2022

YÜKSEK LİSANS TEZİ

Emel TAÇAR

T.C.

ANKARA YILDIRIM BEYAZIT ÜNİVERSİTESİ

SAĞLIK BİLİMLER ENSTİTÜSÜ

ELEKTRONİK SAĞLIK KAYITLARI KULLANIMINDA HEMŞİRELERİN BİLGİ GÜVENLİĞİ FARKINDALIK DÜZEYLERİNİN BELİRLENMESİ

YÜKSEK LİSANS TEZİ

Emel TAÇAR

HEMŞİRELİK PROGRAMI

Ankara, 2022

T.C.
ANKARA YILDIRIM BEYAZIT ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

ELEKTRONİK SAĞLIK KAYITLARI KULLANIMINDA HEMŞİRELERİN BİLGİ GÜVENLİĞİ FARKINDALIK DÜZEYLERİNİN BELİRLENMESİ

YÜKSEK LİSANS TEZİ

Emel TAÇAR

HEMŞİRELİK PROGRAMI

Ankara, 2022

T.C.
ANKARA YILDIRIM BEYAZIT ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

Elektronik Sağlık Kayıtları Kullanımında Hemşirelerin Bilgi Güvenliği Farkındalık Düzeylerinin Belirlenmesi

Emel TAÇAR

Yüksek Lisans Tezi

31.01.2022

Tez Danışmanı
Doç. Dr. Hilal TÜZER

Jüri Üyeleri
Doç Dr. Hilal TÜZER
Doç Dr. Bahar İNKAYA
Doç. Dr. Emine ÖKSÜZ

Okuduğumuz ve Savunmasını dinlediğimiz bu tezin bir Yüksek Lisans derecesi için gereken tüm kapsam ve kalite şartlarını sağladığını beyan ederiz.

Doç. Dr. Fatma Elif KILINÇ
Enstitü Müdürü
Bu tezin Yüksek Lisans derecesi için gereken tüm şartları sağladığını tasdik ederim.

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün aşamalarda patent ve telif haklarını ihlal edici etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, bu tezde kullanılmış olan tüm bilgi ve yorumlara kaynak gösterdiğimi beyan ederim. 31.01.2022

Emel TAÇAR

TEŞEKKÜR

Tez çalışmam boyunca yardımlarını esirgemeyen ve beni her zaman destekleyen danışman hocam Sayın Doç. Dr. Hilal TÜZER'e,

Tez konumu belirlememdeki eşsiz katkılarından dolayı değerli arkadaşım Sayın Nesrin DEMİR EREN'e,

Araştırma izni alma ve anket çalışmasını uygulama sürecimdeki yardımlarından dolayı Sayın Doç. Dr. Halil KARA'ya,

Lisansüstü eğitim sürecimin her anında yanımda olan ve beni teşvik eden Ankara İl Sağlık Müdürlüğü'ndeki çalışma arkadaşlarıma ve amirlerime,

Tez yazdığım süre boyunca teknik olarak desteklerinden ötürü Sayın Serkan ŞENTÜRK'e,

Hayatım boyunca unutmayacağım bir etki bırakan 2018 Bahar dönemi Hemşirelik Esasları Dersi staj uygulamasındaki güzel öğrencilerime,

Tez sürecimde, hayatta karşılaştığımız güçlükler karşısında sabırlı olmayı, emek vermeyi, gerektiğinde vazgeçebilmeyi ve her daim olana şükretmeyi öğütleyen Sayın Dr. Levent ENDER'e,

Sevgi ve anlayışları ile beni hiç yalnız bırakmayan aileme,

Sonsuz teşekkürler.

İÇİNDEKİLER

ÖZET ..... **iv**

ABSTRACT ..... **v**

SİMGELER VE KISALTMALAR DİZİNİ ..... **vi**

ŞEKİLLER DİZİNİ ..... **vii**

TABLOLAR DİZİNİ ..... **viii**

1. GİRİŞ 1

2. GENEL BİLGİLER 6

2.1. İnsan Hakları 6

2.2. Hasta Hakları 6

2.2.1. Mahremiyetin Tanımı ve Önemi 7

2.2.2. Dijitalleşme ve Mahremiyet 8

2.3. Kişisel Veri 10

2.4. Hassas Veri 13

2.5. Kişisel Verilerin Korunması 14

2.6. Bilgi Sistemleri 18

2.6.1. Bilgi Yönetimi 20

2.6.2. Bilgi Güvenliği 21

2.7. Elektronik Sağlık Kayıtları 24

2.7.1. Elektronik Sağlık Kayıtlarında Hemşirenin Rolü 26

2.7.2. Elektronik Sağlık Kayıtlarında Bilgi Güvenliği 29

2.7.3. Elektronik Sağlık Kayıtlarında Bilgi Güvenliğini Etkileyen Faktörler 31

2.7.4 Sağlık Çalışanlarının Bilgi Güvenliği Kültürü 33

2.8. Siber Saldırı 35

2.9. Veri İhlalleri 37

3. MATERYAL VE YÖNTEM 39

3.1. Araştırmanın Şekli 39

3.2. Araştırmanın Yapıldığı Yer ve Özellikleri 39

3.3. Araştırmanının Evren ve Örneklemi 39

3.3.1. Araştırmanının Evreni 39

3.3.2. Araştırmanın Örneklemi 40

3.4. Veri Toplama Araçları 40

3.4.1. Sosyo-Demografik Veri Formu.....40
3.4.2. Bilgi Güvenliği Ölçeği.....40
3.5. Araştırmanın Uygulanması.....43
3.6. Araştırmanın Sınırlılıkları.....44
3.7. Verilerin Değerlendirilmesi.....44
3.8. Araştırmanın Etik Boyutu.....44
4. BULGULAR 45
4.1. Araştırmaya katılanların hemşirelerin kişisel bilgilerine ilişkin dağılım.45
4.2. Araştırmaya katılan hemşirelerin HBYS kullanımında erişimlerin denetimi konusundaki görüşlerine ilişkin dağılım.....46
4.3. Araştırmaya katılan hemşirelerin HBYS kullanımlarına ilişkin dağılım.....47
4.4. Araştırmaya katılan hemşirelerin hastadan onam alma durumlarına ilişkin dağılım.....48
4.5. Araştırmaya katılan hemşirelerin bilgi güvenliği uygulamalarına ilişkin dağılım.....49
4.6. Araştırmaya katılan hemşirelerin bilgi güvenliği konusunda farkındalık uygulamaları tercihlerine ilişkin dağılım.....51
4.7. Araştırmaya katılan hemşirelerin bilgi güvenliği kazaları konusunda bilgilendirilmek için uygulama tercihlerine ilişkin dağılım.....52
4.8. Bilgi Güvenliği Ölçeği ve Alt Boyutlarına ilişkin tanımlayıcı istatistikler…….....……...……..53
4.9. Günlük bilgisayar kullanım sürelerine göre Bilgi Güvenliği Ölçeği puanlarının farklılıklarının incelenmesi.....53
4.10. Günlük internet kullanım süresine göre Bilgi Güvenliği Ölçeği puanlarının farklılıklarının incelenmesi.....54
4.11. Cinsiyete göre Bilgi Güvenliği Ölçeği puanlarının farklılıklarının incelenmesi…….....……...……55
4.12.Yaşa göre Bilgi Güvenliği Ölçeği puanlarının farklılıklarının incelenmesi….....…….……56
4.13. Eğitim durumuna göre Bilgi Güvenliği Ölçeği puanlarının farklılıklarının incelenmesi.....57
4.14. Meslekte çalışma süresine göre Bilgi Güvenliği Ölçeği

puanlarının farklılıklarının incelenmesi.....58
5. TARTIŞMA 60
6. SONUÇ VE ÖNERİLER 69
6.1. Sonuçlar……..…….....……69
6.2. Öneriler……..…….....70
7. KAYNAKLAR 71
8. EKLER 88
EK-1. Etik Kurul Onayı.....88
EK-2. Sosyo-Demografik Veri Formu.....89
EK-3. Bilgi Güvenliği Farkındalık Ölçeği.....91
EK-4. Ölçek İzni.....97
EK-5. SBÜ Etlik Zübeyde Hanım Kadın Hastalıkları EAH Araştırma İzi.....98
EK-6. SBÜ Ankara Dr. Abdurrahman Yurtaslan Onkoloji EAH Araştırma İzni.....100
EK-7. Bilgilendirilmiş Onam Formu.....102
EK-8. Özgeçmiş.....104

ÖZET

Elektronik Sağlık Kayıtları Kullanımında Hemşirelerin Bilgi Güvenliği Farkındalık Düzeylerinin Belirlenmesi

Araştırma, elektronik sağlık kayıtları kullanımında hemşirelerin bilgi güvenliği farkındalık düzeylerinin belirlenmesi amacıyla yapılmıştır. Tanımlayıcı nitelikteki bu araştırma, 20 Eylül-20 Ekim 2021 tarihleri arasında yapılmıştır. Araştırmanın evrenini, Ankara ilindeki iki eğitim ve araştırma hastanesinde çalışan 807 hemşire, örneklemini ise 266 hemşire oluşturmaktadır. Veri toplama aracı olarak "Sosyo-Demografik Veri Formu" ve "Bilgi Güvenliği Ölçeği" kullanılmıştır. Veriler çevrimiçi olarak Google Formlar aracılığıyla toplanmıştır. Anket verilerinin analizinde Kolmogorov Smirnov, T Testi, Tek Yönlü Varyans Analizi (ANOVA) ve Tukey testi kullanılmıştır.

Araştırmaya katılan hemşirelerin %86,8'i kadın, %71,8'i lisans mezunudur. Bilgi Güvenliği Ölçeği puanları günlük bilgisayar kullanım süresi, cinsiyet, yaş değişkenlerine göre istatistiksel olarak anlamlı farklılık göstermektedir ($p<0.05$). Örgütsel Güvenlik alt boyutu, cinsiyete göre istatistiksel olarak anlamlı farklılık göstermektedir. Güvenlik Uygulamaları alt boyutu, çalışılan birim, yaş, eğitim durumu değişkenlerine göre istatistiksel olarak anlamlı farklılık göstermektedir. Erişim ve Yetkilendirme alt boyutu, günlük bilgisayar kullanım süresi, yaş, meslekte çalışma süresi değişkenlerine göre istatistiksel olarak anlamlı farklılık göstermektedir. Hizmet Sunumu alt boyutu, günlük bilgisayar kullanım süresi, yaş, meslekte çalışma süresi değişkenlerine göre istatistiksel olarak anlamlı farklılık göstermektedir. Hemşirelerin, Hastane Bilgi Yönetim Sistemi'nde, hastalara ait bilgilere kolaylıkla erişebildikleri ve bu veriler üzerinde okuma, yazma ve ekleme yetkilerinin olduğu görülmektedir. Bilgi güvenliğine ilişkin sorunların nedenleri arasında ihmal, dikkatsizlik, eğitim yetersizliği, ekranların açık bırakılması ve şifrelerin paylaşılması yer almaktadır.

