DOI: 10.34108/eujhs.1327158

SAĞLIK BİLİMLERİ DERGİSİ
JOURNAL OF HEALTH SCIENCES
Erciyes Üniversitesi Sağlık Bilimleri Enstitüsü Yayın Organıdır

Araştırma 2024; 33(1): 98-105

HASTA GÜVENLİĞİNE BİR BAKIŞ: HEMŞİRELERİN BİLGİ GÜVENLİĞİ FARKINDALIK DÜZEYİNİN DEĞERLENDİRİLMESİ

A VIEW ON PATIENT SAFETY: ASSESSMENT OF NURSES' INFORMATION SECURITY AWARENESS LEVEL

Bilgen ÖZLÜK[1], Melek ÇAKIR[2]

[1] Necmettin Erbakan Üniversitesi, Hemşirelik Fakültesi, Hemşirelikte Yönetim Anabilim Dalı, Konya,
[2]Sağlık Bilimleri Üniversitesi, Ankara Atatürk Sanatoryum Eğitim ve Araştırma Hastanesi, Ankara

ÖZ

Bu çalışmada, hemşirelerin bilgi güvenliği farkındalık düzeyini belirlemek amaçlandı. Tanımlayıcı tipteki çalışma, Ankara ilindeki bir eğitim ve araştırma hastanesinde çalışan 294 hemşire ile Haziran-Ağustos 2022 tarihleri arasında gerçekleştirildi. Veriler, Tanıtıcı Özellikler Formu ve Bilgi Güvenliği Ölçeği ile toplandı. Veri analizinde tanımlayıcı istatistikler, bağımsız örneklem t testi ve tek yönlü varyans analizi kullanıldı. Hemşirelerin %47.3'ünün bilgi güvenliğine yönelik bir eğitim almadığı ve %97.6'sının hastane bilgi sistemine girişte şifre kullandığı saptandı. Ayrıca hemşirelerin % 33.3'ünün diğer kliniklerdeki hastalara ait bilgilere kolaylıkla ulaşabildiği ve %39.1'inin ise hastalara ait olan bilgilerin paylaşımı için hastadan onam almadığı belirlendi. Bilgi Güvenliği Ölçeği'nden alınan toplam puan ortalaması (3.21±0.53), hemşirelerin bilgi güvenliği farkındalığının orta düzeyde olduğunu gösterdi. Ölçek alt boyutlarından en yüksek puan hizmet sunumu (3.50±0.85), en düşük puan ise güvenlik politikası alt boyutundan (2.93±0.85) alındı. Hemşirelerin yaş, cinsiyet, eğitim durumu ve çalışma şekli gibi tanıtıcı özellikleri ile Bilgi Güvenliği Ölçeği toplam ve alt boyut puan ortalamalarının karşılaştırılması sonucunda istatistiksel olarak anlamlı bir farkın olmadığı belirlendi (p>0.05). Hemşirelerin bilgi güvenliği farkındalığının orta düzeyde olması, veri güvenliğini tehdit etmekte ve sağlık hizmet kalitesini olumsuz etkilemektedir. Hemşirelerin bilgi güvenliği farkındalığını artırmak, kaliteli ve güvenli sağlık bakım hizmet sunumunu sağlamak için hizmet içi eğitimler düzenlenmelidir.

Anahtar kelimeler: Bilgi güvenliği, farkındalık, hasta güvenliği, hemşire, hemşirelik

ABSTRACT

This descriptive study was aimed to determine the level of information security awareness of nurses and was conducted with 294 nurses working in a training and research hospital in Ankara between June and August 2022. Descriptive Information Form and the Information Security Scale were used in data collection. Descriptive statistics, independent sample t-test, and one-way analysis of variance were used in data analysis. It was found that 47.3% of the nurses did not receive any training on information security, and 97.6% used passwords to access the hospital information system. In addition, it was determined that 33.3% of the nurses could easily access information about patients in other clinics, and 39.1% did not obtain consent from the patient for sharing information about patients. The ISS total mean score (3.21±0.53) showed that nurses' information security awareness was moderate. In the subdimensions, the highest score was from service delivery (3.50±0.85), and the lowest was from the security policy (2.93±0.85). It was determined that descriptive characteristics of nurses, such as age, gender, educational status, and manner of work, and the ISS total and subscale score averages, it was observed that there was no statistically significant difference (p>0.05). A moderate level of information security awareness of nurses threatens data security and affects health service quality negatively. To increase the information security awareness of nurses and ensure quality and safe health care service delivery, in-service training activities should be organized.

Keywords: Information security, awareness, patient safety, nurse, nursing.

*Bu çalışma 22-25 Eylül 2022 tarihinde Konya/ Türkiye gerçekleştirilen 7. Uluslararası 18. Ulusal Hemşirelik Kongresi'nde sözel bildiri olarak sunulmuştur.

Makale Geliş Tarihi : 13.07.2023
Makale Kabul Tarihi: 22.02.2024

Sorumlu Yazar: Palyatif Servisi Hemşiresi, Melek ÇAKIR, cakir.melek2396@gmail.com, 0000-0001-7756-7337, Sağlık Bilimleri Üniversitesi, Ankara Atatürk Sanatoryum Eğitim ve Araştırma Hastanesi, Kuşcağız, Sanatoryum Cad. No:271, Keçiören/Ankara

Yazarlar: Doç. Dr. Bilgen ÖZLÜK, bilgenozluk@gmail.com, 0000-0002-2560-4199

GİRİŞ

Sağlık hizmeti sunan kurumlar hastaların tıbbi ve kişisel bilgilerini toplayan, kullanan ve depolayan karmaşık organizasyonlardır.[1] Bu kurumlarda bilgi güvenliğinin sağlanması, kaliteli sağlık bakım hizmet sunumunun göstergelerinden biri olarak kabul edilmektedir.[2] Sağlık Bakanlığı (SB) Bilgi Güvenliği Farkındalık Bildirgesi'nde, hasta ya da çalışanlara ait kişisel ve klinik verilerin bütünlüğü bozulmadan güvenli şekilde kayıt edilmesi, depolanması ve doğru kişiye ulaştırılmasının önemi vurgulanmaktadır.[3] Hasta Hakları Yönetmeliği'nde yer alan "sağlık hizmetinin verilmesi sebebiyle edinilen bilgiler, kanun ile müsaade edilen haller dışında hiçbir şekilde açıklanamaz" ibaresi ile de hastanedeki bilgi güvenliği yasal güvence altına alınmıştır.[4]

