Journal of
ORIGINAL STUDIES

Journal of Original Studies
Volume / Cilt: 5, Issue / Sayı: 2, 2024, pp. 73-84
E-ISSN: 2717-719X
https://journals.gen.tr/jos
DOI: https://doi.org/10.47243/jos.2612

Received / Geliş: 25/11/2024
Acccepted / Kabul: 21/12/2024

ARAŞTIRMA MAKALESİ/RESEARCH ARTICLE

Kişisel sağlık verisi ihlallerinin analizi: BWM yaklaşımı ile önceliklendirme

Analysis of personal health data breaches: Prioritization with BWM approach

Emre Yılmaz

Dr. Öğr. Üyesi, İstanbul Medipol Üniversitesi Sağlık Bilimleri Fakültesi Sağlık Yönetimi Bölümü, Türkiye,
e-mail: emreyilmaz@medipol.edu.tr

Öz

Bu çalışmanın amacı kişisel sağlık verisi ihlallerine neden olan faktörleri belirlemek, bu faktörleri BWM (Best Worst Method) yaklaşımı ile önceliklendirmek ve elde edilen öncelikler doğrultusunda sağlık verisi güvenliğini artırmaya yönelik çözüm önerileri sunmaktır. Kişisel sağlık verisi ihlallerinin değerlendirilmesi için literatür taraması sonucunda veri sızıntısı, insan hataları, kötü amaçlı yazılımlar, güvenlik düzeyi (şifreleme), siber saldırılar, yetkisiz erişim, ayrıcalık suistimali ve uygunsuz veri imha politikaları olmak üzere 8 kriter belirlenmiştir. Belirlenen kriterler çok kriterli karar verme yaklaşımı olan BWM yöntemi ile analiz edilmiştir. Değerlendirme, sağlık yönetimi ve sağlık hukuku alanlarında en az 7 yıllık akademik veya profesyonel deneyime sahip 6 farklı uzman tarafından yapılmıştır. Analiz bulgularına göre; kişisel sağlık verisi ihlallerine neden olan en önemli (en iyi) kriter %16,95 ağırlık puanı ile "Siber Saldırılar"'olarak tespit edilmiştir. Daha sonra sırasıyla "Veri Sızıntısı" (%16,77), "Ayrıcalık Suistimali" (%15,10) ve "Kötü Amaçlı Yazılımlar" (%15,07) gelmektedir. "Uygunsuz Veri İmha Politikaları" ise %5,01 ağırlık ile en az önemli (en kötü) kriter olarak tespit edilmiştir. Sonuç olarak, sağlık verilerinin ihlalinin engellenebilmesi ve etkili bir veri güvenliği yönetimi için çok yönlü stratejiler geliştirilmesi gerekmektedir. Siber saldırılara karşı, gelişmiş güvenlik önlemleri, düzenli güvenlik denetimleri ve ağ segmentasyonu gibi yöntemler önerilmektedir. Hasta kimliği; anonimleştirme, veri setlerinin kümelenmesi veya gerçek hasta kimliği yerine bulanıklaştırma tekniği gibi birtakım yöntemler kullanılarak mahremiyetin korunabilmesi sağlanabilir. Ayrıcalık suistimalinin etkilerini azaltmak ise rol tabanlı erişim kontrolü, kullanıcı faaliyetlerinin izlenmesi ve düzenli erişim denetimleri gibi yöntemler uygulanmalıdır.

Anahtar kelimeler: Kişisel Veri, Sağlık, Çok Kriterli Karar Verme, Önceliklendirme, BWM

Citation/Atıf: YILMAZ, E. (2024). Kişisel sağlık verisi ihlallerinin analizi: BWM yaklaşımı ile önceliklendirme. *Journal of Original Studies.* 5(2), 73-84, DOI: 10.47243/jos.2612

Corresponding Author/ Sorumlu Yazar:
Emre Yılmaz
E-mail: emreyilmaz@medipol.edu.tr

Abstract

The aim of this study is to identify the factors that cause personal health data breaches, prioritize these factors with the BWM (Best Worst Method) approach, and propose solutions to improve health data security in line with the priorities obtained. As a result of the literature review, 8 criteria were identified for the evaluation of personal health data breaches: data leakage, human errors, malware, security level (encryption), cyber-attacks, unauthorized access, privilege abuse and inappropriate data destruction policies. The criteria were analyzed using the BWM method, a multi-criteria decision-making approach. The evaluation was conducted by 6 different experts with at least 7 years of academic or professional experience in the fields of health management and health law. According to the findings of the analysis; the most important (best) criterion causing personal health data breaches was determined as "Cyber Attacks" with a weight score of 16.95%. This is followed by "Data Leaks" (16.77%), "Privilege Abuse" (15.10%) and "Malicious Software" (15.07%). "Inappropriate Data Destruction Policies" was identified as the least important (worst) criterion with a weight of 5.01%. As a result, multifaceted strategies need to be developed for preventing health data breaches and effective data security management. Methods such as advanced security measures, regular security audits and network segmentation are recommended against cyber-attacks. Patient identity; privacy can be protected by using a number of methods such as anonymization, clustering of data sets or blurring technique instead of real patient identity. To mitigate the effects of privilege abuse, methods such as role-based access control, monitoring of user activities and regular access audits should be implemented.

Keywords: Personal Data, Health, Multi-Criteria Decision Making, Prioritization, BWM

1. GİRİŞ

Kişisel veri, bireyin şahsi, mesleki ve ailevi özelliklerini gösteren, o bireyi diğer bireylerden ayırmaya ve niteliklerini ortaya koymaya elverişli her türlü bilgidir. 6698 sayılı Kişisel Verilerin Korunması Kanunu'nda (KVKK) kişisel veri; *"kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* şeklinde tanımlanmıştır. Anayasa Mahkemesi de aynı doğrultuda kişisel veriyi, "belirli veya kimliği belirlenebilir olmak şartıyla, bir kişiye ilişkin tüm bilgiler" olarak değerlendirmektedir (Çelik, 2017).

Kişisel veriler, veri sahibinin hak ve özgürlüklerine yönelik potansiyel riskler nedeniyle iki ana kategoriye ayrılmaktadır: özel nitelikli ve genel nitelikli veriler (Orel ve Bernik, 2018). Literatürde, özel nitelikli kişisel veriler "özel koruma gerektiren veri" veya "hassas veri" gibi çeşitli isimlerle anılmaktadır. 6698 sayılı KVKK, bu ayrımı "özel nitelikli kişisel veriler" olarak yapmıştır (Kişisel Verileri Koruma Kurumu, 2018). KVKK'nın 6. maddesi, özel nitelikli kişisel verileri şu şekilde tanımlamaktadır: *"Kişilerin ırkı, etnik kökeni, siyasi düşünceleri, felsefi inançları, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri"* (Kişisel Verileri Koruma Kurumu, 2016). Bu verilerin dışında kalan tüm veriler ise genel nitelikli olarak değerlendirilmekte ve bu doğrultuda, verilerin işlenmesi, aktarılması, depolanması ve korunması hususunda öncelik veya ayrıcalık belirlenmektedir.