Bu araştırmaya göre, hemşirelerin bilgi güvenliği farkındalık düzeyi, kadınlarda daha yüksektir. Bilgisayar kullanım süresi ve yaşın artması ile birlikte farkındalıkta artış görülmektedir. Sonuçlar, hemşirelere bilgi güvenliği konusunda daha fazla eğitim verilmesi gerektiğini göstermektedir.

Anahtar Kelimeler: Bilgi güvenliği, elektronik sağlık kayıtları, hassas veri, hemşire, veri ihlali.

ABSTRACT

Determination of Nurses' Awareness of Information Security Regarding The Use of Electronic Health Records

This research was conducted to determine nurses' awareness of information security regarding the use of electronic health records. This descriptive research was conducted between September 20 and October 20, 2021. The research population consisted of 807 nurses from two training and research hospitals in Ankara. The sample of the research consisted of 266 nurses. "Sociodemographic Data Form" and "Information Security Scale" were used as data collection tools. Data was collected online via Google Forms. The data were analyzed using the Kolmogorov Smirnov test, t-test, one-way Analysis of Variance (ANOVA), and Tukey test.

Most participants were women (86.8%) and had bachelor's degrees (71.8%). Participants' Information Security Scale scores statistically significantly differed by computer use duration, gender, and age ($p<0.05$). Their Information Security Scale "organizational security" subscale scores statistically significantly differed by gender. Their Information Security Scale "security practices" subscale scores differed by the unit of duty, age, and education. Their Information Security Scale "access and authorization" subscale scores differed by computer use duration, age, and work experience. Their Information Security Scale "service delivery" differed by computer use duration, age, and work experience. It is seen that nurses can easily access patient information in the Hospital Information Management System and have the authority to read, write, and add on the data. They experience information security problems due to negligence, carelessness, lack of training, leaving screens on, and sharing passwords.

According to this research, nurses' level of information security awareness is higher in women. There is an increase in awareness with an increase in computer use time and age. The results indicate that nurses should be provided with more training in information security.

Keywords: Information security, electronic health records, sensitive data, nurse, data breach.

SİMGELER VE KISALTMALAR DİZİNİ

AİHM : Avrupa İnsan Hakları Mahkemesi
AB : Avrupa Birliği
BGÖ : Bilgi Güvenliği Ölçeği
BGYS : Bilgi Güvenliği Yönetim Sistemi
GDPR : General Data Protection Regulation
GVKT : Genel Veri Koruma Tüzüğü
HBYS : Hastane Bilgi Yönetim Sitemi
HIPAA : Sağlık Sigortası Taşınabilirliği ve Sorumluluğu Talimatı
KVK : Kişisel Verilerin Korunması
KVKK : Kişisel Verilerin Korunması Kanunu
SKS : Sağlıkta Kalite Standartları

ŞEKİLLER DİZİNİ

Şekil 2.1. Bilgi yönetim sistemi standartlarının hastanelerde karşılanma sayısı ve karşılanma düzeyi…..…….....……..... 21
Şekil 2.2. Sektörlere göre 2017-2018 yılları ortalama siber suç maliyeti.....….30
Şekil 2.3. Bilgi güvenliği uygulamasında yetersiz koşullar….....32
Şekil 2.4. Ülkelere göre 217-2018 yılları siber suç maliyetleri….....35

TABLOLAR DİZİNİ

Tablo 4.1. Araştırmaya katılanların hemşirelerin kişisel bilgilerine ilişkin dağılım.....45
Tablo 4.2. Araştırmaya katılan hemşirelerin HBYS kullanımında erişimlerin denetimi konusundaki görüşlerine ilişkin dağılım.....46
Tablo 4.3. Araştırmaya katılan hemşirelerin HBYS kullanımlarına ilişkin dağılım.....47
Tablo 4.4. Araştırmaya katılan hemşirelerin hastadan onam alma durumlarına ilişkin dağılım.....48
Tablo 4.5. Araştırmaya katılan hemşirelerin bilgi güvenliği uygulamalarına ilişkin dağılım.....49
Tablo 4.6. Araştırmaya katılan hemşirelerin bilgi güvenliği konusunda farkındalık uygulamaları tercihlerine ilişkin dağılım.....51
Tablo 4.7. Araştırmaya katılan hemşirelerin bilgi güvenliği kazaları konusunda bilgilendirilmek için uygulama tercihlerine ilişkin dağılım.....52
Tablo 4.8. Bilgi Güvenliği Ölçeği ve Alt Boyutlarına ilişkin tanımlayıcı istatistikler.....53
Tablo 4.9. Günlük bilgisayar kullanım sürelerine göre Bilgi Güvenliği Ölçeği puanlarının farklılıklarının incelenmesi.....53
Tablo 4.10. Günlük internet kullanım süresine göre Bilgi Güvenliği Ölçeği puanlarının farklılıklarının incelenmesi.....54
Tablo 4.11. Cinsiyete göre Bilgi Güvenliği Ölçeği puanlarının farklılıklarının incelenmesi……55
Tablo 4.12. Yaşa göre Bilgi Güvenliği Ölçeği puanlarının farklılıklarının incelenmesi……56
Tablo 4.13. Eğitim durumuna göre Bilgi Güvenliği Ölçeği puanlarının farklılıklarının incelenmesi……..……..57
Tablo 4.14. Meslekte çalışma süresine göre Bilgi Güvenliği Ölçeği puanlarının farklılıklarının incelenmesi……..……..58

1. GİRİŞ

Tüm dünya'da hızla gelişen teknoloji, bireylerin günlük hayatlarını kolaylaştırmak için kendilerine ait birçok bilgiyi paylaşmasını gerektirmektedir. Bireyler dijital ortamlarda, kendileri ile ilgili bilgileri paylaşmayı, onam alınmaksızın konuşma ve davranışlarının kaydedilmesini kabullenmekte hatta kendileri talep etmektedir (1). Bu sebeple dijitalleşme, hukuksal ve siyasal sistemlerin gündeminde yer alan insan haklarının korunması ile kamu güvenliği arasındaki dengenin sağlanması için, temel haklar kavramının yeniden gözden geçirilmesini gerektirmektedir (2). Dijital platformlarda bilgi paylaşımı yapılırken, insan hakları çerçevesine zarar vermeden bilginin bir bütün olarak korunması gerekmektedir (3). Çünkü bilişim teknolojileri kullanımından kaynaklı olası risk ve tehditler, bireylere maddi kayıplar yaşatabilir, izinsiz olarak kişisel verilerine erişilebilir ve verilerinin değiştirilmesi ya da silinmesi halinde geri dönüştürülemeyen hasarlar yaratabilir (4).

Bilişim teknolojilerinin getirdiği tehdit ve riskler, toplumsal algılardan da etkilenmektedir. Örneğin, 2012 yılında Davos'ta yapılan Dünya Ekonomik Forumu toplantısında, gelişmekte olan ülkelerde mobil cihazlardaki etkileşimlerden kaynaklı olarak dünyada veri patlaması yaşandığı belirtilmekte ve "veri" ekonomik bir değer olarak ifade edilmektedir (5). Oluşturulan bu algı neticesinde ekonomik değer haline gelen veri, siber suçlar için ciddi bir hedef haline gelmektedir. Amerika'da yayınlanan Siber Suç Maliyet Raporu'nda, 2018 yılında ABD'de siber suçlardan kaynaklı olarak 27.37 milyon dolarlık bir maliyet oluştuğu belirtilmektedir. Siber suçların maliyetine ilişkin 2019-2023 yılları içinde küresel olarak risk altında olan değerlere dair yapılan analizde ise siber suçlardan kaynaklı doğrudan ya da dolaylı olarak risk altındaki toplam değerin 5.2 trilyon dolar olabileceği öngörülmektedir (6).

Dijital ortamlarda paylaşılan kişisel verilerin ekonomik bir değer olarak risk taşımaya başlaması bu verilerin niteliklerini önemli hale getirmektedir. Kişinin onamı alınmadan, nasıl ve kim tarafından kullanılacağı bilinmeksizin bu bilgilerin paylaşımı, gizliliği, bütünlüğü ve erişilebilirliği nitelikleri yönünden, hukuken korunması

gerekliliğini ortaya koymaktadır (1,7). Bireyin "ırksal veya etnik kökeni, siyasi görüşü, dinsel veya felsefi inancı, sendika üyeliği, sağlık ve cinsel yaşamı ve her türlü mahkûmiyetleri" konuları, farklı bir korumaya tabi olması gereken, hassas veri şeklinde değerlendirilmekte ve buna yönelik düzenlemeler yapılmaktadır (8,9). Bireye özgü her çeşit bilgi "kişisel veri" olarak tanımlanırken (8) Türkiye'de 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun 3. Maddesinde *"Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi"* olarak ele alınmaktadır. İlgili kanunun 6. maddesinde ise hassas veriler, özel nitelikli kişisel veriler olarak yer almaktadır (10).

Her alanda olduğu gibi sağlık endüstrisi de dijital dönüşümden etkilenmektedir. Hassas veri olarak nitelendirilen sağlık kayıtlarının dijitalleştirilmesi, sağlık hizmetleri endüstrisinde büyük değişimlere yol açmaktadır (11). Sağlık bilişim sistemi olarak anılan bu dijital sistemler sayesinde hizmetin sunumunda sağlık çalışanlarını desteklemek, işlerini kolaylaştırmak amaçlanmaktadır (12,13). Hasta bireye özgü klinik hikâyeler ve tanı raporlarının elektronik ortamda toplanması anlamına gelen elektronik sağlık kayıtları (12,14), sağlık hizmeti sunan pek çok meslek grubu tarafından kullanılmakta ve bilgisayar ortamına aktarılan hasta kayıtlarına erişebilmektedir. Elektronik ortamda depolanan bu kayıtlar; hastalıkların nedenleri, en iyi tedavi yöntemleri, ortaya çıkmış yeni vakalar, hastalık grupları gibi detaylı bilgilere ulaşılabilmeyi sağlamakta (12) ve gelişmiş tedavi sonuçları ile tıbbi bakım deneyimleri sunmaktadır (11). Bununla beraber, giderek daha karmaşık hale gelen dijital sistemler, aynı zamanda büyük güvenlik sorunları da oluşturmaktadır (11).