Bilgi güvenliği yönetiminde amaç, bilgi güvenliği ihlaline yönelik olayların meydana gelmesini engellemek ve önleyici tedbirler almaktır.[5] Bilgi güvenliğinin gizlilik, bütünlük ve erişilebilirlik bileşenlerinden biri zarar görürse bilgi ihlali meydana gelmektedir. Gizlilik bileşeni; bilginin yetkisiz kişilerin eline geçmemesi ve erişiminin engellenmesi, bütünlük bileşeni; kurumun özel bilgilerinin yetkisiz kişi ya da kişiler tarafından değiştirilmeden bilginin doğru ve tam olarak işlenmesi, erişilebilirlik bileşeni ise, kişilerin yetkileri dahilinde bilgiye ulaşabilir ve kullanabilir durumda olmasını ifade etmektedir.[6] Bu üç temel bileşenin korunması ile bilgi güvenliğinin sağlanabilmesi mümkün olacaktır. Bilgi güvenliğinin sağlanmasındaki temel amaç ise bilgiyi korumak, kaliteli, kesintisiz ve güvenli bir hizmet sunumu sağlayarak oluşabilecek bilgi açığını önlemektir.[7] Kurumlarda bilgi güvenliğinin sağlanması için, bilginin izinsiz veya yetkisiz bir biçimde erişiminin, kullanımının, değiştirilmesinin ve ifşa edilmesinin önlenmesi gerekmektedir.[6] Yapılan çalışmalarda kurumun dijital alt yapısı ve sağlık çalışanlarının tıbbi yasalara ve yönetmeliklere göre gizlilik, bütünlük ve erişilebilirlik nitelikleri göz ardı edilmeden bilgi güvenliliğinin iyi planlanmasının gerekli olduğu vurgulanmaktadır.[6,8,9]

Bilgi güvenliğinin istendik düzeyde sağlanabilmesi için yasalara, kurallara ve donanımsal güvenlik konularına uyulması gerekmektedir. Yapılan bir çalışmada sağlık hizmetlerinde bilgi güvenliğinin donanımsal konulardan ve yasal politikalardan etkilendiği belirtmektedir.[10] Başka bir çalışmada ise, optimal hasta bakımı ve yönetimini sağlayarak sağlık hizmet sunumunu geliştirmek için sağlık hizmetleri bilgilerine ilişkin bilgi güvenliği stratejilerinin, kılavuzlarının ve politikalarının benimsenmesi önerilmektedir.[11] Bununla birlikte sağlık hizmeti sunan kurumlarda donanımsal olarak denetimler, kimlik doğrulama, yetkilendirme gibi son derece gelişmiş teknoloji korumalarına ve şifreleme gibi bilgi gizliliği önlemlerine rağmen, insan hatası nedeniyle güvenlik ihlalleri yaşanabilmektedir.[12] Bilgi güvenliği süreçlerinin işleyebilmesi için insan faktörünün de dikkate alınması, bilinçli ve yetkin kişilerin istihdam edilmesi gerekmektedir.[13] Kurumdaki sağlık profesyonellerinin bilgi güvenliği düzeyinin yeterli olması ve bu konudaki kurumsal politikaları ve stratejileri benimsemeleri gerektiği belirtilmektedir.[8] Bilgi güvenliği politikalarına uyumluluk anlayışını artırmada ve bilgi güvenliği politikasıyla kullanıcı uyumluluğunu geliştirmede yöneticilere büyük sorumluluk düşmektedir.[14] Ek olarak, sağlık kurumlarında bilgi güvenliğinin sağlanması ve bilgi güvenliği kültürünün kurum kültürüne dönüştürülmesinde yönetici desteği de önemlidir.[7,15]

Bilgi güvenliğinin doğru şekilde uygulanması için sağlık profesyonellerinde farkındalık oluşturmak önem taşımaktadır.[16] Bilgi güvenliği farkındalığının sağlanmasındaki amaç, sağlık çalışanlarının kurum içinde ve kurum dışında bilgi eksikliğinden kaynaklanabilecek güvenlik tehditlerine karşı önlem almasını sağlamaktır.[5] Yapılan çalışmalarda, bilgi güvenliği farkındalığının oluşması için, çalışanlara uygun ve yeterli eğitimin verilmesi gerektiği vurgulanmaktadır.[6,17] Günümüzde teknolojinin getirdiği riskler, hastanelerin büyük organizasyonlar olması, sağlık hizmetlerinin multidisipliner yapıda olup çok fazla bilgi girdi-çıktısının olması gibi hususlar bilgi güvenliğine yönelik farkındalığın önemini ortaya koymaktadır. Sağlık hizmeti alan bireylerle uzun süre etkileşimde olan hemşirelerin, bilgi güvenliği farkındalık düzeylerinin belirlenmesi, gereksinim analizi yapılabilmesi açısından önemlidir. Mevcut literatürde, hemşirelerde bilgi güvenliği farkındalık düzeyinin araştırıldığı sınırlı sayıda araştırmaya rastlanmıştır.[18,19] Bu çalışmanın amacı, Ankara'da bulunan bir eğitim ve araştırma hastanesinde görev yapan hemşirelerin bilgi güvenliği farkındalık düzeyini değerlendirmek ve literatüre katkı sağlamaktır. Elde edilen bulguların hemşirelerin bilgi güvenliği davranışlarını şekillendirmeye, sağlık bakım hizmetinin güvenirliğini ve kalitesini artırmaya katkı sağlama potansiyeli olacaktır.

Çalışmada aşağıdaki sorulara yanıt aranmıştır.

1. Hemşirelerin bilgi güvenliği farkındalık düzeyleri nasıldır?
2. Hemşirelerin tanıtıcı özellikleri ile Bilgi Güvenliği Ölçeği (BGÖ) puan ortalaması arasında istatistiksel olarak anlamlı bir fark var mıdır?

GEREÇ VE YÖNTEM

Araştırmanın Türü

Bu çalışma, tanımlayıcı tipte gerçekleştirildi.

Araştırmanın Yapıldığı Yer ve Özellikleri

Çalışma, Ankara ilinde yer alan bir eğitim ve araştırma hastanesinde Haziran-Ağustos 2022 tarihleri arasında gerçekleştirildi. Hastanede 896 hemşire çalışmakta olup 15 adet dahili birim, iki adet temel birim, 14 adet cerrahi birim, 10 adet tedavi ünitesi ve iki adet acil tıp kliniği mevcuttur. Kurumda hastaya ait veriler fiziki olarak hastanenin arşivinde ve bilgisayarlarda elektronik olarak saklanmakta ve depolanmaktadır.

Araştırmanın Evren ve Örneklemi

Bu çalışmanın evrenini, Ankara ilindeki bir eğitim ve araştırma hastanesinde çalışan tüm hemşireler oluşturdu (N=896). Örneklem büyüklüğü, %95 güven aralığı ve %5 hata payı ile t değeri 1.96 alınarak, prevelans değeri ise Aksu'nun (2014)[6] çalışmasındaki gibi 0.5 alınarak 270 olarak hesaplandı.