Özel nitelikli kişisel veriler arasında yer alan kişisel sağlık verileri, 2019 yılında çıkarılan Kişisel Sağlık Verileri Hakkında Yönetmelik'in 4. maddesinde, fiziksel ve ruhsal sağlıkla ilgili veriler ile alınan sağlık hizmetleri sonucunda oluşturulan bilgilerin bütünü olarak tanımlanmıştır. (Başar, 2019). Örneğin, bireyin yaptırdığı tahliller, kullandığı ilaçlar veya geçirdiği tüm hastalıklar kişisel sağlık verisi olarak değerlendirilmektedir (Kişisel Verileri Koruma Kurumu, 2018). Bireylerin sağlık durumlarına ilişkin veriler, kişisel sağlık verileri olarak adlandırılmakta ve hem fiziki hem de elektronik ortamlarda toplanmaktadır (Bezirgan Gözmener, 2019). Son yıllarda tele sağlık, giyilebilir cihazlar ve kişisel sağlık kaydı uygulamaları gibi teknolojik yenilikler, bu verilerin toplanmasını önemli ölçüde kolaylaştırmıştır. Aynı zamanda, kişisel sağlık kayıtlarının dijital ortama aktarılması yönünde

çalışmalar hızla devam etmektedir (Ibraimi ve ark., 2009).

Bilgi ve iletişim teknolojilerindeki hızlı gelişmeler, sağlık sektörünü daha iyi ve daha uygun maliyetli hizmetler sunma arayışına itmiştir. Bu süreçte, kağıt kullanan sistemler yerini elektronik sağlık kayıt (ESK) sistemlerine bırakmaktadır. ESK'lar, hasta bakımını iyileştirmenin yanı sıra hasta-hekim işbirliğini artırmakta, hastalık teşhisini kolaylaştırmakta ve uygulama verimliliğini yükseltmektedir. Ayrıca, hasta sağlık bilgilerini her zaman erişilebilir kılmak suretiyle önemli bir rol üstlenmektedir (Seh ve ark., 2020). Hekimlerin, hastaların geçmiş tanı ve tedavilerine erişebilmesi, yeni tanıların doğru bir şekilde konulmasını ve müdahalelerin daha hızlı ve daha az riskli gerçekleştirilmesini sağlamaktadır. Sağlık alanında yapılan araştırmalar, hasta bilgilerinin erişilebilir olmasının birçok avantaj sunduğunu vurgulamaktadır (Küzeci, 2019).

Sağlık kuruluşları, hastalardan topladıkları hassas verileri, her zaman erişilebilir kılmak ve hasta bakımını kolaylaştırmak amacıyla ağ sunucularında saklamaktadır. Ancak, teknolojik gelişmelerin sağladığı bu avantajlar, aynı zamanda ciddi riskleri de beraberinde getirmektedir. Kişisel sağlık verilerinin dijital ortama taşınması ve bu ortamda saklanması, yalnızca bireylerin sağlık kuruluşlarına başvurmasıyla sınırlı değildir. Günümüzde, akıllı cihazlar (tabletler, saatler, telefonlar) ve giyilebilir teknolojilerin yaygınlaşması, kişisel sağlık verilerinin dijital ortamlarda artmasına önemli ölçüde katkıda bulunmaktadır. Bu cihazların her biri, kullanıcı gizliliği ve veri güvenliği yasalarına uygun hareket etmek zorundadır. Kullanıcılar, bu cihazları kullanmaya başlamadan önce, potansiyel riskler hakkında bilgilendirildikleri sözleşmeleri onaylamaktadırlar (Calvaresi vd., 2020). Akıllı telefonlar ve diğer akıllı cihazlar, giderek daha fazla gizlilik ihlallerinin kaynağı haline gelmektedir (Smith, 2016).

Bununla birlikte, kişisel sağlık bilgilerine ulaşmanın, daha iyi sağlık hizmeti sunmak için gerekli olduğunun kabulü, bu hassas verilere erişimin etik ve yasal tartışmalara yol açmasına neden olmaktadır. Özellikle, bu verilere erişimin kolaylaşması ve yaygınlaşması, bireylerin en temel haklarından biri olan sağlık hakkından bile feragat etmeye zorlanabileceği durumları ortaya çıkarabilir (İzgi, 2014). Bu kapsamda, sağlık sektöründe veri ihlallerinin artması, kişisel sağlık verilerinin korunması konusunu önemli bir sorun haline getirmiştir. Bu veriler, bir bireyin tıbbi geçmişi, tedavileri ve diğer sağlıkla ilgili ayrıntıları içeren hassas bilgilerden oluştuğu için yetkisiz erişim ve kötüye kullanım riskine karşı oldukça savunmasızdır (Ponemon Institute, 2023). Sağlık hizmetlerindeki veri ihlalleri sadece bireyleri değil, sağlık hizmet sunucularını ve genel sağlık ekosistemini de ciddi şekilde etkilemektedir. Dolayısıyla, bu ihlallerin önemi anlaşılmalı, riskler minimize edilmeli ve hasta gizliliği ile güvenliğini sağlamak için etkili stratejiler geliştirilmelidir. Çünkü son araştırmalar, sağlık veri ihlallerinin sıklığında ve ciddiyetinde endişe verici bir artış olduğunu ortaya koymaktadır. Sağlık Bilgi ve Yönetim Sistemleri Topluluğu (HIMSS, 2024) verilerine göre, sağlık veri ihlalleri son beş yılda %35 oranında artmış ve milyonlarca insanı potansiyel kimlik hırsızlığı ve dolandırıcılığa maruz bırakmıştır. Bu durum, veri ihlallerinin nedenlerini daha iyi anlamak ve etkili önlemler geliştirmek için acil bir ihtiyaç doğurmaktadır (Lee & Choi, 2021).