Dijital ortamdaki hastane verilerinin olası bir siber saldırı durumunda ne şekilde ve ne kadar sağlam korunacağı bilinememektedir. Örneğin 13 Mayıs 2017 tarihindeki 99 ülkenin etkilendiği bir siber saldırı sonucunda İngiltere Milli Sağlık Sisteminin (National Health Service – NHS) çöktüğü bilinmektedir (15). Amerika'nın en büyük sigorta şirketlerinden birinden 2015 yılında 80 milyon kişinin sağlık verilerinin çalınması olayı sağlık kayıtlarına yönelik tarihteki en büyük hırsızlık olarak yer almaktadır (16). Fidye yazılımı saldırıları (verileri şifrelemeyi ve şifreleme karşılığında ödeme talep etmeyi içeren bir tür siber güvenlik tehdidi), pandemi sırasında pek çok hastaneyi hedef aldığı bilinmektedir. Almanya'da gerçekleşen bir fidye yazılımı saldırısı bir hastanın ölümüne yol açtığı belirtilmektedir. Bu durumun

siber saldırı sonucu sağlık sektöründeki ilk ölüm olabileceği öne sürülmektedir (17). Birleşik Arap Emirliklerinde 562 hemşireyle, elektronik sağlık kayıtlarında mahremiyet, gizlilik, güvenlik ve hasta güvenliği ile ilgili endişelere ilişkin bir çalışma yapıldığı görülmektedir. Bu çalışmada; hemşirelerin özellikle yetkisiz kişilerin erişimi ve sistem içinde meydana gelen hataların denetlenmemesi başta olmak üzere veri bütünlüğü ile ilgili endişeleri olduğu sonucuna ulaşıldığı belirtilmektedir (18).

Dijital ortamdaki kişisel veriler, bireye kendini güçsüz hissettirmekte dolayısıyla bireyin özel hayatının gizliliği ve mahremiyet hakkının ihlali söz konusu olmaktadır (1,8). Böylelikle kişisel verilerin saklanması ve korunması, tıpta temel etik ilkeler arasında yer alan mahremiyet kavramının önemli bir öğesi haline gelmektedir (16). İnsan haklarına yönelik yaşanan gelişmelerin yanında, insanların bilgi ve kültür düzeylerindeki değişim sonucu bakış açılarının farklılaşması, insanın değerli bir varlık olduğu görüşünün yaygınlaşması, hasta haklarını korumak için kurulan uluslararası birlikler, teknolojik gelişmeler, hasta haklarına yönelik oluşturulan ulusal ve uluslararası mevzuatlar, hasta hakları ve hasta mahremiyetine verilen önemi de etkilemektedir (19).

Hastanın mahremiyeti ve gizliliği, sağlık alanında çalışanların en önemli sorumlulukları arasında yer almaktadır (19,20). Elektronik sağlık kayıtları ise bir sağlık kuruluşunun en değerli varlıklarından birisidir (21). Veri ihlallerinin hastaların yaşamları üzerinde doğrudan ve ciddi sonuçları olabileceği ayrıca sağlık kuruluşlarının bilgi güvenliği tehditlerine karşı savunmasız olduğu belirtilmektedir (11).

Hayati verileri garanti altına alma konusunda diğer önde gelen endüstrilerden geri kalan sağlık sektörü, tıbbi bilgi hırsızlığında temel bir hedefe dönüşmektedir (22). Dijital sağlık teknolojileri yaygınlaştıkça kişisel sağlık bilgilerinin mahremiyeti, güvenliği, ifşası ve kullanımı tartışma konusu olmaktadır (23). Kişilerin, sağlık sisteminin ve diğer kapsam dışı kuruluşların kişisel sağlık bilgilerine nasıl eriştiğini, kullandığını ve ifşa ettiğini bilmesi ve kontrol edebilmesi önemlidir (24).

Kişisel sağlık kayıtlarını olabilecek her tür hasara karşı korumak için bütçe dâhilinde gerekli her şey yapılsa da insan kaynaklı hatalar dikkate alınması gereken en önemli konudur (21,25). İnsanlar, bilgi güvenliği yönetiminde en zayıf halkayı oluşturmaktadır (9,11). Bilgi güvenliğini sağlayan zincirdeki en zayıf halka da insan

kaynaklı tehditlerdir (4,26,27). Bilgi güvenliği politikalarını ihlal eden herhangi bir çalışan, sağlık kuruluşlarını bir siber saldırıya karşı savunmasız hale getirebilmektedir (11).

Hastaların veri gizliliğine yönelik en büyük iki tehdit; yürürlükte olan çeşitli politika ve düzenlemeler ile bunların hastaların verilerinin işlenmesini nasıl etkilediğinin anlaşılmaması ve bilgisayar korsanlarının oluşturduğu tehditlerdir (28). Sağlık sektöründe, son zamanlarda diğer sektörlerden daha fazla veri ihlali yaşanmakta ve bulut, büyük veri ve diğer teknolojilerin kullanımı nedeniyle risk artmaktadır (29).

Siber saldırılar, hasta mahremiyetini, sağlık çalışanlarının bakım sunma yeteneğini ve sağlık kuruluşlarının güvenliğini olumsuz yönde etkilemektedir (30). Kullanıcıların farkındalık düzeyinin, bilgi güvenliği seviyesi üzerinde önemli bir etkiye sahip olduğu ifade edilmektedir (19). Sağlık sektöründe istihdam edilen unvanlar arasında sayıca çoğunlukta olan hemşirelerin (31), hasta bakımı ve sağlık teknolojisi kullanımının ön saflarında yer almaları sebebiyle, siber suçlardan korunma ve bunların bildirimi için benzersiz bir konuma sahip oldukları belirtilmektedir (30).

Hemşirelerin, Hastane Bilgi Yönetim Sistemi (HBYS) üzerinden hastalara ait hangi bilgilere erişebildiği, bu bilgiler üzerindeki yetkileri, denetim mekanizmaları ve bilgi güvenliğine yönelik farkındalık düzeylerinin bilinmesi ve olası riskler konusunda önlem alınması gerekmektedir. Özel ve kamuya bağlı sağlık kuruluşlarında, veri ihlalleri yaşandığı yönündeki başvuru, şikâyet ve bildirimler gündeme gelmekte ve konuya ilişkin adli, idari ve disiplin yönünden işlem tesis edildiği bilinmektedir. Hem hasta mahremiyeti hem de hukuki açıdan bireysel ve kurumsal yükümlülükler göz önüne alındığında, bilgi güvenliği hakkında hemşirelerin farkındalıkları oldukça önem arz etmektedir.

Hemşirelerin elektronik sağlık kaydı bilgisi ve tutumlarına yönelik yapılan birçok çalışma bulunmaktadır (9,32,33,34,35). Elektronik sağlık kayıtlarında bilgi güvenliği konusunda ise yurtdışında hemşireler ile yapılan çalışmalar bulunmakta (36,37) ancak Türkiye'de sağlık sektöründe çalışan farklı meslek gruplarıyla yapıldığı anlaşılmaktadır (7,38,39,40,41,42). Bilgi güvenliği farkındalık düzeylerini belirlemek amacıyla Türkiye'de hemşireler açısından değerlendirilen ve doğrudan hemşireler ile yapılan bir çalışma olmadığı görülmektedir. Dijitalleşen dünyaya hızlıca entegre olan

sağlık sektöründe elektronik sağlık kayıtlarını en yoğun kullanan, hasta ile uzun süre vakit geçiren hemşirelerdir. Birlikte çalıştıkları ekip üyelerinde de bu konuda farkındalık oluşturma potansiyelleri olan hemşirelerin, elektronik sağlık kayıtları kullanımında bilgi güvenliği farkındalık düzeylerinin belirlenmesi ile araştırmamızın, bu alanda özgün bir çalışma olacağı düşünülmektedir. Bu çalışmanın, elektronik sağlık kayıtlarında bilgi güvenliğini sağlamak adına gelecekte yapılacak hizmet içi eğitimler, yasal düzenlemeler ve hemşirelik eğitim müfredatlarının geliştirilmesine rehberlik etmesi beklenmektedir.

2. GENEL BİLGİLER

2.1. İnsan Hakları

Doğumla elde edilen insan hakları; evrensel bildirgeler, sözleşmeler ve her ülkenin kendi kanunları çerçevesinde hukuki açıdan güvence altına alınmaktadır (1). II. Dünya Savaşı'nda insan haklarına yönelik yaşanan ağır ihlaller sonrasında oluşturulan İnsan Hakları Evrensel Beyannamesi ve Avrupa İnsan Hakları Sözleşmesi, Türkiye'de 1961 ve 1982 Anayasalarının hazırlanmasına zemin oluşturmuştur (43). Türkiye'de 1982 Anayasası'nın kişisel, sosyal, ekonomik ve siyasi hak ve ödevler olarak sınıflandırıldığı görülmektedir. Türkiye'de 1982 Anayasası'nın 17. ve 40. Maddeleri arasında yer alan; Kişinin Dokunulmazlığı, Kişi Hürriyeti ve Güvenliği, Maddî ve Manevî Varlığı, Özel Hayatın Gizliliği, Din ve Vicdan Hürriyeti, Temel Hak ve Hürriyetlerin Korunması, Mülkiyet Hakkı başlıkları altındaki kişisel haklar ile birey korunmaktadır (1).

Özel hayatın gizliliğine ve kişisel mahremiyete ilişkin 1982 Anayasası, Avrupa İnsan Hakları Sözleşmesi ve İnsan Hakları Evrensel Beyannamesi'nin 3. ve 12. maddelerinde özel alana dair düzenlemelerin yapıldığı görülmektedir (44).