Çalışmaya katılımın gönüllülük esasına dayalı olması ve kayıplar olabileceği göz önüne alınarak örneklem sayısı %10 artırılarak 297 hemşireye ulaşılması hedeflendi. Araştırma kapsamına, araştırmanın yapıldığı kurumda en az altı ay çalışmış olan ve çalışmaya katılmayı kabul eden hemşireler dahil edildi. Araştırma sürecinde 302 hemşireye ulaşıldı. Tam olarak doldurulmamış olan üç soru formu ve istatistiksel analizde, veri dağılımında gözlenen yüksek veya düşük olan aykırı değer olarak belirlenen beş soru formu çalışmaya dahil edilmedi.

Araştırma 294 hemşireden elde edilen verilerle tamamlandı.

Veri Toplama Tekniği ve Araçları

Veriler "Tanıtıcı Özellikler Formu" ve "Bilgi Güvenliği Ölçeği" ile toplandı. Veri toplama aracı, hemşirelere çalışma hakkında bilgi verilerek araştırmacılardan biri tarafından elden dağıtıldı. Gündüz vardiyasında vardiya başladıktan sonra dağıtıldı, vardiya sonunda toplandı. Aynı şekilde gece vardiyasına gelen hemşirelere vardiya başlandıktan sonra dağıtıldı, sabaha karşı vardiya bitmeden önce toplandı. Gündüz ve gece vardiyasında dağıtılan tüm formlar boş da olsa aynı vardiya bitiminde geri alındı. Veriler aralıklı olarak aynı süreci izleyerek toplanmaya devam etti. Soru formunun doldurulma süresinin ortalama olarak 10 dakika olduğu gözlendi.

Tanıtıcı Özellikler Formu

Araştırmacılar tarafından ilgili literatür[1,6,20] incelenerek oluşturulan bu formda, hemşirelerin tanıtıcı özellikleri ve bilgi güvenliğine ait toplam 12 soru yer aldı.

Bilgi Güvenliği Ölçeği (BGÖ)

Upfold ve Sewry'nin (2005)[21] geliştirdiği BGÖ, Türkçe'ye Aksu (2014)[6] tarafından uyarlanmıştır. Ölçek beş alt boyuttan (erişim ve yetkilendirme, güvenlik uygulamaları, hizmet sunumu, örgütsel güvenlik ve güvenlik politikası) ve toplam 27 maddeden oluşmaktadır. Ölçeğin puanlama yöntemi, 5'li likert tipinde 1-kesinlikle katılmıyorum'dan 5-kesinlikle katılıyorum'a doğru derecelendirilmiştir. Ölçekte ters madde bulunmamaktadır. Katılımcıların ölçek maddelerine verdikleri puan toplamlarının, ölçekteki madde sayısına bölünmesiyle toplam ölçek ve alt boyut puan ortalamaları belirlenmektedir. Ölçek toplamından ve altboyutlarından alınan puan ortalaması "5" puana yaklaştıkça bilgi güvenliği farkındalığının arttığı, "1" puana yaklaştıkça bilgi güvenliği farkındalığının azaldığı şeklinde değerlendirilmektedir. Türkçe versiyonunda Cronbach alfa katsayısı 0.81-0.90 olarak bildirilmiştir.[6] Bu çalışmada ise ölçeğin toplam Cronbach alfa katsayısı 0.89, alt boyutlarının ise 0.71-0.87 aralığında hesaplandı.

Araştırmanın Etik Boyutu

Araştırmanın yürütülebilmesi için Etik Kuruldan (Karar No: 2022/220) ve araştırmanın yapıldığı kurumdan yazılı izin alındı. Hemşireler araştırmanın amacı ve katılımın gönüllü olduğu doğrultusunda bilgilendirildi, katılım için sözel izinleri alındı.

Veri Analizi

Araştırma verileri SSPS 29.0 paket programı ile değerlendirildi. Hemşirelerin tanıtıcı özellikleri ve bilgi güvenliğine yönelik soruların değerlendirilmesinde frekans ve yüzde, ölçeğin ortalama puanının değerlendirilmesinde ise ortalama ve standart sapma değerleri kullanıldı. Verilerin normal dağılıma uygunluğu Kolmogorov-Smirnov testi ve Skewness ve Kurtosis değerleri ile belirlendi. Hemşirelerin tanıtıcı özellikleri ile ölçeğin toplam ve alt boyut puan ortalamasının karşılaştırılmasında ise bağımsız örneklem t testi ve tek yönlü varyans analizi (ANOVA) kullanıldı.

BULGULAR

Hemşirelerin yaş ortalaması 30.97±7.06 yıl olup, % 55.8'i 29 yaş ve altındaydı ve %73.5'i kadındı. Eğitim durumuna göre %71.1'i lisans mezunuydu. Hemşirelerin %33'ü yoğun bakımda ve %83.3'ü vardiyalı olarak çalışıyordu. Hemşirelerin meslekte çalışma yıl ortalamaları 8.43±7.41 yıl ve bulundukları kurumda çalışma yıl ortalamaları ise 6.12±5.38 yıl olarak belirlendi (Tablo 1).

Hemşirelerin %52.7'sinin kurumda bilgi güvenliğine yönelik eğitim aldığı saptandı. Hemşirelerin %96.6'sı hastanenin bilgi sistemine girişte kullanıcı adı, %97.6'sı şifre, %2'si ise akıllı kart kullandığını belirtti. Araştırmada, hemşirelerin tamamı çalıştıkları klinikteki hastaların bilgilerine erişirken, %33.3'ü ise diğer kliniklerdeki hastaların bilgilerine de kolayca erişebildiğini ifade etti. Hemşirelerin hastanede kolaylıkla ulaşabildikleri diğer bilgilerin sırasıyla; kurum prosedürleri (%50), çalışan-

Tablo 1. Hemşirelerin Tanıtıcı Özellikleri (n=294)