Bunlara ek olarak teknoloji firmalarının, ilaç ve tıbbi cihaz şirketlerinin ve sigorta endüstrisinin kişisel sağlık verilerine olan ilgisi, bu verilerin güvenliği ve gizliliği konusundaki endişeleri daha da artırmaktadır. Orak (2019), biyoteknoloji gibi geleceğin teknolojilerine olan ilginin giderek arttığını ve bu piyasanın beslendiği en önemli kaynağın kişisel sağlık verileri olduğunu ifade etmektedir. Teknolojinin sağladığı imkanlar göz önünde bulundurulduğunda, kişisel sağlık verilerinin gizliliği ve mahremiyeti büyük bir önem kazanmaktadır. Bansal ve ark. (2010), bireylerin kişisel sağlık verilerinin nasıl kullanıldığı, korunduğu ve paylaşıldığı konularında ciddi gizlilik endişeleri taşıdıklarını belirtmektedir. Bu nedenle, veri işleme süreçlerinin tüm aşamalarında gizliliğin korunması ve yetkisiz erişimin önlenmesi kritik bir önem taşımaktadır (Abouelmehdi ve ark., 2018; Mehraeen ve ark., 2016). Yazılım açıkları, güvenlik zafiyetleri ve insan hataları nedeniyle, bu veri tabanlarına zaman zaman yetkisiz kişiler erişebilmekte ve bu durum hassas verilerin ihlal edilmesine yol açabilmektedir. Bu

tür ihlaller, bazen içeriden saldırganlar tarafından gerçekleştirilen bilinçli eylemler sonucu da meydana gelebilmektedir ve sağlık verilerinin kaybolmasına, çalınmasına veya ifşa edilmesine neden olabilmektedir (Seh ve ark., 2020). Bu bağlamda, veri işleme sürecinde şeffaflık ve dürüstlük ilkelerine bağlı kalmak, olası etik ihlallerin engellenmesi açısından kritik bir rol oynamaktadır (Zeybek Ünsal ve Örnek Büken, 2018).

Sağlık hizmetleri verileri, diğer veri türlerine kıyasla daha hassas olarak kabul edilir, çünkü herhangi bir veri tahrifatı, hatalı tedavilere yol açabilir ve bu durum hastalar için ölümcül ve geri dönüşü olmayan sonuçlar doğurabilir. Bu nedenle, sağlık verilerinin daha gelişmiş güvenlik önlemleriyle korunması ve ihlallere karşı dirençli hale getirilmesi gerekmektedir (Seh ve ark., 2020). Diğer veri sektörleriyle kıyaslandığında, sağlık sektörü bu tür ihlallerden en çok etkilenen alanlardan biridir (Liu ve ark., 2015).

İlgili konular çerçevesinde literatürde yapılan çalışmalara bakıldığında sağlık verilerinin yönetimi ve işlenmesine (Safran ve ark., 2007), veri sahipliğinin önemine ve risklerine (Spencer ve ark., 2016), ESK'ların risk ve dezavantajlarının faydaları ile karşılaştırılmasına (Enzzerdou ve ark., 2018), veri güvenliği ve gizliliğine ilişkin paydaşların endişelerine (Häikiö ve ark., 2020), Türkiye'de yapılan bir araştırmada da bireylerin verilerin güvenliği ve gizliliğindeki endişelerine ve herhangi bir ihlal durumunda izlenecek yolu belirlemedeki algılarına (Yılmaz ve ark., 2021) ve güvenilir veri ölçümü, veri iletişimi ve veri analizi sağlanmasında etkili bir araç geliştirilmesine yönelik olduğu görülmektedir.

Bu çalışma, literatürdeki önemli bir boşluğu doldurarak, kişisel sağlık verisi güvenliğine ilişkin sorunların çözümünde doğrudan karar vericilere yol göstermeyi amaçlamaktadır. Literatürde, kişisel sağlık verisi ihlallerini analiz eden çalışmalar genellikle ihlal sonrası etkiler, genel güvenlik önlemleri veya teorik çerçeveler üzerine odaklanmıştır. Ancak bu çalışmada, kişisel sağlık verisi ihlaline neden olan spesifik faktörlerin belirlenmesi, bu faktörlerin önceliklendirilmesi ve doğrudan bu faktörlere yönelik önleyici stratejiler geliştirilmesi hedeflenmiştir. Özellikle, karar vericilere uygulamaya yönelik somut öneriler sunan bir tasarım yaklaşımı benimsenmiş olması, çalışmayı mevcut literatürden farklılaştırmaktadır. BWM gibi sistematik bir karar verme tekniği ile, karar vericilere, kaynakların en etkili şekilde kullanılması ve stratejilerinin önceliklendirilmesi konusunda proaktif bir yaklaşım sunarak; bu yönüyle literatürdeki hem teorik hem de pratik boşluğu doldurmaktadır.

Bu kapsamda çalışmanın amacı, kişisel sağlık verisi ihlallerine neden olan faktörleri belirlemek, bu faktörleri BWM (Best Worst Method) yaklaşımı ile önceliklendirmek ve elde edilen öncelikler doğrultusunda sağlık verisi güvenliğini artırmaya yönelik çözüm önerileri sunmaktır.

2. MATERYAL VE METOT

Çalışmada ÇKKV yöntemlerinden biri olan BWM (Best-Worst Method) ile veriler analiz edilmiştir. Bu yöntem, aralarında en iyisini ve en kötüsünü belirlemek için bir küme içindeki kriterleri karşılaştırmayı içerir ve karar vericilerin bu karşılaştırmalara dayanarak ağırlıklar atamasını sağlar. Bu doğrultuda çalışmanın temel amaç sorusu;

- Kişisel sağlık verisi ihlalleri nasıl önlenebilir?

Bu temel amaç doğrultusunda, çalışmanın alt amaç soruları şu şekilde sıralanabilir;

- Kişisel sağlık verisi ihlallerine neden olan en iyi (önemli) faktör nedir?
- Kişisel sağlık verisi ihlallerine neden olan en kötü (önemsiz) faktör nedir?
- Kişisel sağlık verisi ihlallerine neden olan faktörlerin önem dereceleri nedir?

2.1. BWM Yöntemi

BWM, karar vericilerin kriterleri ve alternatifleri göreceli önemlerine göre verimli bir şekilde değerlendirmelerine olanak tanıyan yapılandırılmış çiftler halinde karşılaştırma sistemi ile ayırt edilir (Rezaei, 2020). En iyi ve en kötü kriterleri karşılaştırarak, BWM karar alma için ağırlıkların belirlenmesini kolaylaştırır ve en uygun alternatiflerin seçilmesine yardımcı olur (Hidayat vd., 2021). BWM'nin karar alma sürecini kolaylaştırma ve değerli içgörüler sağlama kapasitesi, onu karmaşık senaryolarda alternatifleri değerlen-

dirmek ve önceliklendirmek için tercih edilen bir yöntem haline getirmiştir (Sujanto, 2024). Yöntem süreci 6 aşamada ifade edilebilir;

1. Kriterlerin belirlenmesi: Karar verme problemi için önemli kriterler belirlenir. Bu aşamada, karar verme sürecine dahil edilecek tüm kriterlerin kapsamı tanımlanır.

$$n = \{c_1, c_2, c_3, \ldots, c_n\} \quad (1)$$

2. En iyi ve en kötü kriterlerin seçimi: Karar verici, kriterler arasında en önemli olanını (en iyi) ve en az önemli olanını (en kötü) seçer. Bu seçim, karar vericinin kriterler arasında hangi kriterlerin daha öncelikli olduğunu belirtir.