2.2. Hasta Hakları

Her hasta kaliteli bakım alabilme hakkına sahiptir. Bu sebeple hastaların çalışanlara güven duyabilmesi, hasta memnuniyetinin sağlanabilmesi, hasta mahremiyeti ve haklarının korunabilmesi oldukça önemlidir (20). Hasta hakları, sağlık hizmeti sunumunun her hali ve seviyesinde geçerliliğini koruyan bir hak olmasından dolayı birçok meslek grubunu ilgilendirmektedir. Kişinin sağlık hakkı, yaşam hakkı gibi konuların dolaylı da olsa hasta hakları kapsamına alındığı bilinmektedir (19).

Hasta Hakları Yönetmeliği'ndeki 4.bölüm, hasta haklarının korunmasına değinir. Yönetmeliğin 21.maddesine göre;

"Hastanın mahremiyetine saygı gösterilmesi esastır. Hasta mahremiyetinin korunmasını açıkça talep de edebilir. Her türlü tıbbi müdahale, hastanın

mahremiyetine saygı gösterilmek suretiyle icra edilir." denilmiştir. Yine aynı yönetmeliğin 20.maddesine (Değişik:RG-8/5/2014-28994) göreyse;

"İlgili mevzuat hükümleri ve/veya yetkili mercilerce alınacak tedbirlerin gerektirdiği haller dışında kişi, sağlık durumu hakkında kendisinin, yakınlarının ya da hiç kimsenin bilgilendirilmemesini talep edebilir. Hasta bilgi verilmemesi talebini istediği zaman değiştirebilir ve bilgi verilmesini talep edebilir." hükmü ile hastanın kendi bilgileri üzerindeki kontrol gücüne yer verilmektedir (45).

Mahremiyete saygı, tüm hastaların hakkıdır ve hastalara saygı duyulmaması, kaygı, stres, sağlık çalışanlarına dair güven eksikliği, fizik muayenenin reddedilmesi ve iyileşmenin bozulmasına yol açabilmektedir (46). Hastaların mahremiyeti ve gizliliğini korumak etik zorunluluktur (47). Hasta Hakları Yönetmeliği'nde mahremiyet hakkına açık şekilde yer verildiği görülmektedir (45).

2.2.1. Mahremiyetin Tanımı ve Önemi

Türk Dil Kurumu'na göre mahremiyet "gizlilik" olarak tanımlanmaktadır. Ancak mahremiyet kavramının tanımlanması oldukça zordur (48). Mahremiyetin, insanoğlunun var olduğu an itibariyle ortaya çıktığına inanılmakta ancak mahremiyet kavramı üzerinde uzlaşılmış bir evrensel tanım bulunmamaktadır. Bu mahremiyet algısının kültürel, toplumsal ve zamansal bakımdan değişkenlik göstermesinden kaynaklanmaktadır. Yine de mahremiyeti "gizli olması ve gizli kalması gereken şey" anlamında en yalın haliyle tanımlamak mümkündür (49).

Özgürlük ile mahremiyet kavramları doğrudan ilişkilendirilmektedir. Birey, sahip olduğu benlik bilinci ve kendini gerçekleştirme haliyle, beden, özel yaşam, giz, mülkiyet ve cinsellik gibi kavramlarla anılan, mahremiyete dayanak oluşturmaktadır Birey, şahsi eylemlerinde belirleyici ve paylaşımlarının sınırlarını oluşturan mahremiyet hakkıyla karar alabilmektedir (1). Dolayısıyla insanın saygınlığını koruma hususunda mahremiyet hakkına özen gösterilmesi dikkat edilmesi gereken en mühim konulardan biri olarak görülmektedir. Sağlık hizmetleri mahremiyet hakkının en çok gündeme geldiği alanlardan birisidir. Hastaya ait tüm bilgilerin gizli olması durumu olarak ifade edilen hasta mahremiyeti, hasta hakları arasında önemli bir konu olarak yer almakta ve giderek daha fazla gündeme gelmektedir (19).

2.2.2. Dijitalleşme ve Mahremiyet

Bireyin hayatı süresince davranış tarzı ve eğilimlerini yansıtan nitelikleri için kuşak kavramı devreye girmektedir. Bireyin gelecekteki davranış şekilleri ve karar alma mekanizmaları, yaşadığı zaman, toplumsal çevre ve farklı değişkenlerden etkilenir. Kuşaklar arasında ortaya çıkan farklılıkların temel sebepleri bunlar olsa da aslında insanların içinde bulunulan duruma uyum sağlama becerisi olarak ifade edilebilmektedir (50).

Enformasyon ve bilişim açısından bakıldığında; teknolojide yaşanan gelişmelerin hızına yetişemeyip teknolojiyle savaşmaktan vazgeçen ilk kuşağın X (1965- 1980) kuşağı olduğu belirtilmektedir. Y kuşağının (1981-1994) ise teknoloji ile şekillenmiş olması en önemli özelliğidir. Y kuşağının teknoloji ve tüketimle gönüllü bir ilişki içinde olması, X kuşağından ayıran en belirgin özelliktir. Teknolojinin içine doğmuş olan Z kuşağı (1995 ve Sonrası) ise, teknolojideki tüm gelişmelere hızlıca adapte olmakta ve bu gelişmeleri benimsemektedir (51). Dijital mahremiyet algısı kuşaktan kuşağa farklılık gösterse de bireyin, veri tabanlarında "dijital kod" algılandığı görülmektedir. Dijital ortamlara aktarılan bu kişisel verilerin ise, kim ve nasıl sorularının yanıtları bilinmeden paylaşılabilir, depolanabilir, yaygınlaştırılabilir ve analiz edilebilir şekilde olduğu ifade edilmektedir. Bu durum bireye kendini güçsüz hissettirmekte dolayısıyla bireyin özel hayatının gizliliği ve mahremiyet hakkının ihlali söz konusu olmaktadır (1,8,51).

Bilgilerin kurumsal bir ortamda nasıl işlendiği, iletildiği ve saklandığı konusunda genel nüfusun bilgi eksikliği olduğu belirtilmektedir (28). Böylece günümüz teknolojisi sayesinde, hem hükümetler hem de özel şirketler, bireylere ait kişisel verilere kolayca erişebilmekte ve bu verileri kendi çıkarlarına göre kullanabilmektedir. Bu yüzden bireyin temel haklarının savunmasız hale geldiği belirtilmektedir (52). Örnek olarak küresel bir sağlık sorunu olan COVID-19 pandemisinin yönetiminde temaslı takibiyle salgının yayılımının azaltılması hedeflendiği bilinmektedir (53). Popüler işletim sistemi markaları olan Apple ve Google işbirliği yaparak COVID-19 pozitif vakası ile yakın teması bulunan kişilerin tespiti için geliştirdikleri "maruz kalma arayüzünü" Nisan 2020'de piyasaya sürüldüğü belirtilmektedir (54,55). Ulusal kamu sağlığı otoriteleri tarafından geliştirilen temaslı takibi uygulamalarının Android ve iOS işletim sistemlerinde etkin çalışmaması

sebebiyle salgınla mücadele eden birçok ülke bu arayüzü kullanmak zorunda kaldığı ifade edilmektedir (56). Temaslı takibi uygulamaları ile elde edilen verilerin, Google ve Apple ile paylaşılmaması kullanıcılara, mahremiyetlerinin korunacağına ilişkin güven verse de; COVID-19 salgınıyla dünya nüfusunun büyük çoğunluğunun tek bir uygulama programlama arayüzü (API) ile kontrol edilebildiğini test etmelerine olanak sağladığı düşünülmektedir (55).

Enformasyon ve iletişim teknolojilerinde ortaya çıkan gelişmeler ile dünyayı çevreleyen iletişim ağları, yaşamın her alanında olduğu gibi; mahremiyet algısı üzerinde de değişimlere sebep olmaktadır. Mahremiyet; Avrupa'nın endüstrileşmesi ile başlayan kamusal ve özel alan ayrımının bir sonucu olarak değişime uğramaktadır. Küreselleşmeyle beraber iletişim teknolojileri ve taşıma araçlarındaki gelişim, özel ve kamusal alanlarda homojenleştirmeye yol açmaktadır (51). Örnek olarak, 11 Eylül olaylarından sonra terör saldırılarına karşı önlem almak amacıyla ABD'de geliştirilen gözetleme ve denetleme araçları, güvenlik için mahremiyeti kurban etmeyi meşru hale getirmektedir. Sharon'a göre, COVID-19 salgınını kontrol etmek üzere tasarlanan filyasyon uygulamalarıyla da "mahremiyet ve toplumsal sağlık" iki zıt kutup gibi sunulmakta insanlar kısıtlı bir tercih yapmaya zorlanmaktadır (56).

Bilişim teknolojileri ve internetin giderek artan gelişimi; internetin sağladığı avantajların artması neticesinde internet kullanım oranları oldukça yükselmekte ve çevrimiçi ortamlarda hızlı ve çok yoğun bir enformasyon akışı oluşmasına neden olmaktadır. Enformasyondaki bu akış, farklı amaçlar ile gözetim teknolojilerini sayesinde kontrolü elinde tutmak isteyen devlet, reklam şirketi ve bilgisayar korsanlarının etkinlikleri, internet güvenliği ve çevrimiçi gizlilik ihlallerine yol açmaktadır (49). Mahremiyet ihlalleri, yanlış kişinin bilgiye erişmesi, bilgiye erişim sürecinin ihlal edilmesi veya erişim amacının uygun olmaması vb. nedenlerle meydana gelmektedir (48). Kişilere ait birçok bilginin bilgi sistemleri sayesinde erişilebilir hale geldiği anlaşılmakla beraber, kişisel verilerin korunması ihtiyacı ortaya çıkmaktadır (57).

Aslanyürek'in (2016) çalışmasında; internet kullanıcılarının internette kendilerini daha özgür hissettikleri ve internette var olmayı kişisel güvenlikten daha çok önemsedikleri sonucuna ulaşıldığı görülmektedir. Aynı zamanda, katılımcıların

çoğu siber ortamda internet güvenliği ve çevrimiçi gizliliğin bilgisayar korsanları, pazarlama şirketleri ve devlet tarafından ihlal edildiği belirtilmektedir (49).