Özellikler	n	%
Yaş		
29 ve altı	164	55.8
30 ve üzeri	130	44.2
Cinsiyet		
Kadın	216	73.5
Erkek	78	26.5
Eğitim durumu		
Sağlık Meslek Lisesi-Önlisans	67	22.8
Lisans	209	71.1
Lisansüstü	18	6.1
Çalışılan Birim		
Dahili Servis	92	31.3
Cerrahi Servis	56	19.0
Yoğun Bakım	97	33.0
Acil Servis	49	16.7
Çalışma Şekli		
Gündüz	49	16.7
Vardiyalı	245	83.3
	Ort±SS	**Min-Maks**
Yaş	30.97±7.06	21- 52
Meslekte Çalışma Yılı	8.43±7.41	0.7- 28
Kurumda Çalışma Yılı	6.12±5.38	0.7- 24

lara ait bilgiler (%19), sosyal güvence bilgileri (%18.4), yönetimsel raporlar (%8.2) ve hastaneye ait mali bilgiler (%5.4) olduğu görüldü. Hastaya ait bilgilerin üçüncü kişilerle paylaşımında, hemşirelerin %60.9'u hastadan yazılı onam formu aldığını belirtti. Hemşirelerin bilgi güvenliğinin artırılmasına yönelik önerilerinin sırasıyla; şifre kullanımı (%95.9) ve şifrenin kesinlikle başkalarıyla paylaşılmaması (%85), şifre kalitesinin uygun seçimi (%80.3), anti-virüs programının kullanımı (%73.1), yazılım ve donanımın ihtiyaca göre güncellenmesi (% 73.1), klinik bilgisayarların yetkili kişiler dışında kullanmasına izin verilmemesi (%58.2), çalışanın birimden ayrılırken bilgisayarda kendi oturumunu kapatması (% 58.2) ve bilgisayarda kişisel USB'lerin kullanımına izin verilmemesi (%39.1) olduğu görüldü (Tablo 2).

Hemşirelerin BGÖ toplam puan ortalamasının 3.21±0.53, Hizmet Sunumu alt boyutu puan ortalamasının 3.50±0.85, Erişim ve Yetkilendirme alt boyutu puan ortalamasının 3.38±0.63, Güvenlik Uygulamaları alt boyutu puan ortalamasının 3.08±0.73, Örgütsel Güvenlik alt boyutu puan ortalamasının 3.04±0.78 ve Güvenlik Politikası alt boyutu puan ortalamasının ise 2.93±0.85 olduğu belirlendi (Tablo 3).

Hemşirelerin tanıtıcı özellikleri ile BGÖ toplam ve alt boyut puan ortalamalarının karşılaştırılması sonucunda istatistiksel olarak anlamlı bir farkın olmadığı saptandı (p>0.05) (Tablo 4).

TARTIŞMA

Bir eğitim ve araştırma hastanesinde çalışan hemşirelerin bilgi güvenliğine yönelik farkındalık düzeyinin değerlendirildiği bu çalışmada, hemşirelerin %52.7'sinin bilgi güvenliği eğitimi aldığı belirlendi. Bu sonuç hemşirelerin yarıya yakınının bilgi güvenliği eğitimi almadığını göstermekte ve bilgi güvenliği açısından bu durumun bir tehdit oluşturduğunu düşündürmektedir. Bu çalışma sonucuna benzer şekilde Kurt (2019)[22], Hastane Yönetim Bilgi Sistemlerini (HBYS) kullanan klinik ve idari

Tablo 2. Hemşirelerin Bilgi Güvenliğine Yönelik Sorulara Verdiği Cevaplar

	Evet		Hayır	
Bilgi Güvenliğine Yönelik Sorular	**n**	**%**	**n**	**%**
Kurumunuzda bilgi güvenliğine yönelik herhangi bir eğitim aldınız mı?	155	52.7	139	47.3
***Hastane bilgi sistemine girişte hangi yöntemi kullanıyorsunuz?**				
Kullanıcı adı	284	96.6	10	3.4
Şifre	287	97.6	7	2.4
Akıllı kart	6	2.0	288	98.0
Parmak izi	0	0	294	100
***Hastanenizdeki hangi tür bilgilere ulaşımız kolaydır?**				
Kendi kliniğimdeki hastaya ait bilgiler	294	100	0	0
Diğer kliniklerdeki hastalara ait bilgiler	98	33.3	196	66.7
Kurum prosedürleri	147	50.0	147	50.0
Çalışanlara ait bilgiler	56	19.0	238	81.0
Sosyal güvence bilgileri	54	18.4	240	81.6
Yönetimsel raporlar	24	8.2	270	91.8
Hastaneye ait mali bilgiler	16	5.4	278	94.6
Hastanın kimlik ve tıbbi bilgilerinin paylaşımında hastadan onam alıyor musunuz?	179	60.9	115	39.1
***Hasta güvenliğinin artırılması için hangi önlemlerin alınmasını önerirsiniz?**				
Şifre kullanımı	282	95.9	12	4.4
Şifrenin kesinlikle başkalarıyla paylaşılmaması	250	85.0	44	15.0
Şifre kalitesinin uygun seçilmesi	236	80.3	58	19.7
Anti-virüs programlarının kullanımı	215	73.1	79	26.9
Yazılım ve donanımın ihtiyaca göre güncellenmesi	215	73.1	79	26.9
Klinik bilgisayarların yetkili kişiler dışında kullanmasına izin verilmemesi	171	58.2	123	41.8
Çalışanın birimden ayrılırken bilgisayarda kendi oturumunu kapatması	171	58.2	123	41.8
Bilgisayarda kişisel USB'lerin kullanımına izin verilmemesi	115	39.1	179	60.9

*Birden fazla seçenek işaretlenmiştir.

Tablo 3. BGÖ Puan Ortalamalarının Dağılımı

Alt Boyutlar	Ort±SS	Min	Maks
Hizmet Sunumu	3.50±0.85	1.00	5.00
Erişim ve Yetkilendirme	3.38±0.63	1.44	4.89
Güvenlik Uygulamaları	3.08±0.73	1.00	5.00
Örgütsel Güvenlik	3.04±0.78	1.00	5.00
Güvenlik Politikası	2.93±0.85	1.00	5.00
BGÖ Toplam Ortalama Puanı	3.21±0.53	1.70	4.52