3. Çiftler halinde karşılaştırma: En iyi kriter ile diğer tüm kriterler arasındaki karşılaştırmalar yapılır. Aynı şekilde, en kötü kriter ile diğer tüm kriterler arasındaki karşılaştırmalar yapılır. Bu karşılaştırmalar genellikle 1'den 9'a kadar olan bir ölçek kullanılarak yapılır.

4. Karşılaştırma matrisi oluşturulması: Tercihler matrisinin, 1 ile 9 arasındaki rakamlar kullanılarak en kötü kriterin diğerlerine göre karşılaştırılmasına dayalı olarak tasarlanır.

5. Ağırlıkların hesaplanması

5.1. En iyi kriter ile diğer kriterler arasındaki karşılaştırmalar: Bu karşılaştırmalar, en iyi kriterin diğer kriterler karşısındaki göreli önemini yansıtır. Diğerlerine göre en iyiler vektörü; $A_B = (a_{B1}, a_{B2}, a_{B3}, \ldots, a_{Bn})$, burada a_{Bj} en iyi *B* kriterinin *j* kriterine göre tercihini gösterir. $a_{BB} = 1$

5.2. En kötü kriter ile diğer kriterler arasındaki karşılaştırmalar: Bu karşılaştırmalar, en kötü kriterin diğer kriterler karşısındaki göreli önemini belirtir. Diğerlerine göre en kötüler vektörü $Aw = (a_{1w}, a_{2w}, a_{3w}, \ldots, a_{nW})^T$, burada a_{jW}, *j* kriterinin en kötü kriter olan *W* kriterine göre tercihini gösterir. $a_{WW} = 1$

6. Sonuçların analizi ve doğrulama

Bu karşılaştırma sonuçları kullanılarak, her bir kriterin ağırlığı hesaplanır.

Optimal ağırlıklar (w_1 *, w_2 *, w_3 *, …,w_n *) hesaplanır. Kriterlerin optimal ağırlıkları aşağıdaki gerekçeleri karşılar. Her bir w_B/w_j and w_j/w_W, çifti için ideal durum $w_B/w_j = a_{Bj}$ and $w_j/w_W = a_{jW}$ olacaktır. Bu nedenle, ideal duruma olabildiğince yakın olmak için, küme arasındaki maksimum en aza indirgenmelidir. Bu durum şu şekilde formüle edilmektedir;

$$\left\{\left|\omega_B - \alpha_{B_j}\omega_j\right|, \left|\omega_j - \alpha_{j_w}\omega_w\right|\right\} \quad (2)$$

$$\min \max_j \left\{\left|\omega_B - \alpha_{B_j}\omega_j\right|, \left|\omega_j - \alpha_{j_w}\omega_w\right|\right\} \quad (3)$$

$$\sum_j \omega_j = 1$$

$w_j \geq 0$, tüm j için

Problem denklemi aşağıdaki doğrusal programlama problemine aktarılabilir:

$$\min \xi^L$$

$$|\omega_B - \alpha_{B_j}\omega_j| \leq \xi^L \quad (4)$$

$$|\omega_j - \alpha_{j_w}\omega_w| \leq \xi^L \quad (5)$$

$$\sum_j \omega_j = 1$$

$w_j \geq 0$, tüm j için

Bu adımlar, BWM'nin sistematik bir şekilde kriterlerin ağırlıklarını belirlemesini sağlar ve karar verme sürecini daha şeffaf ve tutarlı hale getirir.

2.2. Katılımcılar

Literatür taraması sonucunda, kişisel sağlık verisi ihlalleri tespit edilmiştir. Elde edilen ihlallerin değerlendirilmesi, sağlık yönetimi ve sağlık hukuku alanlarında en az 7 yıllık akademik veya profesyonel deneyime sahip 6 farklı uzman tarafından yapılmıştır. Bu kesitsel araştırma 20.10.2024-25.10.2024 tarihleri arasında gerçekleştirilmiştir. Uzmanlara ait değerlendirmeler yüz yüze BWM anket formu aracılığıyla toplanmıştır. Uzmanlar, konuya ilişkin değerlendirmelerini BWM (Best-Worst Method) formları üzerinden gerçekleştirmiştir. Uzmanlara ilişkin bilgiler Tablo 1'de yer almaktadır.

3. BULGULAR

Kişisel sağlık verisi ihlallerinin değerlendirilmesi için literatür taraması sonucunda belirlenen kriterler açıklamaları ve kaynakları ile Tablo 2'de gösterilmektedir.

Karar verici uzmanların en iyi ve en kötü kriter seçimleri ve (en iyi-diğer) ve (en kötü-diğer) karşılaştırmaları Tablo 3'te ifade edilmektedir. En iyi kriterin diğerlerine ve en kötü kriterin diğerlerine göre karşılaştırmaları uzmanlar tarafından 1-9 arasındaki rakamlar üzerinden yapılmıştır.

Tablo 4'de uzmanlara ait görüşler doğrultusunda modelin ilgili optimizasyon hesaplamaları yapılarak her bir kriter ağırlığı belirlenmiştir. Ayrıca kriter ağırlıkları doğrultusunda tutarlılık oranı hesaplanmıştır. Tutarlılık oranının <0,10 olması uzman görüşlerinin güvenirliğini ortaya koymaktadır.

Tablo 1. Uzmanlara İlişkin Detaylar

Uzmanlar	Uzmanlık Alanı	Eğitim Seviyesi	Pozisyon	Deneyim
U1	Sağlık Yönetimi	Doktora	Doç. Dr.	10 yıl
U2	Sağlık Yönetimi	Doktora	Dr. Öğr. Üyesi	8 yıl
U3	Sağlık Yönetimi	Doktora	Dr. Öğr. Üyesi	7 yıl
U4	Sağlık Yönetimi	Yüksek Lisans	Öğr. Gör.	7 yıl
U5	Sağlık Hukuku	Doktora	Dr. Öğr. Üyesi	11 yıl
U6	Sağlık Hukuku	Yüksek Lisans	Avukat	8 yıl