Charbonneau (2016), sağlıkla ilgili sosyal destek amacıyla oluşturulan çevrimiçi topluluklara ait sosyal ağ sitelerinin gizlilik uygulamalarının durumunu değerlendirmek amacıyla 25 çevrimiçi over kanseri topluluğunun gizlilik politikalarını incelediği görülmektedir. Çalışma örneğinde yer alan tüm sağlık sosyal ağ sitelerinin, kullanıcılara gizlilik bildirimlerini sağladığı, ancak gizlilik uygulamalarının siteler arasında önemli ölçüde farklılık gösterdiği belirtilmektedir. Sitelerin çoğu, katılımcılar hakkında kişisel bilgilerin toplandığı ve üçüncü taraflarla paylaşıldığı konusunda kullanıcıları bilgilendirdiğini, sitelerin yarısından fazlasıysa kullanıcı davranışlarını izlemek için çerez teknolojisi kullandığını ifade etmektedir. Sitelerin çok azının bireylerin kişisel bilgilerini silmelerine izin verdiği görülmektedir. Çevrimiçi ortamlarda mahremiyet, gizlilik, tüketici seçimi ve veri güvenliğine ilişkin çıkarımlar tartışmaya açık olduğu belirtilmektedir (58). Kişisel verilerin saklanması ve korunmasının, tıpta temel etik ilkeler arasında yer alan mahremiyet kavramının önemli bir öğesi haline geldiği görülmektedir (16).

2.3. Kişisel Veri

Veri, çoğul bir terim olarak geçen "data" kavramıyla ifade edilmektedir (16). Gelişmekte olan ülkelerde mobil cihazlarda artan etkileşimlerden kaynaklı olarak dünyada yaşanan veri patlaması sonucu veri selleri oluştuğu vurgulanmaktadır. Bu veri sellerinin, kullanıcıların ihtiyaçları belirlemek ve hizmet sağlamak için kullanılabileceği potansiyeli fark edildiği belirtilmektedir (5). Verinin depolandığı süreçten bilgiye dönüşümüne kadar olan tüm süreçlerin büyüklüğünü tanımlayan bir kavrama dönüşen büyük verinin (big data), 2012 yılı sonrasında ivme kazandığı görülmektedir. Ancak büyük verinin analizine dayalı olan bu süreç, temelde kişilere ait verilerin veri tabanlarında oluşturulan ortak bir havuzda toplanması sonucu elde edilmektedir (16).

Kişisel veri "*Belirli veya belirlenebilir nitelikteki bir kişiye ait her türlü bilgi*" şeklinde tanımlanmaktadır (10). Veri bir kişiye ait olmalı ve bu kişi de belirlenebilir olmalıdır. Bireyin isimden, duygu ve düşüncelere, tercihlere kadar uzanan geniş bir yelpazedeki verilerine dair denetim yetkisini kaybetmesi bireyin özgürlüğünü,

özerkliğini, mahremiyetini kısaca "ben" olma özelliğinin kaybetmesine neden olmaktadır. Tüm bunlar "ben"e ait veriler üzerinde bireyin denetim yetkisini gerekli kılmaktadır. İçinde bulunduğumuz postmodern süreç, her şeyi metalaştırmakta ve değer kavramını ekonomik bir değer şekline dönüştürmekte böylece tüketimin de hızla artmasına yol açmaktadır. Teknolojinin yarattığı hız ile ekonomik değere dönüşen meta için sürecin gereksinim duyduğu hız birbiriyle sinerjik bir etki içindedir. Kişisel veriler açısından da süreç, veriyi metalaştırarak ekonomik bir değer haline getirmektedir (1).

Kişisel veri, tartışmaya açık ve sınırları net bir şekilde çizilememiş bir kavram olsa da "insana ait, bireyi tanımlayabilecek her türlü bilgi" olarak ifade edilmektedir. Örneğin kişinin ismi, adres bilgileri, etnik kökeni, medeni durumu, cinsel tercihleri, hastalıkları, siyasi düşünceleri kişisel veri olarak nitelendirilmektedir. Bilim ve teknolojide yaşanan gelişmelerin toplumsal yaşamın bileşenlerine ve topluma yansımasıyla birçok bilgi kişisel veri halini almaktadır. Bu kapsamda vatandaşlık numarası, sosyal güvenlik numarası, banka hesap numarası ve e-posta adresi şifresi bunlara birer örnek olarak verilebilmektedir (8).

İnternetin gelişmesi, kişisel verilerle ilgili tartışmaları arttıran bir dönüm noktası olarak ifade edilmektedir. Bilgisayar ekranları bir pencere olarak genel kabul görmekte ve internet kullanıcılarının aradığı her bilginin dışarıya da akmasıyla veri tabanlarında depolanmaktadır (1). Önceden az sayıda kişi ya da kurumun bünyesinde yazılı halde dosyalanan bu bilgiler bilişim teknolojisindeki gelişmelerle dijital ortama aktarılarak, internetin yaygınlaşmasıyla da hukuka uygunluğuna bakılmaksızın ilgili ya da ilgisiz herkesin erişimine açılmaktadır (8).

IP adreslerini izleyerek, çerezler ve casus yazılımlar kullanarak, GPS'ler aracılığıyla araçların takibine kadar birçok teknikle bilgi akışı sağlanmaktadır. Bireyin kendi istemiyle internet kullanıcısı olması, web sitelerine üye olabilmek için kendi bilgilerini vermesi, bireyin rızası olarak sayılması gerektiği belirtilmektedir. Ancak birey, bilgilerini kendi istemiyle verdiği için rızaya dayalı olduğu şeklinde yorumlansa da sonrasında toplanma amacının dışında başka amaçlar için bu verilerin işlenmesinin rızaya dayalı olmadığı oldukça açıktır (1). Tüm bu bilgiler ışığında, toplumun son yıllarda hızla artan dijitalleşme konusunda, yarar ve zararlarını fark edebilecek düzeyde veri okuryazarlığına sahip olması gerektiği belirtilmektedir (59).

Türkiye' de kişisel veri ve buna yönelik yasal düzenlemelere bakıldığında; 06.02.2004 tarih ve 25365 sayılı Resmi Gazete'de yayınlanarak yürürlüğe giren "Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik"te "*Kişisel bilgiler/veriler: Tanımlanmış ya da doğrudan veya dolaylı olarak, bir kimlik numarası ya da fiziksel, psikolojik, zihinsel, ekonomik, kültürel ya da sosyal kimliğinin, sağlık, genetik, etnik, dini, ailevi ve siyasi bilgilerinin bir ya da birden fazla unsuruna dayanarak tanımlanabilen gerçek ve/veya tüzel kişilere ilişkin herhangi bir bilgi*" şeklinde ifade edilmektedir (8,60).

Türkiye'de genel olarak 108 numaralı Avrupa Konseyi Sözleşmesi ve Veri Koruma Yönergesi temel alınarak hazırlanan Kişisel Verilerin Korunması Kanunu (KVKK) 24.03.2016 tarih ve 6698 sayı ile yürürlüğe girmiştir. Söz konusu kanunun 3. maddesinde kişisel veri, "*kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi*" şeklinde yer almaktadır (8,10).

Avrupa Birliğine üye ülkelerce doğrudan bağlayıcılığı olan ve 25 Mayıs 2018 yılında yürürlüğe giren (General Data Protection Regulation–GDPR) Genel Veri Koruma Tüzüğü (GVKT), özellikle kişisel verilerin korunması hakkını vurgulamaktadır (9,52,61,62).

KVKK'nın 6. Maddesi 3. Bendinde, sağlık ve cinsel hayata ilişkin kişisel verilerin işlenmesine dair düzenlemelere yer verilmektedir (10). Hasta mahremiyetinin sağlanması açısından kişisel sağlık verilerinin, özel hayatın gizliliği kapsamında yasal düzenlemeye kavuşturulduğu ve bu verilerin hukuka aykırı şekilde elde edilmesi ve amacı dışında kullanılması halinde Türk Ceza Kanunu'nda suç olarak ele alındığı görülmektedir (19,63).

Sağlık hizmeti sunumunda, teşhis, tedavi ve tedavi sonrasındaki bakım hizmetleri de dâhil olmak üzere tüm süreçlerde hastaya ait sağlık bilgilerini üçüncü kişilerle paylaşmanın yasak olduğu belirtilmektedir. Hastaya ait sağlık bilgileri ancak kamu yararı, adli vaka vb. istisnai bir durum oluştuğunda gereken yasal süreçler işletilerek üçüncü kişiler ile paylaşılabilir. İnsan hayatı süresince devam eden bu gizlilik ilkesinin ölüm halinde bile ortadan kalkmadığı görülmektedir. Ölen kişinin hatırasını itibarsızlaşma riski sebebiyle kişinin ölümünden sonra bile bilgilerini gizli

tutmak esastır. Hastanın hastalık/sağlık bilgileri dışında özel hayatı, aile yaşamı, özgeçmişi, inancı, psikolojik durumu gibi tüm bilgiler hasta mahremiyeti kapsamına girmektedir (19).

2.4. Hassas Veri

Veri koruma mevzuatı olan birçok ülkenin ve uluslararası düzenlemelerin, özel bir veri çeşidi olarak kabul ettiği ve hassasiyet gösterilmesi gereken bu veri türünün, özel olarak farklı bir korumaya tabi tutulması gerektiği düşüncesiyle bu yönde düzenlemelere gidildiği anlaşılmaktadır. Kişinin *"ırksal veya etnik kökeni, siyasi görüşü, dinsel veya felsefi inancı, sendika üyeliği, sağlık ve cinsel yaşamı ve her türlü mahkûmiyetleri"* hassas veri olarak nitelendirilmekte ve bu verilerin işlenmesinin yasak olduğu belirtilmektedir (8,9). Hassas kişisel verileri bazı ek güvencelerle koruma gerekliliğindeki temel mantık, bu tarz bilgilerin başta ayrımcılık olmak üzere diğer verilere nazaran ilgili kişi açısından daha ciddi zararlara neden olabileceği düşüncesinden kaynaklanmaktadır (8).

Avrupa Konseyi'nin 108 nolu Sözleşmesi ve Veri Koruma Yönergesinde sağlık verileri "tıbbi veri" olarak nitelendirilmekte ve hassas veri olarak kabul edilen tıbbi verilerin ancak üye devletlerin iç hukukunda gerekli güvenceleri sağlamaları koşuluyla işlenebileceği belirtilmektedir (8).

Hasta mahremiyetine ilişkin yer aldığı bir çalışmada; hekim ve hemşireler, hastanın paylaşılmasına rıza göstermediği tüm bilgileri, mahrem olarak değerlendirmektedir. Sağlık çalışanlarıyla özellikle hekim ve hemşirelerle paylaşılan bütün bilgilerin üçüncü şahıslarla paylaşılmaması konusunda hemfikir oldukları görülmektedir (19).