*BGÖ: Bilgi Güvenliği Ölçeği, **Ort: Ortalama, ***SS: Standart sapma

Tablo 4. Hemşirelerin Özellikleri ile BGÖ Puan Ortalamalarının Karşılaştırılması

Özellikler	Erişim ve Yetkilendirme Ort±SS	Güvenlik Uygulamaları Ort±SS	Hizmet Sunumu Ort±SS	Örgütsel Güvenlik Ort±SS	Güvenlik Politikası Ort±SS	Bilgi Güvenliği Ölçeği Toplam Ort±SS
Yaş						
29 ve altı	3.35±0.65	3.14±0.71	3.42± 0.84	3.12 ±0.77	2.98±0.87	3.23±0.56
30 ve üzeri	3.41±0.59	3.01±0.75	3.60± 0.86	2.94 ±0.79	2.85±0.82	3.19±0.49
t	-0.709	1.481	-1.810	1.907	1.329	0.499
p	0.479	0.140	0.071	0.057	0.185	0.618
Cinsiyet						
Kadın	3.35±0.62	3.10±0.72	3.46 ±0.85	3.08± 0.76	2.96±0.84	3.21±0.54
Erkek	3.46±0.65	3.05±0.77	3.62±0.86	2.94± 0.84	2.82±0.87	3.22±.0.49
t	-1.396	0.502	-1.411	1.324	1.283	-0.093
p	0.164	0.616	0.159	0.187	0.201	0.926
Eğitim durumu						
Sağlık Meslek Lisesi-Önlisans	3.41±0.68	2.98±0.74	3.57±0.88	2.99±0.811	2.94±0.77	3.21±0.51
Lisans	3.36±0.61	3.12±0.73	3.47±0.85	3.05±0.78	2.92±0.88	3.21±0.54
Lisansüstü	3.46±0.62	3.10±0.76	3.61±0.80	3.14± 0.68	2.94±0.79	3.28±0.51
t	0.363	0.883	0.471	0.302	0.023	0.141
p	0.696	0.414	0.625	0.740	0.977	0.869
Çalışılan Birim						
Dahili Servis	3.34±0.68	2.95±0.73	3.44±0.83	2.98±0.77	2.89± 0.84	3.15±0.53
Cerrahi Servis	3.53±0.55	3.08±0.78	3.65±0.91	3.07±0.83	2.98± 0.83	3.30±0.49
Yoğun Bakım	3.27±0.64	3.10±0.71	3.39±0.87	3.00±0.75	2.89±0.83	3.15±0.56
Acil Servis	3.47±0.55	3.31±0.69	3.66±0.78	3.22±0.78	3.00±0.95	3.35±0.49
F	2.529	2.575	1.832	1.161	0.292	2.508
p	0.057	0.054	0.141	0.325	0.831	0.059
Çalışma Şekli						
Gündüz	3.34±0.59	3.03±0.77	3.47±0.76	2.98±0.77	2.90±0.81	3.17±0.48
Vardiyalı	3.38±0.64	3.10±0.73	3.50±0.87	3.05±0.78	2.93±0.86	3.22±0.54
t	-0.449	-0.594	-0.220	-0.577	-0.243	-0.596
p	0.654	0.553	0.826	0.564	0.808	0.552

*BGÖ: Bilgi Güvenliği Ölçeği, **Ort: Ortalama, ***SS: Standart sapma

birim çalışanlarının (hemşire, doktor, tıbbi sekreter ve idari birimde masa başı personel) %57.8'inin bilgi güvenliği eğitimi aldığını bulmuştur. Karadağ ve Abuhanoğlu (2015)[23] çalışmasında, sağlık çalışanlarının (hemşire, doktor, teknisyen, diş hekimi, idari personel) %96.5'i bilgi güvenliği riskleri konusunda bilinçlendirilmeleri gerektiğini ifade etmiştir. Bilgi güvenliği farkındalığının sağlanması için çalışanlarda güvenlik bilincinin oluşturulması ve bilgi güvenliğine yönelik tehditlere karşı nasıl korunması gerektiği konusunda bilinçlendirme yapılması gerekmektedir.[24] Ayrıca bu sürecin kurum içinde hiyerarşinin tüm basamaklarında uygulanması ve kurumların tüm çalışanlarına eğitim verilmesi önerilmektedir.[25] Bilgi güvenliği farkındalık eğitimi, bilgilerin nasıl ve ne şekilde korunması gerektiği konusunda çalışanlarda güvenlik bilinci oluşturması açısından önem taşımaktadır.[16]

Bu çalışmada hemşirelerin neredeyse tamamına yakını, bilgi güvenliğinin sağlanması için kurumlarında kendi bilgi sistemlerine kullanıcı adları ve şifreleri ile giriş yaptığını belirtmiştir. Taçar (2022)[18] hemşirelerle yaptığı çalışmada çalışmamıza benzer şekilde, hemşirelerin neredeyse tamamına yakını bilgi sistemine girişte kullanıcı adı (%96.2) ve şifre (95.9) ile giriş yaptığı görülmüştür. Dijital veya dijital olmayan ortamlarda verilerin bütünlüğünün korunması ve izinsiz erişimlerin engellemesi amacıyla sisteme girişte uygun kimlik belirleme yöntemleri kullanılmalıdır. Karadağ ve Abuhanoğlu'nun (2015)[23] yaptığı çalışmada sağlık çalışanlarının (hemşire, doktor, teknisyen, diş hekimi, idari personel) %96.9'u bilgilerin kaybolma ve hasar görme riskine yönelik koruma altına alınması gerektiğini belirtmiştir. Kurumlarda kimlik belirleme yöntemi olarak kullanılan kullanıcı adı ve şifrelerin telefon, e-posta gibi iletişim araçlarıyla kolaylıkla paylaşılıyor olma ihtimaline karşı parmak izi sisteminin hastanelere entegre edilmesi, bilgi gizliliğini sağlayabilme düzeyini artıracaktır.

Bu araştırmada hemşirelerin üçte biri hastanın rızası alınmadan hastaya ait bilgilerin paylaşıldığını ifade etmiştir. Bu sonuç hastanın mahremiyet ve gizlilik hakkının ihlal edilebileceğini düşündürmektedir. İspanya'da

bir hastanede doğrudan gözlem yoluyla yapılmış olan bir çalışmada, bilgi gizliliğinin ihlal edildiği durumlar araştırılmış, gözlemlenen ihlallerin %54.6'sının hastanın tıbbi tedavisinde yer almayan sağlık personeline bilgi paylaşımı ile gerçekleştiği belirtilmiştir.[26] Sağlık hizmeti sunumunda hastaya uygulanan tüm işlemlerin kayıt altına alınması gerekmektedir.[25] Kayıt altına alınan bilgilerin gizliliği göz ardı edilmeden, kurum içi ve kurumlar arası paylaşımlarda hastalardan bilgilendirilmiş rıza alınması gerekmektedir. Hastanın rızası alınmadan hastaya ait bilgilerin, gizlilik ve mahremiyet göz ardı edilerek hasta dışında sigorta şirketleri, medikal firmalar, ilaç şirketleri, sosyal medya paylaşımları veya bilimsel araştırmalarda kullanılmak üzere üçüncü kişilerle paylaşılma ihtimali bilgi güvenliği açısından dikkat edilmesi gereken bir hususdur.[27] Hastadan rıza alınmadan yapılan her türlü bilgi paylaşımı hukuki sorunları da beraberinde getirmektedir. Hasta ve çalışan güvenliği açısından hemşireler, hastalara ait bilgilerin paylaşımında hastanın rızasının alınmış olmasını kontrol etmelidir.

