sağlık bilgi sistemleri/ e-devlet uygulamaları kapsamında aşağıdaki bilgilerin dijital ortamda kayıt altına alındığını biliyorum.

İletişim bilgilerim (Adres, telefon, vb.)

1.Evet

2.Hayır.

3.Fikrim Yok

Özlük bilgilerim (TC kimlik no, doğum tarihi, vb.)

1.Evet

2.Hayır.

3.Fikrim Yok

Aile sağlık bilgilerim (Kalıtsal hastalıklar, genetik bilgiler, vb.)

1.Evet

2.Hayır.

3.Fikrim Yok

Muayene sonuçlarım (şikayetler, doktor bulguları, vb.)

1.Evet

2.Hayır.

3.Fikrim Yok

Laboratuvar sonuçlarım (kan/idrar tahlilleri, röntgen, MR sonuçları, vb.)

1.Evet

2.Hayır.

3.Fikrim Yok

Kullandığım ilaçlar

1.Evet

2.Hayır.

3.Fikrim Yok

Geçirdiğim operasyonlar

1.Evet

2.Hayır.

3.Fikrim Yok

Hastalık tanılarım

1.Evet

2.Hayır.

3.Fikrim Yok

Uzman doktorumun adı

1.Evet

2.Hayır.

3.Fikrim Yok

Aile hekimimin adı

1.Evet

2.Hayır.

3.Fikrim Yok

Sağlık kurumunun adı

1.Evet

2.Hayır.

3.Fikrim Yok

Sağlık bilgilerinizin gizliliği ile ilgili aşağıdaki ifadelere katılma derecenizi işaretleyiniz.

Sağlık verilerimin sağlık kurumları arasında paylaşılması beni endişelendirir.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Sağlık verilerimin kötü amaçla kullanılabileceğini düşünüyorum.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Muayene olduğum doktor dışında bir doktorun sağlık verilerimi görmesinden rahatsız olurum

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

İşverenimin, bilgim olmadan sağlık verilerime ulaşabileceğini düşünüyorum.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Sağlık verilerime kimlerin eriştiğini bilmek isterim.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Muayene olduğum doktor dışındaki bir sağlık personelinin (hemşire, sağlık memuru, vb.) sağlık verilerimi görmesinden rahatsız olurum.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Sağlık verilerime kimlerin erişebileceğine ben karar vermek isterim.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Sağlık harcamalarıma kimlerin erişebileceğine ben karar vermek isterim

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Sağlık bilgilerinin dijital ortamda saklanmasıyla ilgili aşağıdaki ifadelere katılma derecenizi işaretleyiniz.

Sağlık verilerime ihtiyaç duyduğum zaman erişemeyeceğimi düşünüyorum.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Mevcut sağlık verilerime yanlış ve eski bilgiler içerdiğini düşünüyorum.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Sağlık verilerimin çalınabileceğini ve değiştirilebileceğini düşünüyorum.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Sağlık verilerimin kazara kaybolabileceğini veya zarar görebileceğini düşünüyorum.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Sağlık bilgilerimin bilgim olmadan 3.şahıslar ile paylaşıldığını düşünüyorum.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Herhangi olumsuz bir durumun oluşması ihtimaline karşı (çalınması, kötüye kullanılması, vb.) sağlık verilerimin kurum, kuruluş ve kanunlarla korunduğuna inanıyorum.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Dijital ortamda saklanan sağlık bilgilerinizin kullanımı ilgili aşağıdaki ifadelere katılma derecenizi işaretleyiniz.

Kendime ait tüm sağlık verilerine İnternet üzerinden erişebilmek isterim.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Kendime ait tüm sağlık verilerine İnternet üzerinden erişebilmek isterim.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Kendime ait tüm sağlık verilerine İnternet üzerinden erişebilmek isterim.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Muayene olduğum doktorun, tüm sağlık geçmişime erişebilmesini isterim.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Sağlık kurumları (hastane, eczane vs.) arasındaki işbirliği tedavim için önemli ve yararlı olabilir.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Acil servise başvurmam gerektiğinde sağlık verilerimin tamamına ulaşılabilmesini isterim.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Doktorumla dijital ortamda iletişim kurmak (e-posta, anında mesajlaşma programları, vb.) isterim.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Doktorumun sağlık durumumu uzaktan takip edebilmesini isterim.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Doktorumun muayene sırasında dijital ortamdaki sağlık verilerimden yararlandığını düşünüyorum.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Kişisel bilgilerim gizlenerek, sağlık verilerimin bilimsel araştırmalarda kullanılması beni rahatsız etmez.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Dijital ortamda saklanan sağlık bilgilerinizin güvenlik sorumluluğu ile ilgili aşağıdaki ifadelere katılma derecenizi işaretleyiniz.

Sağlık verilerimin güvenliğini sağlamaktan devletin sorumlu olması gerektiğini düşünüyorum.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Sağlık verilerimin ilgili tüm haklar bana aittir.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Doktorum sağlık verilerimle ilgili hak sahibidir.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Sağlık kurumu sağlık verilerimle ilgili hak sahibidir.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Sağlık verilerimin özel nitelikli kişisel veri olduğunu biliyorum.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

Sağlık verilerim KVKK (Kişisel Verilerin Korunması Kanunu) kapsamında korunduğunu biliyorum.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum

E-devlet uygulamaları üzerinden sağlık verilerime kimlerin erişebileceği ile ilgili yetkilendirmeyi kendimin yapabileceğini biliyorum.

1.Kesinlikle katılıyorum

2.Katılıyorum

3.Kararsızım

4.Katılmıyorum

5.Kesinlikle katılmıyorum