Tablo 2. Kişisel Sağlık Verisi İhlalleri Kriterleri

Kısaltma	Kriterler (İhlal Türleri)	Kriter Açıklamaları	Kaynak
VS	**Veri Sızıntısı**	Veri sızıntısı, sağlık verilerinin yetkisiz kişilere yanlışlıkla veya bilinçli olarak ifşa edilmesi anlamına gelir.	Yaraghi ve Gopal, 2018
İH	**İnsan Hataları**	Çalışanların bilinçsiz davranışları, dikkatsizlikleri veya yanlış işlemler yapmaları sonucunda verilerin yanlış kişilere iletilmesi veya yanlışlıkla silinmesi gibi durumları kapsar.	Kwan vd., 2020
KAY	**Kötü Amaçlı Yazılımlar**	Kötü amaçlı yazılımlar (malware), sistemlere sızarak verileri çalma, şifreleme veya yok etme gibi zararlar verebilir. Phishing saldırıları veya güvensiz yazılımların kullanımı ile sistemlere bulaşır.	Carter ve Hartridge, 2018
GD	**Güvenlik Düzeyi (Şifreleme)**	Güvenlik düzeyi, verilerin şifrelenmesi ve korunması ile ilgilidir. Yetersiz veya hatalı şifreleme uygulamaları, sağlık verilerinin güvenliğini tehdit eder ve yetkisiz kişilerin bu verilere erişmesini kolaylaştırabilir.	Molitor, 2024
SS	**Siber Saldırılar**	Sistemlerin zafiyetlerinden faydalanarak verileri çalmayı, değiştirmeyi veya yok etmeyi hedefleyen Ransomware, DDoS ve veri hırsızlığı gibi saldırılardır.	Kruse vd., 2017
YE	**Yetkisiz Erişim**	Yetkisiz erişim, veriye erişme yetkisi olmayan kişilerin verilere ulaşması anlamına gelir. Sağlık kurumlarında yetkisiz erişim, verilerin gizliliğini ihlal eder ve hasta güvenliği için ciddi tehditler oluşturur.	Masuch vd., 2022
AS	**Ayrıcalık Suistimali**	Ayrıcalık suistimali, sistemde yetkisi olan bireylerin bu yetkilerini kötüye kullanarak verilere izinsiz erişim sağlaması anlamına gelir. Örneğin, bir sağlık çalışanının erişim izni olan hasta kayıtlarını kişisel çıkarları için kullanması veya paylaşması bu kategoriye girer.	Seh vd., 2021
VİP	**Uygunsuz Veri İmha Politikaları**	Uygunsuz veri imha politikaları, verilerin güvenli bir şekilde imha edilmemesi sonucunda oluşan ihlalleri ifade eder. Yanlış imha edilen veri, siber saldırılara açık hale gelir ve kişisel verilerin kötüye kullanılmasına yol açar.	Flanagin vd., 2020

Her bir kritere ait ağırlıkların ortalamaları alınarak elde edilen kriter sıralamaları Tablo 5'te yer almaktadır.

Tablo 5'e göre, kişisel sağlık verisi ihlallerine neden olan en önemli (en iyi) kriter %16,95 ağırlık puanı ile "Siber Saldırılar"'dır. Daha sonra sırasıyla "Veri Sızıntısı" (%16,77), "Ayrıcalık Sustimali" (%15,10) ve "Kötü Amaçlı Yazılımlar" (%15,07) gelmektedir. Bu doğrultuda ilk 4 kriter %63,9 ağırlık puanı ile önemli bir çoğunluğu ifade etmektedir. "Uygunsuz Veri İmha Politikaları" ise %5,01 ağırlık ile en az önemli (en kötü) kriter olarak tespit edilmiştir.

Tablo 3. Uzmanların En İyi ve En Kötü İhlal Kriterlerine İlişkin Karşılaştırmalı Tercihleri

Uzman	En İyi/En Kötü	Seçim	VS	İH	KAY	GD	SS	YE	AS	VİP
U1	En İyi	AS	3	6	3	4	6	7	1	9
	En Kötü	VİP	5	3	4	3	3	2	9	1
U2	En İyi	SS	2	8	2	3	1	4	4	4
	En Kötü	İH	4	1	7	6	5	5	5	6
U3	En İyi	VS	1	3	4	3	4	4	6	2
	En Kötü	VİP	7	2	2	4	3	2	2	1
U4	En İyi	KAY	3	6	1	4	2	7	3	2
	En Kötü	VİP	4	2	7	3	2	2	4	1
U5	En İyi	SS	2	5	2	4	1	3	5	8
	En Kötü	VİP	8	4	3	4	7	5	5	1
U6	En İyi	İH	3	1	5	5	3	2	2	8
	En Kötü	VİP	4	7	3	4	4	6	6	1

Tablo 4. Kriter Ağırlıkları ve Tutarlılık Oranları

Kriterler	Uzman 1	Uzman 2	Uzman 3	Uzman 4	Uzman 5	Uzman 6
VS	0,1403	0,1728	0,2713	0,1327	0,1777	0,1116
İH	0,0701	0,0305	0,1407	0,0663	0,0711	0,2767
KAY	0,1403	0,1728	0,1055	0,2559	0,1631	0,0669
GD	0,1052	0,1152	0,1407	0,0995	0,0888	0,0669
SS	0,0701	0,2491	0,1055	0,1990	0,2802	0,1116
YE	0,0601	0,0864	0,1055	0,0568	0,1185	0,1674
AS	0,3766	0,0864	0,0703	0,1327	0,0711	0,1674
VİP	0,0369	0,0864	0,0603	0,0568	0,0292	0,0312

***CR** 0,0892*

CR: Consistency ratio.

Tablo 5. Ortalama Ağırlıklar ve Sıralama

Kriterler	Ağırlıklı Ortalamalar	Sıralama
Veri Sızıntısı	0,1677	2
İnsan Hataları	0,1092	5
Kötü Amaçlı Yazılımlar	0,1507	4
Güvenlik Düzeyi (Şifreleme)	0,1027	6
Siber Saldırılar	0,1695	1
Yetkisiz Erişim	0,0991	7
Ayrıcalık Suistimali	0,1510	3
Uygunsuz Veri İmha Politikaları	0,0501	8

4. TARTIŞMA VE SONUÇ

Çalışmada, kişisel sağlık verisi ihlallerine sebebiyet veren en iyi ve en önemli kriterlerin siber saldırılar, veri sızıntısı, ayrıcalık suistimali ve kötü amaçlı yazılımlar olduğu tespit edilmiştir.

En yüksek öneme (%16,95) sahip siber saldırılar kriterine yönelik alan yazında bu kanıyı destekleyen araştırmalar mevcuttur. Kruse vd. (2017) siber saldırıların 2010 yılından bu yana %125 oranında arttığını ve sağlık verileri güvenliği ihlallerinde baskın faktör haline geldiğini vurgulamaktadır. Bu eğilim, sağlık hizmetleri ortamlarında mobil cihazların giderek daha fazla benimsenmesinin güvenlik açıklarını artırdığını ve sağlık kuruluşlarını siber tehditler için birincil hedef haline getirdiğini belirtenler tarafından da desteklenmektedir (Coventry & Branley, 2018). Benzer şekilde Lee ve Choi (2021) sağlık hizmetlerinde bildirilen veri ihlallerinde 2016'da 329'dan 2020'de 642'ye önemli bir artış olduğunu belgeleyen ve sağlık kuruluşlarını etkileyen siber olaylarda artan bir eğilime işaret etmişlerdir. Kessel (2023) ise sağlık alanındaki veri ihlallerinin %76'sının temel web uygulaması saldırılarından kaynaklı siber saldırılar olduğunu vurgulamaktadır. Awaludin vd. (2023) pandeminin sağlık kurumlarında siber saldırılarda nasıl bir artışa yol açtığını değerlendirdiği çalışmalarında çevrimiçi hizmetlere hızlı geçişin siber saldırıları ve suçluları artırarak yeni veri ihlallerine neden olduğunu vurgulamışlardır. Benzer şekilde Škiljić (2020) çalışmasında özellikle kimlik avı saldırılarının, sağlık hizmetleri de dahil olmak üzere çeşitli sektörlerde veri ihlallerinin önde gelen kaynağı olarak tanımlandığını ve yaygın bir siber saldırı biçimi olduğunu ifade etmektedir.