Hassas veri olan kişisel sağlık bilgilerinin, özel haller dışında kimseyle paylaşılmaması, saklanması ve işlenmemesi söz konusu olduğunda, sır saklama yükümlülüğü akla gelmektedir. Sır saklama yükümlülüğü, sağlık çalışanının sadakat yükümlülüğünden gelen bir alt yükümlülüktür. Hasta bilgilerini saklama yükümlülüğü kapsamında sır, gizli tutulması hastanın menfaatine olan her şeyi içine almaktadır. Hastaya ait tıbbi kayıtlara yalnızca ilgili kişiler erişebilir; tedavi sürecinde yer almayan sağlık personelleri de dâhil olmak başkaları görmemeli ve bu bilgilere ulaşamamalıdır

(8). Sağlık verilerine bir şekilde yetkisiz bir şekilde erişilirse, hastalar için güvenli olmayan ilaç veya tedavi değişiklikleri gibi tehlikeli bir şekilde kötüye kullanılabilir ve ciddi sorunlara neden olabilir veya hastanın ölümüne neden olabilir (64). Nitekim Hasta Hakları Yönetmeliği'nin 16. Maddesinde *"Hasta, sağlık durumu ile ilgili bilgiler bulunan dosyayı ve kayıtları, doğrudan veya vekili veya kanuni temsilcisi vasıtası ile inceleyebilir ve bir suretini alabilir."* şeklinde düzenlendiği görülmektedir (45).

Hasta bilgilerinin merkezi veri tabanında yanlış kişilerin ellerine düşmesinden korunması gerekmektedir. Hasta bilgileri, ağ üzerinden birkaç başka ağa iletildiğinde veya dağıtılmış bulut sunucularında depolandığında da veri ihlalleri oluşabilir (65,66,67). Sağlık verisi, son derece hassas ve kişisel olduğu için sağlık bilgi sistemlerinde hastanın mahremiyetinin korunması önemlidir. Özellikle bilimsel araştırmalar için paylaşılmak durumunda kalınan hasta verilerinin mahremiyetinin sağlanması gerekmektedir. Hastalara ait verilere yetkisiz erişim olması halinde kurumlara yasal yaptırımların uygulanması, hastane bilgi sistemlerinin fiziksel güvenliğinden, siber güvenliğine kadar detaylı önlemler alınması gerekmektedir (57).

2.5. Kişisel Verilerin Korunması

Gizlilik mevzuatı, veri yönetimi için bir çerçeve sağlar (68). Bu amaçla yetkililer, kişisel sağlık kayıtlarını çeşitli güvenlik tehditlerinden ve saldırılardan korumak için dünyanın belirli yerlerinde veri koruma düzenlemeleri uygulanmaktadır. En yaygın veri koruma düzenlemeleri arasında Genel Veri Koruma Tüzüğü (GVKT) ve Sağlık Sigortası Taşınabilirliği ve Sorumluluğu Talimatı (HIPAA) yer alır (69).

GVKT'nin, 26 Mayıs 2018'de tüm AB ülkelerinde yürürlüğe girmesiyle 1995'ten önceki Veri Koruma düzenlemelerinin kaldırıldığı belirtilmektedir (52,61,62). GVKT, AB hukuku haline gelen ve tüm AB üyeleri tarafından takip edilmesi gereken bir düzenleme olarak kabul edilmektedir. AB hukukunun bu entegrasyonu, sağlık verileri de dahil olmak üzere saklanan, değiş tokuş edilen ve kullanılan tüm kişisel bilgileri içermektedir. Sağlık verilerinin AB vatandaşları tarafından ele alınmasının sağlık uzmanlarına ve sağlık analistlerine maliyet ve fayda getireceği ifade edilmektedir (9). Teorik olarak GVKT, konumlarından bağımsız olarak kişisel verilerle ilgilenen tüm "kontrolörler" ve "işleyiciler" için geçerlidir

(70,71). Kontrolörlerin ve işleyicilerin adli görevleri benzerdir, ancak kontrolör hassas veri konularına birincil erişime sahiptir (61).

Verilerin işlenmesi rızaya bağlı olsa da kullanıcının her an rızasını geri alma hakkına sahip olması ve bu sürecin rıza verme kadar basit olması gerektiği ifade edilmektedir. Kontrolörler, veri işlenmesine yönelik onayın kanıtlanmasından sorumlu tutulmaktadır. Reşit olmayanlar için ebeveyn onayı gerekmektedir (72).

GVKT, bireylere aşağıdakiler de dâhil olmak üzere birçok önemli ayrıcalık sağlamaktadır:

- ❖ Verilerin toplandığını bilme hakkı,
- ❖ Bilgiye erişim hakkı,
- ❖ Verilerin doğru taşınabilirliği,
- ❖ Saklamaya itiraz etme hakkı,
- ❖ Yanlış verileri düzeltme hakkı,
- ❖ Unutulma hakkı,

GVKT kapsamında, AB Veri Koruma Yetkilileri, suçlulara brüt gelirin %4'üne kadar para cezası verebilmektedir. Bireyler, denetleyicilere ve işleyicilere karşı özel yasal haklara sahip olabilmektedir (73,74).

GVKT, sağlık verileri ve bilimsel çalışma için birçok kritere sahiptir. Genel olarak, sağlık ve bilimsel amaçlar için veri toplama, kullanma ve aktarmada veri koruma bölümünü daha düzenli hale getirir. “Hassas” kabul edilen sağlık ve kişisel genetik veriler için özel kurallar geçerlidir. Bu tür herhangi bir bilgiyi işlemeden önce birçok özel kılavuz ve koşula uyulması gerekmektedir. Bu koşullar;

- ❖ Bilinçsiz bir hastanın tıbbi acil durumu gibi rıza veremeyen hastalar için bir veri öznesinin güvence altına alınması,
- ❖ Bir doktorun diğer doktor veya sağlık hizmeti sağlayıcısından veriye ihtiyacı varmış gibi sağlık hizmeti sunmanın zorunlu olduğu durumlar,
- ❖ Sınır ötesi sağlık tehditlerinden korunma veya sağlık güvenliğini koruma gibi sağlık ihtiyaçlarını ele alma durumlarında veri sahibi tarafından "açık" rıza verildiğini içermektedir (75).

Türkiye'de yürürlüğe giren, 24.03.2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu ile kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esaslarının düzenlenmesi amaçlanmaktadır (10). Türk Ceza Kanunun 10. Bölümünde de 243-246. Maddelerinde Bilişim Suçlarına yer verilmektedir (63).

Kişisel Verilerin Korunması Kanunun 4. Maddesinin 2. Bendi

"*Kişisel verilerin işlenmesinde aşağıdaki ilkelere uyulması zorunludur:*

a) Hukuka ve dürüstlük kurallarına uygun olma,

b) Doğru ve gerektiğinde güncel olma,

c) Belirli, açık ve meşru amaçlar için işlenme,

ç) İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma,

d) İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme" hükümleriyle kişisel verilerin işlenmesine yönelik düzenleme yapıldığı görülmektedir (10).

Kişisel verilerin işlenmesinde ise belirli şartların sağlanması halinde;

"MADDE 5- (1) Kişisel veriler ilgili kişinin açık rızası olmaksızın işlenemez.

(2) Aşağıdaki şartlardan birinin varlığı hâlinde, ilgili kişinin açık rızası aranmaksızın kişisel verilerinin işlenmesi mümkündür:

a) Kanunlarda açıkça öngörülmesi,

b) Fiili imkânsızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin kendisinin ya da bir başkasının hayatı veya beden bütünlüğünün korunması için zorunlu olması,

c) Bir sözleşmenin kurulması veya ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesinin gerekli olması,

ç) Veri sorumlusunun hukuki yükümlülüğünü yerine getirebilmesi için zorunlu olması,

d) İlgili kişinin kendisi tarafından alenileştirilmiş olması,

e) Bir hakkın tesisi, kullanılması veya korunması için veri işlemenin zorunlu olması,

f) İlgili kişinin temel hak ve özgürlüklerine zarar vermemek kaydıyla, veri sorumlusunun meşru menfaatleri için veri işlenmesinin zorunlu olması," işlenebileceğine değinilmektedir (10).

Bilgi sistemlerinde bilgi sahibi, bilgi kullanıcısı veya bilgi sistemini yönetenlerden biri olunması hali, kişiye sorumluluk yüklemektedir. Bilgi güvenliği seviyesinin kullanıcılara bağlı olduğu belirtilmekte ve kullanıcıların farkındalığının bilgi güvenliğinin sağlanmasında oldukça kritik bir öneme sahip olduğu ifade edilmektedir (27).

Veri sorumlusu: Kişisel verilerin işleme amaçlarını ve vasıtalarını belirleyen, veri kayıt sisteminin kurulmasından ve yönetilmesinden sorumlu olan gerçek veya tüzel kişiyi ifade etmektedir (76).

Veri işleme konusunda veri güvenliğini sağlamak adına *KVKK*

"Madde 12- (1) Veri sorumlusu;

a) Kişisel verilerin hukuka aykırı olarak işlenmesini önlemek,

b) Kişisel verilere hukuka aykırı olarak erişilmesini önlemek,

c) Kişisel verilerin muhafazasını sağlamak, amacıyla uygun güvenlik düzeyini temin etmeye yönelik gerekli her türlü teknik ve idari tedbirleri almak zorundadır.

(2) Veri sorumlusu, kişisel verilerin kendi adına başka bir gerçek veya tüzel kişi tarafından işlenmesi hâlinde, birinci fıkrada belirtilen tedbirlerin alınması hususunda bu kişilerle birlikte müştereken sorumludur.

(3) Veri sorumlusu, kendi kurum veya kuruluşunda, bu Kanun hükümlerinin uygulanmasını sağlamak amacıyla gerekli denetimleri yapmak veya yaptırmak zorundadır.

(4) Veri sorumluları ile veri işleyen kişiler, öğrendikleri kişisel verileri bu Kanun hükümlerine aykırı olarak başkasına açıklayamaz ve işleme amacı dışında kullanamazlar. Bu yükümlülük görevden ayrılmalarından sonra da devam eder.

(5) İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da

uygun göreceği başka bir yöntemle ilan edebilir." hükümleri ile yükümlülüklerinin detaylı şekilde ele alındığı görülmektedir (10).