Bu araştırmadan elde edilen sonuçta hemşirelerin bilgi güvenliğine yönelik farkındalıklarının orta düzeyde olduğu belirlendi. Bu sonuç verilerin erişim, gizlilik ve bütünlüğünün istendik düzeyde sağlanamadığını göstermektedir. Hastanelerdeki bilgi yönetim sistemlerinde yer alan verilere erişebilmeleri ve bu verileri düzenleyebilmeleri nedeniyle hemşireler bilgi güvenliğinden sorumlu sağlık çalışanları arasında yer almaktadır. Çelikçöp ve Yarar'ın (2020)[28] yaptığı çalışmada hastanede çalışan kalite yönetim direktörleri ve kalite birim sorumlularının bilgi güvenliği farkındalıklarının orta düzeyde olduğu, bilgi güvenliği bilincine yeteri kadar sahip olmayan çalışanların bilgi güvenliğine yönelik tehdit unsuru oluşturabileceği raporlanmıştır. Hemşireler, sağlık kurumlarında farklı meslek üyeleriyle eşgüdüm halinde çalışmaktadır.[29] Bu nedenle hemşirelerin bilgi güvenliğinin sağlanmasına yönelik farkındalıkları hem kendi meslektaşlarına, hem de birlikte çalıştığı diğer meslek üyelerine rol model olması açısından önem arz etmektedir. Bilgi güvenliği endişelerini gidermek ve yüksek kaliteli sağlık hizmetleri sunmak için hemşirelerin bilgi güvenliğine yönelik farkındalıklarının tam olarak sağlanması yöneticilerin sorumlulukları arasında yer almaktadır.[30]

Bu çalışmada hemşirelerin BGÖ "hizmet sunumu" alt boyut düzeyinin ortalamanın üzerinde ve en yüksek puanı aldığı görüldü. Bu sonuç ölçek alt boyut maddeleri doğrultusunda, fazla iş yükünün bilgi güvenliği ihlaline neden olmadığını göstermektedir. Ayrıca kurumun bilgi güvenliğine yönelik uyguladığı süreçlerin sağlık hizmet kalitesini olumsuz etkilemediği, sağlık hizmet sunumundaki değişikliklerin de bilgi güvenliğine verilen önemi etkilemediğini düşündürmektedir. Yapılan çalışmalarda bu çalışmaya benzer şekilde "hizmet sunumu" alt boyutunun iyi düzeyde olduğu belirtilmektedir.[6,22]Taçar (2022)[18] hemşirelerle yaptığı çalışmada, hizmet sunumu alt boyut düzeyinin yüksek olmasını, hastalara sunulan hizmet kalitesinin bilgi güvenliği süreçlerinden etkilenmediği şeklinde yorumlamaktadır. Sağlık hizmeti sunumunda çalışanların hastaya ait verileri doğru şekilde sisteme aktarması, iletmesi ve yetkili kişilerin erişebilmesi kurumun bilgi güvenliği standartları için oldukça önemlidir.[22]

Araştırma sonucumuzda BGÖ "erişim ve yetkilendirme" alt boyut puanının orta düzeyin biraz üzerinde olduğu görülmüştür. Hemşirelerin hastanedeki hangi tür bilgilere kolaylıkla ulaşabiliyorsunuz?" sorusuna verdiği cevaplar arasında üçte birinin diğer klinikteki hastalara ait bilgilere kolaylıkla ulaştıklarını belirtmeleri bu sonucu destekler niteliktedir. Bu sonuçlar hastane yönetiminin sağlık çalışanlarını, bilgiye erişiminde yetkilendirmesine yönelik bir standardının ve kurum politikasının net olmadığını düşündürmektedir. Bilgiye erişim konusunda çalışanlara yetki tanımının yapılmaması, bilgi güvenliği açısından ciddi bir tehdit unsuru oluşturmaktadır.[5] Kurumlarda hasta ya da çalışan verilerine erişimin nasıl olacağı doğru tanımlanmalıdır. Hollanda'da hastanelerdeki bilgi güvenliği memurlarıyla yapılan bir çalışmada, çalışanların kendi çalışma koşulları ve yükümlülüklerini dikkate alarak, kurum içerisinde hangi bilgiye erişmesi gerektiği hakkında yeterli bilgiye sahip olması gerektiği vurgulanmaktadır.[31] Kurumda kimlerin hangi verilere erişim sağlayacağı ve bu erişimin hangi seviyede olacağı, kurumun yetkilendirme prosedürü göz önüne alınarak düzenlenmesi sağlık hizmet sunumu açısından önem taşımaktadır.[5,6]

Çalışmamızda BGÖ "güvenlik uygulamaları" alt boyutunda hemşirelerin orta düzeyde farkındalıklarının olduğu görülmüştür. Hemşirelere sorulan sorularda da bilgi güvenliğinin artırılmasına yönelik önerilerinin bulunması bilgi güvenliği uygulamaların kısmen de olsa farkında olduklarını göstermektedir. Bilgi güvenliğinin sağlanmasında güvenlik uygulamalarının önemi büyüktür. Bilgi güvenliğini tehdit eden unsur oluştuğunda çalışanların yapması gerekenleri ve yardım için kimin aranacağını bilmesi oluşabilecek riskler karşında kuruma fayda sağlayacaktır. Ayrıca yazılım ve donanımın ve anti-virüs programlarının belirli periyotlarda güncellenmesi, şifre yönetim sisteminin belirli kurallar doğrultusunda oluşturulması ve bilgi erişimi açısından yetkilendirme prosedürünün kullanılması kurumlarda bilgi güvenliğinin gizlilik, bütünlük ve erişilebilirlik ilkelerini temel alarak sürekliliği sağlayacaktır.[23]

Araştırmamızın BGÖ "örgütsel güvenlik" alt boyutunda hemşirelerin orta düzeyde farkındalıkları olduğu belirlendi. Bu sonuç, çalışmanın yapıldığı hastanede örgütsel güvenlik kültürünün yeteri kadar oluşmadığını düşündürmektedir. Hemşirelerin yarısının bilgi güvenliği eğitimi almaması, hemşirelerin üçte birinden fazlasının bilgi paylaşımı için hastadan onam almaması, bilgiye erişim ve yetkilendirmede düzenlemeler yapılmaması yönetsel anlamda örgütsel güvenlikle ilgili eksiklikleri göstermektedir. Kurt (2019)[22] HBYS kullanan tıbbi ve idari personeller (hekim, hemşire, tıbbi sekreter gibi) ile yaptığı çalışmada, bu çalışmayla paralel olarak örgütsel güvenlik alt boyutunun orta düzeyde olduğu görülmektedir. Sağlık hizmeti veren kurumlarda bilgi güvenliğinin sağlanması, örgütlerin kurumsal anlamda bilgi güvenliği ve çalışanların bilgi güvenliği farkındalık düzeyinin yüksek olmasıyla mümkündür.[16] Hastanedeki bilgi gizliliğinin sürdürebilmesi için denetleyici uzman kişi ve ekiplerin olması, bilgi güvenliği ihlali durumunda çalışanlara disiplin uygulamalarının bildirilmesi, çalışanların kurumdan uzaklaştığında bilgisayarlarını daima güvenli şekilde bırakması örgütsel güvenlik kültürünün oluşmasına yardımcı olmaktadır.[8]