İkinci en iyi ve yüksek öneme (%16,77) sahip kriter veri sızıntısıdır. Bu bulguyla örtüşecek şekilde alan yazında Fang vd. (2019) yaptıkları çalışmalarında hassas bilgilerin siber suçlular tarafından sıklıkla hedef alındığı sağlık sektöründe veri sızıntısının yaygın bir sorun olduğunu vurgulamaktadır. Benzer şekilde Ewoh (2024) sağlık sektörünün sağlık bilgilerinin korunması açısından diğer sektörlerin gerisinde kaldığını ve ihlallerin önemli bir kısmının veri sızıntısından kaynaklandığını belirtmektedir. Kwan vd. (2020) ise hasta bilgilerinin gizliliğine yönelik birçok tehdidin kurumsal olarak ilişkili olduğunu ve veri sızıntısının önemli bir faktör olduğunu ifade etmişlerdir. Looi (2024) çalışmasında psikiyatrik elektronik sağlık kayıtlarındaki veri ihlallerinin sonuçlarını tartışmakta ve hassas bilgilere sızıntıyı önlemek için sıkı veri koruma önlemlerine duyulan ihtiyacı vurgulamaktadır. Benzer şekilde Choi vd. (2019) sağlık verileri ihlalleri bağlamında, veri sızıntısının sonuçlarını tartıştığı çalışmalarında, bu tür riskleri azaltmak için etkili veri yönetimi uygulamalarına duyulan ihtiyacı vurgulamaktadır.

Üçüncü en iyi ve yüksek önemli kriter (%15,10) ise ayrıcalık suistimalidir. Alan yazına bakıldığında Choi vd. (2019) çalışmalarında sağlık kuruluşlarında yaşanan birçok veri

ihlalinin yetkili personel tarafından ayrıcalıkların kötüye kullanılmasıyla bağlantılı olduğunu vurgulamışlardır. Benzer şekilde Almaghrabi ve Bugis (2022) çalışmalarında sağlık çalışanları tarafından yetkisiz erişim ve ayrıcalıkların kötüye kullanılmasının hasta verilerinde önemli ihlallere yol açabileceğini vurgulayarak sağlam erişim kontrol mekanizmalarına duyulan ihtiyacın altını çizmektedirler. Bir diğer yandan Seh vd. (2021) çalışmalarında ayrıcalıkların kötüye kullanılmasının sağlık hizmetleri veri güvenliğine yönelik en yaygın tehditler arasında yer aldığını vurgulamışlardır.

Dördüncü önemli kriter (%15,07) ise kötü amaçlı yazılımlardır. Jiang ve Bai (2019) sağlık verisi ihlallerinin nedenlerine ilişkin ampirik kanıtları araştırdığı çalışmalarında kötü amaçlı yazılımları en önemli nedenlerden biri olarak belirtmişlerdir. Benzer şekilde Ismail (2024) çalışmasında fidye yazılımları ve diğer kötü amaçlı yazılımların sağlık sistemlerinde önemli veri ihlallerine yol açabilecek yaygın bir tehdit olduğunu vurgulamaktadır. Diğer bir yandan Taher vd. (2023) çalışmasında siber suçluların sürekli olarak mobil cihazlardaki ve uygulamalardaki güvenlik açıklarından yararlanabilen ve böylece kişisel sağlık verileri için önemli bir risk oluşturan yeni kötü amaçlı yazılım türleri geliştirdiğini belirtmektedir. Ullah vd. (2019) ise IoT cihazlarını hedef alan kötü amaçlı yazılımların yaygınlaştığını bu sebeple kişisel sağlık verisi ihlallerinin arttığını savunmaktadır.

Sonuç olarak, sağlık verilerinin ihlalinin engellenebilmesi ve etkili bir veri güvenliği yönetimi için çok yönlü stratejiler geliştirilmesi gerekmektedir. Siber saldırılara karşı, gelişmiş güvenlik önlemleri, düzenli güvenlik denetimleri ve ağ segmentasyonu gibi yöntemler önerilmektedir. Tüm çalışanları için siber güvenlik uygulamalarının önemini vurgulayan kapsamlı eğitim programları uygulanmalıdır. Bu durum kimlik avı girişimlerini tanımayı, veri sızıntısının sonuçlarını anlamayı ve hassas bilgilerin uygun şekilde değerlendirilmesi ve paylaşılması bilincini artıracaktır. Veri sızıntılarının önlenmesi için veri şifreleme, erişim kontrol politikaları ve çalışan farkındalık eğitimleri kritik öneme sahiptir. Hassas sağlık verilerinin hem beklemede hem de aktarım sırasında şifrelenmesi, veri sızıntısı riskini önemli ölçüde azaltabilir. Hasta kimliği; anonimleştirme, veri setlerinin kümelenmesi veya gerçek hasta kimliği yerine bulanıklaştırma tekniği gibi birtakım yöntemler kullanılarak mahremiyetin korunabilmesi sağlanabilir. Güvenli iletişim protokollerinin (HTTPS ve VPN'ler gibi) uygulanması, verileri iletim sırasında saldırılara karşı korumaktadır. Ayrıcalık suistimalinin etkilerini azaltmak ise rol tabanlı erişim kontrolü, kullanıcı faaliyetlerinin izlenmesi ve düzenli erişim denetimleri gibi yöntemler uygulanmalıdır. Sağlık yöneticileri, çalışanların sorumluluklarını yerine getirmek için gerekli minimum erişim düzeyinin verildiği en az ayrıcalık ilkesinin uygulanmasını gerektiren politikaları yürütmelidir. Erişim günlüklerinin düzenli olarak denetlenmesi ve yetkisiz erişim girişimlerinin tespit edilmesi önemlidir. Kötü amaçlı yazılımlara karşı düzenli yazılım güncellemeleri, güçlü anti-malware çözümleri ve çalışanların siber hijyen konusundaki farkındalığının artırılması gerekmektedir. Saldırı tespit sistemleri (STS) gibi araçlar şüpheli faaliyetler için ağ trafiğini izleyerek sağlık yöneticilerini potansiyel tehditlere karşı uyarmaktadır.