Veri Sorumlusu olan Sağlık Bakanlığı tarafından Kişisel Veri İşleme Envanteri oluşturulduğu; merkez ve taşra teşkilatları ile bünyelerinde faaliyet gösteren kamu sağlık hizmet sunucularının Kişisel Veri İşleme Envanteri doğrultusunda Veri Sorumluları Sicil Bilgi Sistemi (VERBİS) bildirimi yapıldığı belirtilmektedir (77). Veri sorumluları siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edilmesi halinde Kişisel Verileri Koruma Kurumunun Veri Sorumluları Sicili Hakkında Yönetmeliği kapsamında;

> *"MADDE 17 – (1) Veri sorumluları siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edenler hakkında Kanunun 18 inci maddesinin birinci fıkrasının (ç) bendinde yer alan idari para cezası uygulanır.*
> *(2) Veri sorumluları siciline kayıt ve bildirim yükümlülüğüne aykırı hareket edilmesi eyleminin, kamu kurum ve kuruluşları ile kamu kurumu niteliğindeki meslek kuruluşları bünyesinde işlenmesi hâlinde, Kurulun yapacağı bildirim üzerine, ilgili kamu kurum ve kuruluşunda görev yapan memurlar ve diğer kamu görevlileri ile kamu kurumu niteliğindeki meslek kuruluşlarında görev yapanlar hakkında disiplin hükümlerine göre işlem yapılır ve sonucu Kurula bildirilir."* hükmü doğrultusunda işlem tesis edilmesi gerekmektedir (76).

2.6. Bilgi Sistemleri

Günlük alışkanlıklarımızı etkileyen bilgi ve iletişim teknolojileri; aynı zamanda ticaretten eğitime, iletişimden bankacılığa kadar birçok alanda hayatı kolaylaştırmaktadır. Bilindik kavramların, elektronik sözcüğünün ilk harfi ile birleşmesiyle e-devlet, e-posta, e-imza, e-okul gibi yeni kavramlar oluşmaktadır. Dijital ortamda üretilip saklanan bilgilerin artması, bilgi güvenliği açısından birçok risk ve tehdidi de beraberinde getirmektedir (4).

Artık kurumların iş süreçlerinin büyük bir kısmında elektronik iletişim sistemleri ile bilgi kaynakları kullanılmaktadır. Bilgi teknolojilerini kullanarak iş süreçlerini hızlandırmak, kaliteyi arttırmak ve denetimi kolaylaştırarak kurumun toplam etkinliğini yükseltmek hedeflenmektedir (25). Sürekli değişim gösteren ve yenilenen bilgi sistemleri sebebiyle kurumlarda eğitim ihtiyacı oluşmaktadır (78).

Çünkü iletişim altyapısı ya da bilgi kaynaklarına erişimde oluşabilecek bir kesinti, iş süreçlerinin aksamasına, bu iş süreci kritik sistemlerden birinde oluşmuşsa, kurumsal güvenlik zafiyetlerinin oluşmasına, çalışanlar ve müşterilerin kuruma ve kurumun bilişim altyapısına duydukları güvenin olumsuz yönde etkilenmesine neden olacağı ifade edilmektedir (25). Bilgi kaynaklarına erişimlerde;

- Güvenli erişim seçeneklerini tercih etmemek,
- Hesap sahipleri tarafından genellikle zayıf parolalar kullanmak veya parolaları başka kişilerle paylaşıyor olmak,
- Birçok kurumda görev değişikliği ya da işten ayrılma durumunda personellerin kapatılmayan hesaplarıyla işlem yapmaya devam etmek,
- Bilgi kaynaklarına saldırı yapıldığında sorumluları ve olayların detaylarını tespit edememek gibi durumlarla sıklıkla karşılaşılmaktadır.

Bunlara ek olarak kamu kurumları tarafından yayınlanan birtakım listelerde kişilere özel detaylı bilgilerin yer alması ve bazı bilgilerin gereken zamandan önce paylaşılması vb. Türkiye'de yaşanmakta olan bilgi güvenliği olayları arasındadır. Özellikle yetkilendirme ve bilgi kaynaklarına erişim konusunda, çoğu kurumun büyük bir bilgi eksikliği olduğu anlaşılmakta, bilgi kaynaklarına dair tehditlerle karşılaşıldığında sorumluları tespit etmede yaşanan zorluk ve zayıflıklar nedeniyle bilgi kaynaklarının güvenliğinin istenilen düzeyde izlenemediği ve erişimlerin standartlar doğrultusunda uygun biçimde kaydedilemediği yönünde değerlendirilmektedir (25).

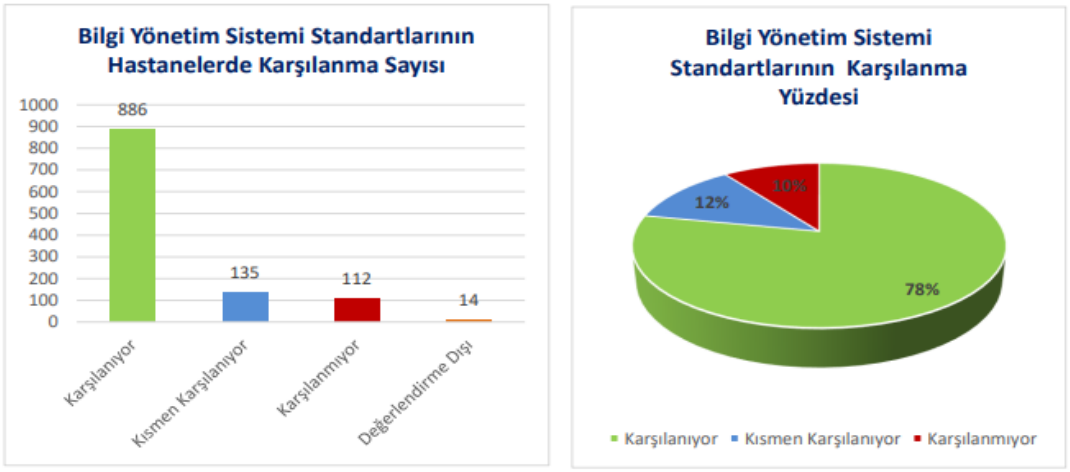
Teknolojinin ilerleme hızıyla bağlantılı olarak sağlıkta hizmet sunumunda kullanılan cihazlar da sürekli geliştirilmektedir. Buna bağlı olarak bu hizmeti veren kuruluşlarının bünyesinde barındırdıkları ekipmanların çağa ve teknolojiye uyumlu olarak değiştirilmeleri gerekliliği oluşmaktadır. Çünkü bu kuruluşların hizmet almak için gelen her bireyin hayatından mesul oldukları bilinmektedir (78). Bilgi teknolojisinin hızlı gelişimi, giderek daha uygun bilgi sistemi ve gelişmiş ve esnek bilgi ağı, bilgi çağında insan toplumunu destekleyen önemli bir sütun haline gelmiştir ve beraberindeki sorun bilgi güvenliğidir (79).

2.6.1. Bilgi Yönetimi

Bilginin, hangi şekilde olduğu (konuşulan bilgi, ses kayıtları, çizimler, video görüntüleri, tıbbi tahlil sonuçları vb.), hangi durumda bulunduğu (basılı veya elektronik ortamda) ya da bilgi transferinde hangi araç kullanıldığı (fax, bilgisayar ağları, posta vb.) fark etmeksizin korunması gerektiği belirtilmektedir (7).

Bilgi yönetimi, işletmeler ve ulusal ekonomilerin mevcut ve potansiyel rakiplerine kıyasla rekabet güçlerini artırması ve sürdürmesi için bilginin etkin bir biçimde tanımlanması, elde edilmesi ve kullanılmasını amaçlayan stratejiler veya süreçler olarak ifade edilebilir (80).

Kamera sistemleri, güç kaynakları ve telefon santrallerinin doğal afetler sebebiyle arızalanması; online alışveriş, e-posta, internet bankacılığı ve donanım kaynaklı sorunlar; bilgisayar virüsleri, erişim yetkilerinin kötüye kullanımı gibi dijital verilerin güvenliğini tehdit etmekte olan birçok faktör vardır (4). Bilişim teknolojilerinin etkin kullanılabilmesi için, bilgi güvenliği ilkelerine dikkat edilmesi ve güvenlik ihlallerine ihtimal bile vermeden sürecin işleyişinin sağlanması gerekmektedir. Karmaşık yapıya sahip olan hastanelerin tüm çalışanlarının bu bilgi yönetim sistemlerine sahip çıkması ve bu bilgi yönetim sistemlerini başarı ile kullanabilmesi kilit noktadır. Elbette ki bu son derece önemlidir çünkü işletmenin kaliteli hizmet sunabilmesi ve aynı zamanda rekabet avantajını da elinde bulundurarak sektörde öncü bir sağlık kuruluşu olarak varlığını devam ettirebilmesi bu kilit noktasının başarısına bağlı bulunmaktadır (42). Bu kapsamda, 6 Ağustos 2013 tarih ve 28730 sayılı Sağlık Hizmeti Kalitesinin Geliştirilmesi ve Değerlendirilmesine Dair Yönetmelik ile Bilgi Yönetimi kalite standartları arasına dâhil edildiği görülmektedir (81).



Şekil 2.1. Bilgi Yönetim Sistemi Standartlarının Hastanelerde Karşılanma Sayısı ve Karşılanma Düzeyi (82).

Şekil 2.1.'de yer alan 2017 yılına ait raporda, Bilgi Yönetim Sistemi Standartlarının Hastanelerde Karşılanma Sayısı ve Karşılanma Düzeyine bakıldığında %10 oranında standartların karşılanmadığı %12 oranında ise kısmen karşılandığı görülmektedir. "Sunucu odalarının güvenliğinin sağlanması" %55.11 ve "Hastane Bilgi Yönetim Sistemindeki verilerin yedeklenmesine yönelik düzenleme" %71.45 olarak yer almaktadır (82). Bir ülkenin hastane altyapısının siber güvenlik açığı, tüm hastanelerin güvenlik açıklarından etkilendiği görüşü (83) ile Bilgi Yönetim Sistemlerinde sağlıkta kalite standartların karşılanması hem hasta mahremiyeti açısından hem de sunulan hizmet kalitesi açısından oldukça önemlidir.