Araştırmamızdan elde edilen sonuca göre BGÖ "güvenlik politikası" alt boyutunun orta düzeyin altında

ve hemşirelerin en düşük farkındalık düzeyine sahip alt boyut olduğu bulundu. Bu sonuç yöneticiler ve çalışanların bilgi güvenliğine dair politika ve uygulamalarda yeteri kadar gerekli özeni ve sorumluluğu gösterdiğini düşündürmektedir. Karadağ ve Abuhanoğlu (2015)[23] sağlık çalışanlarıyla (hemşire, doktor, teknisyen, diş hekimi, idari personel) yaptığı çalışmada, katılımcıların %93.7'si bilgi güvenliğinin sağlanması konusunda kurumun üst yöneticilerinden başlayarak tüm çalışanların sorumluluk sahibi olması gerektiğini belirtmiştir. Taçar (2022)[18] ise hemşirelerle yaptığı çalışmada güvenlik politikası alt boyutundan düşük puan alınmasını bilgi güvenliğine ilişkin eğitimler, politikalar ve çalışanların sorumluluklarına dair yeterlilik ve memnuniyetin düşük olması ile ilişkilendirmiştir. Güvenlik politikaları, yönetim tarafından desteklenen ve iyi yönetilebilen, anlaşılabilir, uygulanabilir olmalıdır.[32] Ayrıca bilgilerin saklanması, korunması ve taşınması sırasında gerekli önlemlerinin alınması için, kurumlar yasa ve yönetmeliği göz önüne alarak kendilerine uygun güvenlik politikası oluşturması gerekmektedir.[33,34]

SONUÇ

Bir kamu hastanesinde çalışan hemşirelerin bilgi güvenliği farkındalık düzeyini değerlendirmek amacıyla yapılan bu çalışma sonucunda hemşirelerin, bilgi güvenliği farkındalığının orta düzeyde olduğu bulundu. Bu sonuçlar doğrultusunda, hemşirelere bilgi güvenliğinin kalıcı şekilde benimsetilmesine yardımcı olmak için uygulamalı eğitimler düzenlenmesi, eğitim öncesi ve sonrası bilgi düzeylerini ölçen deneysel tasarımda araştırmalar yapılması, bilgi güvenliğinin sürdürülebilir olması için kurumun oluşturduğu bilgi güvenliği prosedürleri ve politikaların net olması ve denetlemesi önerilmektedir.
Bu çalışma sadece bir eğitim ve araştırma hastanesinde çalışan hemşirelerde yapıldığı için sonuçların tüm hemşirelere genellenebilirliği araştırmanın sınırlılığını oluşturmaktadır. Araştırmanın verileri yapıldığı zaman kapsamında geçerlidir, zamana bağlı değişiklik gösterebilmektedir.

Etik Komite Onayı: Araştırmanın yürütülebilmesi için Etik Kuruldan (Karar No: 2022/220) ve araştırmanın yapıldığı kurumdan yazılı izin alındı.
Bilgilendirilmiş Onam: Araştırmaya katılmayı gönüllü olarak kabul edenlerden sözel onam alınmıştır.
Hakem Değerlendirmesi: Dış bağımsız.
Yazar Katkıları: Fikir- BÖ, MÇ; Tasarım- BÖ, MÇ; Denetleme- BÖ, MÇ; Kaynaklar- BÖ, MÇ ; Malzemeler- ; Veri Toplanması ve/veya işlenmesi- MÇ, BÖ; Analiz ve/veya yorum- BÖ, MÇ; Literatür taraması- MÇ, BÖ; Yazıyı yazan- MÇ, BÖ ;Eleştirel inceleme- BÖ
Çıkar Çatışması: Yazarlar herhangi bir çıkar çatışmasının olmadığını beyan ederler.
Finansal Destek: Bu araştırma için herhangi bir kurumdan finansal destek alınmamıştır.
Teşekkür: Çalışmaya katılan tüm hemşirelere teşekkür ederiz.

Ethics Committe Approval: In order to conduct the research, written permission was obtained from the Ethics Committee (Decision No: 2022/220) and the institution where the research was conducted.
Informed Consent: Verbal consent was obtained from those who voluntarily agreed to participate in the research.
Peer-review: Externally peer-reviewed.
Author Contributions: Concept: BÖ, MÇ; Design: BÖ, MÇ; Supervision: BÖ, MÇ: Resources: BÖ, MÇ; Materails: -; Data Collection and/ Processing: MÇ, BÖ; Analysis and/or Interpretation: BÖ, MÇ; Literature Search: MÇ, BÖ; Writing Manuscript: MÇ, BÖ; Critical Review: BÖ.
Declaration of Interest: The authors declare that they have no conflict of interest.
Funding: No financial support was received from any institution for this research.
Acknowledgements: We thank all the nurses who participated in the research.

KAYNAKLAR

1. Chen R, Hsiao J. An investigation on physicians' acceptance of hospital information systems: a casestudy. *Int J Med Inform.* 2012;8(12):810-820. doi:10.1016/j.ijmedinf.2012.05.003.
2. Rockwern B, Johnson D, Snyder Sulmasy L. Health information privacy, protection, and use in the expanding digital health ecosystem: A position paper of the American College of Physicians. *Annals of Internal Medicine.* 2021;174(7):994-998. doi:10.7326/M20-7639.
3. T.C. Sağlık Bakanlığı. Bilgi Güvenliği Farkındalık Bildirgesi. https://dosyaism.saglik.gov.tr/Eklenti/60617/0/bgsz03-bilgi-guvenligi-farkindalik-bilpdf.pdf. 2020. Erişim Tarihi: Şubat 6, 2023.
4. T.C. Sağlık Bakanlığı. Sağlık Bakanlığı Hasta Hakları Yönetmeliği. https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=4847&MevzuatTur=7&MevzuatTertip=5. 2019. Erişim tarihi: Şubat 7, 2023.
5. İleri YY. Örgütlerde bilgi güvenliği yönetimi, kurumsal entegrasyon süreci ve örnek bir uygulama. *Anadolu Üniversitesi Sosyal Bilimler Dergisi.* 2016;17(4):55-72. doi:10.18037/ausbd.417372.
6. Aksu PK. Hastane Bilgi Yönetim Sisteminin Bilgi Güvenliği Açısından Değerlendirilmesi. [yüksek lisans tezi] İstanbul, Türkiye: Marmara Üniversitesi Sağlık Bilimleri Enstitüsü; 2014.
7. Safa NS, Solms VR, Furnell S. Information security policy compliance model in organizations. *Comput Secur.* 2016;56:70-82. doi:10.1016/j.cose.2015.10.006.
8. Baran S, Şener E. Hastanelerde bilgi güvenliği yönetimi: nitel bir araştırma. *SDÜ Vizyoner Derg.* 2018;10(23):108-125. doi:10.21076/vizyoner.444451.
9. Oguz M. Kişiselleştirilmiş mobil sağlık uygulamaları bilgi güvenlik gereksinimleri. *Sağlık Akademisyenleri Dergisi.* 2017;4(2):110-114. doi:10.5455/sad.13-1493676116.
10. Smaradottir BF. Security management in health care information systems a literature review. Paper presented at the Interantional Conference Computational Science and Computational Intelligence; December 12-14, 2017, Las Vegas, USA doi:10.1109/CSCI.2017.303.
11. Rençber ÖF, Mete S. Bilgi güvenlik farkındalığını etkileyen faktörlerin belirlenmesi: Yüksekokul öğrencileri üzerine bir inceleme. *İktisadi ve İdari Bi-*