Kişisel sağlık verisi ihlallerinin önüne geçebilmek ve veri güvenliğini sağlamak için belirtilen öneriler sağlık kuruluşlarının tehditlere karşı daha dirençli hale gelmesini ve sağlık yöneticilerinin bu süreç dahilinde kanıta dayalı ve etkili kararlar alabilmesini desteklemektedir.

KAYNAKÇA

ABOUELMEHDI, K., BENI-HESSANE, A., & KHALOUFI, H. (2018). Big Healthcare Data: Preserving Security and Privacy. *Journal of Big Data*, 5(1), 1-18. https://doi.org/10.1186/s40537-017-0110-7.

ALMAGHRABI, N. S. & BUGIS, B. A. (2022). Patient Confidentiality of Electronic Health Records: A Recent Review of the Saudi Literature. *Dr. Sulaiman Al Habib Medical Journal*, 4(3), 126-135. https://doi.org/10.1007/s44229-022-00016-9.

ATALAY, H. N. (2022). Kişisel Sağlık Verileri Paylaşma Niyeti ile Gizlilik Endişesi ve Algılanan Kontrol Arasındaki İlişkide Algılanan Risk ve Algılanan Faydanın

Aracı Rolü. (Yüksek Lisans Tezi). Selçuk Üniversitesi Sağlık Bilimler Enstitüsü, Konya.

AWALUDIN, A., SULISTYADI, W., & CHANDRA, A. F. (2023). Analysis of Attacks and Cybersecurity in the Health Sector During a Pandemic COVID-19: Scoping Review. *Journal of Social Science*, 4(1), 62-70. https://doi.org/10.46799/jss.v4i1.512.

BANSAL, G., ZAHEDI, M. F., & GEFEN, D. (2010). The Impact of Personal Dispositions on Information Sensitivity, Privacy Concern and Trust in Disclosing Health Information Online. *Decision Support Systems*, 49(2), 138-150. https://doi.org/10.1016/j.dss.2010.01.010.

BASKAN, S. A., KARAKURT, P., & KASIMOGLU, N. (2021). Assessment of Nursing Students' Attitudes Towards Recording and Protecting Patients' Personal Health Data: A Descriptive Study. *Galician Medical Journal*, 28(3), E202133. https://doi.org/10.21802/gmj.2021.3.3.

BAŞAR, C. (2019). Türk İdare Hukuku ve Avrupa Birliği Hukuku Işığında Kişisel Verilerin Korunması. (Doktora Tezi). Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir.

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

BEZIRGAN GÖZMENER, S. (2019). Kişisel Sağlık Verilerinin Kayıt ve Korunmasında Hemşirelerin Cezai Sorumluluğu. (Yüksek Lisans Tezi). Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İzmir.

CALVARESI, D., SCHUMACHER, M., & CALBIMONTE, J. P. (2020). 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.

CHOI, S. J., JOHNSON, M. E., & LEHMANN, C. U. (2019). Data Breach Remediation Efforts and Their Implications for Hospital Quality. *Health Services Research*, 54(5), 971-980. https://doi.org/10.1111/1475-6773.13203.

COVENTRY, L., & BRANLEY, D. (2018). Cybersecurity in Healthcare: A Narrative Review of Trends, Threats and Ways Forward. *Maturitas*, 113, 48-52.

ÇELİK, Y. (2017). Özel Hayatın Gizliliğinin Yansıması Olarak Kişisel Verilerin Korunması ve Bu Bağlamda Unutulma Hakkı. *Türkiye Adalet Akademisi Dergisi*, 32, 391-410. https://dergipark.org.tr/tr/pub/taad/issue/52657/693992.

ÇOBAN, Ç., & TÜYSÜZ, M. F. (2019). E-Sağlık ve Güvenlik: Riskler, Fırsatlar ve Çözüm Önerileri. *Academic Perspective Procedia*, 2(3), 925-934. https://doi.org/10.33793/acperpro.02.03.104.

DURMUŞ, V. (2021). Kişisel Sağlık Verilerinin Korunmasında İdarenin Hukuki Sorumluluğu. *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi (DEUHFED)*, 14(1), 67-76.

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

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. *Healthcare Technology Letters*, 5(1), 54-60. https://doi.org/10.1049/htl.2017.0017.

ESKİMEZ, Z., & TOSUNOZ, İ. K. (2023). Hemşirelik Öğrencilerinin Kişisel Sağlık Verilerinin Kayıt ve Korunması Konusundaki Tutumları. *Etkili Hemşirelik Dergisi*, 16(4), 513-523.

EWOH, P. & VARTIAINEN, T. (2024). Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review. *Journal of Medical Internet Research*, 26, e46904. https://doi.org/10.2196/46904.

FANG, Y., GUO, Y., HUANG, C., & LIU, L. (2019). Analyzing and Identifying Data Breaches in Underground Forums. *IEEE Access*, 7, 48770-48777. https://doi.org/10.1109/access.2019.2910229.

GÖKÇAY, B., & ARDA, B. (2019). Kişisel Sağlık Verilerinin Korunması Kapsamında Sağlık Araştırmalarında Etik Bakış. *Turk Kardiyol Derneği Araştırmaları*, 47(3), 218-227.

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.

IBRAIMI, L., ASIM, M., & PETKOVIĆ, M. (2009). Secure Management of Personal Health Records by Applying Attribute-Based Encryption. In *Proceedings of the 6th International Workshop on Wearable, Micro, and Nano Technologies for Personalized Health* (pp. 71-74). https://doi.org/10.1109/PHEALTH.2009.5754828.

ISMAIL, S. J. I., HENDRAWAN, RAHARDJO, B., JUHANA, T., & MUSASHI, Y. (2024). Malssl—Self-Supervised Learning for Accurate and Label-Efficient Malware Classification. *IEEE Access*, 12, 58823-58835. https://doi.org/10.1109/access.2024.3392251.

İZGİ, M. C. (2014). Mahremiyet Kavramı Bağlamında Kişisel Sağlık Verileri. *Türkiye Biyoetik Dergisi*, 1(1),

25-37. Erişim adresi: http://turkishbioethics.org/jvi.aspx?pdir=tjob&plng=tur&un=TJOB65375.

JIANG, J. X., & BAI, G. (2019). Evaluation of Causes of Protected Health Information Breaches. *JAMA Internal Medicine*, 179(2), 265-267.

KİŞİSEL VERİLERİ KORUMA KURUMU. (2018). Kişisel Verilerin Korunması Kanunu Hakkında Sıkça Sorulan Sorular. Erişim adresi: https://www.kvkk.gov.tr/Icerik/4196/KisiselVerilerin-Korunmasi-Kanunu-Hakkinda-Sikca-Sorulan-Sorular.