limler Fakültesi Dergisi. 2017;8(3):800-823.
12. Kamerer JL, Mc Dermott D. Cybersecurity: Nurses on the front line of prevention and education. *Journal of Nursing Regulation.* 2020;10(4):48–53. doi:10.1016/S2155-8256(20)30014-4.
13. Kessler SR, Pindek S, Kleinman G, Andel SA, Spector PE. Information security climate and the assessment of information security risk among health careemployees. *Health Informatics J.* 2020;26 (1):461-473. doi:10.1177/1460458219832048.
14. Humaidi N, Balakrishnan V. Indirect effect of management support on users' compliance behaviour to wards information security policies. *Health Information Management J*. 2018;47(1):17-27. doi:10.1177/1833358317700255.
15. Yıldız Z, Yurttaş H, Ozan, B. Bilgi güvenliği kapsamında yer alan rol gruplarının değerlendirilmesi. *Journal of 5N1 Quality.* 2023;1(1):19–28. doi:10.5281/zenodo.7761218.
16. İleri YY. Kurumsal bilgi kaynaklarına erişimde güvenlik: hekimlerin şifre yönetimine yönelik bir araştırma. *Uluslararası Sağlık Yönetimi ve Stratejileri Araştırma Dergisi.* 2018;4(1):15-25.
17. Henkoğlu T. Kişisel verileriniz ne kadar güvende? Bilgi güvenliği kapsamında bir değerlendirme. *Arşiv Dünyası Dergisi*. 2017;17-18.
18. Taçar E. Elektronik Sağlık Kayıtları Kullanımında Hemşirelerin Bilgi Güvenliği Farkındalık Düzeylerinin Belirlenmesi. [yüksek lisans tezi] Ankara, Türkiye: Ankara Yıldırım Beyazıt Üniversitesi Sağlık Bilimleri Enstitüsü; 2022.
19. Turaç İS. Hemşirelerin Kanıta Dayalı Hemşireliğe Yönelik Tutumları ve Bilgi Güvenliğinin Hasta Güvenliği Kültürü Üzerine Etkisi. [yüksek lisans tezi] Ankara, Türkiye: Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü; 2022.
20. Moğol HŞ. Bilgi Güvenliği Farkındalığının Önemi. [yüksek lisans tezi]. Ankara, Türkiye: Yıldırım Beyazıt Üniversitesi Fen Bilimleri Entitüsü; 2016.
21. Upfold CT, Sewry DA. An Investigation of Information Security in Small and Medium Enterprises (SME's) in the Eastern Cape. [PhD thesis]. South Africa: Rhodes University; 2005.
22. Kurt HÖ. Kurumlarda Bilgi Güvenliği Yönetimi: Hastane Bilgi Sistemleri Üzerine Bir Araştırma. [yüksek lisans tezi]. Konya, Türkiye: Necmettin Erbakan Üniversitesi Sağlık bilimleri Enstitüsü; 2019.
23. Karadağ M, Abuhanoğlu H. Sosyo-kültürel özelliklerin bilgi güvenliği farkındalığı üzerine etkisi: Gülhane askeri tıp fakültesi eğitim hastanesinde bir çalışma. *The Journal of Academic Social Science Studies.* 2015;36:379-386. doi:10.9761/JASSS2884.
24. T.C. Sağlık Bakanlığı. Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu. https://bilgiguvenligi.saglik.gov.tr/files/Bilgi%20G%C3%BCvenli%C4%9Fi%20Politikalar%C4%B1%20K%C4%B1lavuzu%20(S%C3%BCr%C3%BCm%202.1).pdf. 2019. Erişim Tarihi: Şubat 7, 2023.
25. Yıldırım BF. Sağlığın kişiselleşmesi ve kişisel sağlık bilgi sistemleri. *Bilgi Yönetimi.* 2019;2(2):127-135. doi:10.33721/by.642698.
26. Beltran-Aroca CM, Girela-Lopez E, Collazo-Chao E, Montero-Pérez-Barquero M, Muñoz-Villanueva MC. Confidentiality breaches in clinical practice: what happens in hospitals? *BMC Med Ethics*. 2016;17 (1):52. doi:10.1186/s12910-016-0136-y.
27. Dokholyan RS, Muhlbaier LH, Falletta JM, et al. Regulatory and ethical considirations for linking clinical and administirative data bases. *Am Heart J.* 2009;157(6):971-982. doi:10.1016/j.ahj.2009.03.023.
28. Çelikçöp Ç, Yarar O. Kalite yönetim direktörlerinin bilgi güvenliği farkındalığı: İstanbul ili örneği. *Sağlıkta Performans ve Kalite Dergisi*. 2020:17(2);29-48.
29. Yorgancılar FE, Özlük B. (2022). Hemşirelik hizmetlerinde yönetsel sorun çözme ve karar verme üzerine bir derleme. *Genel Sağlık Bilimleri Dergisi.* 2022;4(1):68-80. doi:0.51123/jgehes.2022.45.
30. Kim L. Cybercrime, ransom ware, and the role of the informatics nurse. *Nursing Management.* 2020;50(3):63-65. doi:10.1097/01.NURSE.0000654064.67531.c5.
31. Wirken G. Information Security in Dutch Hospitals. [master thesis]. Utrecht, Holland: Utrecht University Content and Knowledge Engineering Faculty of Science; 2012.
32. Tekerek M. Bilgi güvenliği yönetimi. *KSÜ Doğa Bilimleri Dergisi.* 2008;11(1):132-137.
33. Mehraeen E, Ayatollahi H, Ahmadi M. Health information security in hospitals: the application of security safe guards. *Acta Inform Med*. 2016;1 (24):47-50. doi:10.5455/aim.2016.24.47-50.
34. Naicker V, Mafaiti M. The establishment of collaboration in managing information security through multisourcing. *Comput Secur*. 2019;80:224-237. doi:10.1016/j.cose.2018.10.005.