KİŞİSEL VERİLERİ KORUMA KURUMU. (2018a). 100 Soruda Kişisel Verileri Koruma Kanunu. KVKK Yayınları, Ankara.

KİŞİSEL VERİLERİ KORUMA KURUMU. (2018b). Kişisel Verilerin Korunması Kanunu ve Uygulaması. Erişim adresi: https://www.kvkk.gov.tr/yayinlar/K%C4%B0%C5%9E%C4%B0SEL%20VER%C4%B0LER%C4%B0N%20KORUNMASI%20KANUNU%20VE%20UYGULAMASI.pdf.

KİŞİSEL VERİLERİ KORUNMASI KANUNU. (2016). 6698 Sayılı Kişisel Verilerin Korunması Kanunu.

KRUSE, C. S., FREDERICK, B., JACOBSON, T., & MONTICONE, D. K. (2017). Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends. *Technology and Health Care*, 25(1), 1-10.

KÜZECİ, E. (2019). Kişisel Verilerin Korunması (3. Baskı). Seçkin Yayıncılık, Ankara.

KWAN, H. H., RILEY, M., PRASAD, N., & ROBINSON, K. (2020). An Investigation of the Status and Maturity of Hospitals' Health Information Governance in Victoria, Australia. *Health Information Management Journal*, 51(2), 89-97. https://doi.org/10.1177/1833358320938309.

LEE, J., & CHOI, S. J. (2021). Hospital Productivity After Data Breaches: Difference-in-Differences Analysis. *Journal of Medical Internet Research*, 23(7), e26157.

LI, J. (2015). Ensuring Privacy in a Personal Health Record System. *Computer*, 48(2), 24-31. https://ieeexplore.ieee.org/abstract/document/7042698.

LIU, V., MUSEN, M. A., & CHOU, T. (2015). Data Breaches of Protected Health Information in the United States. *JAMA*, 313(14), 1471-1473.

LOOI, J. C., LOOI, R. C., MAGUIRE, P. A., KISELY, S., BASTIAMPILLAI, T., & ALLISON, S. (2024). Psychiatric Electronic Health Records in the Era of Data Breaches – What Are the Ramifications for Patients, Psychiatrists and Healthcare Systems?. *Australasian Psychiatry*, 32(2), 121-124. https://doi.org/10.1177/10398562241230816.

MEHRAEEN, E., AYATOLLAHI, H., & AHMADI, M. (2016). Health Information Security in Hospitals: The Application of Security Safeguards. *Acta Informatica Medica*, 24(1), 47-50. https://doi.org/10.5455/aim.2016.24.47-50.

ORAK, B. (2019). Kişisel Sağlık Verilerinin Korunması. (Yüksek Lisans Tezi). Hacettepe Üniversitesi, Ankara.

OREL, A., & BERNIK, I. (2018). GDPR and Health Personal Data; Tricks and Traps of Compliance. *Studies in Health Technology and Informatics*, 255, 155-159. PMID: 30306927.

ÖKSÜZOĞLU, H. T. (2019). 6698 Sayılı Kişisel Verilerin Korunması Kanunu ve Avrupa Birliği Hukukunda Kişisel Verilerin Silinmesi ve Düzeltilmesi. *Bilişim Hukuku Dergisi*, 2, 185-242.

ÖZDEMİR, M., YILMAZ, M., & KAYA, H. (2022). Kişisel Sağlık Verilerinin 6698 Sayılı Kanun Çerçevesinde Korunması. *19 Mayıs Sosyal Bilimler Dergisi*, 3(1), 85-96. https://doi.org/10.52835/19maysbd.1079524.

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.

SEH, A. H., AL-AMRI, J. F., SUBAHI, A. F., AGRAWAL, A., KUMAR, R., & KHAN, R. A. (2021). Machine Learning Based Framework for Maintaining Privacy of Healthcare Data. *Intelligent Automation & Soft Computing*, 29(3), 697-712. https://doi.org/10.32604/iasc.2021.018048.

SEH, A. H., ZAROUR, M., ALENEZI, M., SARKAR, A. K., AGRAWAL, A., KUMAR, R., & AHMAD KHAN, R. (2020). Healthcare Data Breaches: Insights and Implications. In *Healthcare* (Vol. 8, No. 2, p. 133). MDPI.

ŠKILJIĆ, A. (2020). Cybersecurity and Remote Working: Croatia's (Non-)Response to Increased Cyber Threats. *International Cybersecurity Law Review*, 1(1-2), 51-61. https://doi.org/10.1365/s43439-020-00014-3.

SMITH, T. T. (2016). Examining Data Privacy Breaches in Healthcare. Erişim adresi: https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=3726&context=dissertations (12 Mayıs 2020'de erişildi).

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), 66.

TAHER, F., ALFANDI, O., AL-KFAIRY, M., HAMADI, H. A., & ALRABAE, S. (2023). DroidDetectMW: A Hybrid Intelligent Model for Android Malware Detection. *Applied Sciences*, 13(13), 7720. https://doi.org/10.3390/app13137720.

ULLAH, F., NAEEM, H., JABBAR, S., KHALID, S., LATIF, M. A., AL-TURJMAN, F., … & MOSTARDA, L. (2019). Cyber Security Threats Detection in Internet of Things Using Deep Learning Approach. *IEEE Access*, 7, 124379-124389. https://doi.org/10.1109/access.2019.2937347.

VAN KESSEL, R., HAIG, M., & MOSSIALOS, E. (2023). Strengthening Cybersecurity for Patient Data Protection in Europe. *Journal of Medical Internet Research*, 25, e48824.

YILDIRIM, B. F. (2019). Sağlığın Kişiselleşmesi ve Kişisel Sağlık Bilgi Sistemleri. *Bilgi Yönetimi Dergisi*, 2(2), 127-135.

YILMAZ, D., ERGÜNER ÖZKOÇ, E., & ÖĞÜTÇÜ, G. (2021). Elektronik Sağlık Kayıtlarında Farkındalık. *Hacettepe Sağlık İdaresi Dergisi*, 24(4), 777-792.

ZEYBEK ÜNSAL, Ç., & ÖRNEK BÜKEN, N. (2018). Biyotıp Araştırmaları İle İlgili Olarak, "Kişisel Verilerin Korunması Kanunu" ve "Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik" Ne Diyor?. *Türkiye Klinikleri Journal of Medical Ethics Law and History-Special Topics*, 4(1), 82-90.

Notlar

Araştırmanın yapılabilmesi için İstanbul Medipol Üniversitesi Girişimsel Olmayan Klinik Araştırmalar Etik Kurulu Başkanlığı'ndan bilimsel ve etik açıdan uygun olduğuna dair (16.10.2024; E-10840098-202.3.02-6360 sayılı yazı) görüş alınmıştır.