2.6.2. Bilgi Güvenliği

Bilgi, iş sürekliliğini sağlama konusunda bir kurumun en önemli değerlerinden biri olarak belirtilmektedir. Kaybedilmesi halinde birçok varlığın telafisi mümkün olsa da kaybedilen bilginin parasal bir karşılığı bulunmamaktadır. Bu yüzden gelişen ve değişen günümüz şartlarında bilginin önemi ve korunması zorunluluğu da giderek artmaktadır. Bilgi; yazıyla elektronik ortamlarda, sözle, çalışanların hafızalarında ve daha pek çok şekilde saklanabilir ve kullanılabilir. Teknolojik gelişmelerden dolayı bu kullanım şekillerinin bir kısmı zaman içinde kullanılmaz hale gelebilir veya değişebilir. Bahsedilen bu gelişim ve değişimden ötürü sürekli olarak bilginin

güvenliğinin sorgulamak ve kontrol etmek gerekmektedir (84). Bilgi güvenliğinin sağlanması, bilginin gizliliğinin, bütünlüğünün, kullanılabilirliğinin korunmasından oluşmaktadır (79,84).

Bilgi güvenliği davranışı, kurumsal kültürün bir uzantısı olarak bilgi güvenliği kültürünü teşvik eden bir örgütsel davranış haline gelmek üzere gelişir. Box ve ark. (2013) kullanıcı güvenlik davranışını kontrol eden faktörleri ve sonuçlarını ele almış ve kurumsal kültürü değiştiren ve bilgi güvenliği politikalarıyla güçlendirilen bir bilgi güvenliği farkındalık kültürünün gelişimini gözden geçirmiştir (85). Sağlık hizmeti sağlayıcıları tarafından sağlanan hasta bakımının iyileştirilmesi de dâhil olmak üzere kuruluşun güvenlik kültürünün geliştirilmesi ile önemli güvenlik kazanımları elde edilmektedir (86,87). Bir bilgi güvenliği kültürü kurmanın amacı, çalışanların ve paydaşların kuruluşun bilgi güvenliği politikalarına bağlılığını teşvik etmektir (88). Bilgi güvenliği kültürü, politika ve kontrollere uyumu sağlamak için bilgi varlıklarını korumak ve güvenlik davranışını etkilemek amacıyla kurumsal sistemler ve süreçlerle etkileşime girerken çalışanların veya paydaşların algıları, tutumları, varsayımları, inançları, değerleri ve bilgileri olarak tanımlanabilir (86,89). Bilgi güvenliği kültürü bir kurumsal kültürün bir uzantısı olduğu için (85,86), beklenen kültürü yerleştirmek her bir kurumun birçok faktörden etkilenen koşullarına bağlıdır; bu nedenle, bilgi güvenliği kültürünün başarısına katkıda bulunabilecek faktörleri anlamak hayati önem taşımaktadır (29). Hastanelerde kalite odaklı bir yönetim anlayışının varlığının, kuruluş çalışanlarının bilgi güvenliği kültür düzeyini yükselteceği düşünülmektedir (78).

Bilgi güvenliğinin temel amacı, kurumsal güvenlikle ilgili farklı tehditlerin ve kurumsal zayıflıkların etkilerini ortadan kaldırmak veya en aza indirmek için uygun kontrol önlemlerinin uygulanmasıdır (90). Bilgi güvenliğinin organizasyonlarda etkin ve ekonomik olarak nasıl uygulanabileceği sorusunun cevabı Bilgi Güvenliği Risk Yönetimidir (91). Zarei ve ark. (2016) tarafından, sağlık bilgi sistemlerinde bilgi güvenliği risk yönetimini değerlendirmek amacıyla İran'da 551 hastane ile yapılan çalışmada, hastanelerin bilgi güvenliği politikaları ve bilgi güvenliği risk yönetimini takip etmedikleri sonucuna ulaşıldığı görülmektedir (90).

Bilgi güvenliği politikaları, kurumsal bilgi güvenliğinin amaç ve hedeflerini içerecek şekilde, çalışanların görev ve sorumluluklarıyla birlikte gerekli görülen yönetimsel denetim mekanizmalarının da belirlendiği, kurumsal yapı ve kültüre uygun kurallar bütünü olarak hazırlanmaktadır (25). Kurumsal bilgi güvenliği kültürü oluşturulmasında, yönetimsel destek ile birlikte belli bir zaman, eğitim ve özümseme gerektiği vurgulanmaktadır (25). Nitekim sağlık bilgi güvenliği eğitiminin hemşirelerin konuyla ilgili farkındalığını arttırdığı ve uygulama üzerinde olumlu bir etkisi olduğu belirtilmektedir (85, 92). Bilgi güvenliği yönetim sisteminin çalışanlar tarafından sahiplenilmesi ve bilgi güvenliği kültürünün kuruma yerleştirilebilmesi hususunda yöneticiler tarafından, sistemin temel gereklilikleri yerine getirilirken organizasyonel ve sektörel değişkenlere de gereken önem verilmesi gerekmektedir (25).

Bilgi teknolojilerinde yaşanan gelişmeler, bilgi güvenliğini sağlamayı daha kapsamlı ve karmaşık hale getirmektedir (93). Bunun yanı sıra bilginin gizliliği, bütünlüğü ve ulaşılabilirliğine dair güven ortamı oluşturulması stratejik bir öneme sahiptir (84). Bu amaçla KVKK ve TSE 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardı dikkate alınarak Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü tarafından "Bilgi Güvenliği Politikaları Kılavuzu" hazırlandığı, oluşturulan politikalar ile siber güvenlik ve kişisel veri güvenliği de dâhil olmak üzere etkin bir BGYS tesis edilmesi planlandığı görülmektedir (93). Bilgi Güvenliği Yönetim Sistemi (BGYS): Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak üzere; sistemli, kuralları koyulmuş, planlı, yönetilebilir, sürdürülebilir, dokümante edilmiş, kurumun yönetimince kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütününü,

Bütünlük: Varlıkların doğruluğunu ve tamlığını koruma özelliğini,

Erişilebilirlik: Yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliğini,

Gizlilik: Bilginin yetkisiz kişiler, varlıklar ya da süreçlere kullanılabilir yapılmama ya da açıklanmama özelliğini ifade etmektedir (94).

Bilgi Güvenliği Yönetim Sistemi dokümantasyonu gerekliliklerine aykırı davranılması durumunda 657 Sayılı Devlet Memurları Kanununa tabi olanlar aynı kanunun 125. maddesinde sayılan hükümlere göre değerlendirilecek olup 657 Sayılı

Devlet Memurları Kanununun dışında kalan çalışanlar ile ilgili olarak (Danışmanlar, Firma Personelleri) sözleşmelerinde belirtilen özel hükümlere yoksa genel hukuk kuralları çerçevesinde hareket edilecektir (95). Hastane bilgi sistemlerine erişimde, sağlık çalışanlarının kimliklerinin doğrulanması yöntemine başvurulması bilgi güvenliğini sağlama açısından önemlidir. Bu sayede sadece yetkili kişiler bilgilere ulaşabilir konumda olmaktadırlar (78).

2.7. Elektronik Sağlık Kayıtları

Kişisel Sağlık Kaydı, bir bireyin "sahip olduğu" ve kontrol ettiği elektronik tıbbi kayıtların veya elektronik sağlık kayıtlarının bir parçası olarak tanımlanmaktadır. Tıbbi kayıtlar, laboratuvar sonuçları, fiziksel değerlendirme, tıbbi geçmiş, ilaç geçmişi, fizyolojik ölçümler, diyet kayıtları, egzersiz kayıtları vb. içermektedir (96).

Günlük olarak büyük miktarda klinik veri üretilir. Bilgi ve iletişim teknolojilerindeki ilerlemeler, sağlık hizmeti sağlayıcılarının bunları dijital olarak saklamasına ve elektronik sağlık kaydı olarak anılmasına olanak sağlamaktadır. Bu kayıtlar doktorlar, hemşireler ve sağlık hizmeti sağlayıcıları gibi çeşitli paydaşlarla paylaşılır. Bu sağlık kayıtlarına ayrıca devlet kurumları, eczaneler, laboratuvarlar, sigorta acenteleri rıza ile veya bir süre rıza olmaksızın erişilebilir (9).

Kişisel sağlık kaydında, bağlı, bağımsız ve entegre kişisel sağlık kaydı olmak üzere üç yaygın türden bahsedilmektedir. Bağlı kişisel sağlık kaydı, hasta tarafından erişilebilen ve bir şekilde bir kuruluşun sistemine bağlı olan bir sistemdir. Bu sistemler, sağlık pratisyenlerinin girdileri de dâhil olmak üzere çeşitli avantajlar sunduğu belirtilmektedir. Ancak, bu normalde kişisel sağlık kayıtlarına sahip olan ve onunla ilişkili olan kuruluş içinde uygulama yapmakla sınırlıdır. Bağımsız kişisel sağlık kaydının ise iki olası formu vardır. İlk formda, hasta verileri, kişisel sağlık kayıtları akıllı kartlarında depolanır. Bazı taşınabilir medya cihazları vardır ve yazılım tarafından desteklenen akıllı karttır. Verileri görüntülemek, değiştirmek veya düzenlemek için akıllı karta bilgisayar tarafından erişilebilir. İkinci formda, birleştirici kişisel sağlık kayıtları genellikle merkezi internet portalları biçimindedir. Bu formda hasta diğer kaynaklardan veri toplayabilir ve istediği verileri de girebilir. Entegre kişisel sağlık kaydı ise sistem tarafından yönlendirilir ve çeşitli kaynaklardan hasta verilerini tek bir görünümde toplar ve sunar. Entegre sistemler karmaşıktır ancak

karmaşıklık, kullanılabilirlik ve esneklik sağlar (21). Elektronik sağlık kayıtları, diğer alanlardaki veri setlerinden farklı özellikler gösterir. Bu özellikler:

- ❖ Veriler yaşamsal öneme sahiptir.
- ❖ Hatalı dahi olsa verilerin silinmesi yasaktır.
- ❖ Bir kayıtta birden fazla kişi (meslek üyesi) tarafından girilmiş veri vardır.
- ❖ Kullanıcılar kayıtlara erişebilirler ancak yetkilerinin bulunmadığı alanlarda değişiklik yapamazlar.
- ❖ Sisteme giriş izni, ihtiyaç ve bakım ile bağlantılı özel görev/uygulamalara dayalıdır.
- ❖ Verilerin sistem içinden ya da dışından elde edilebilmesi, ulaşılabilmesi ihtimali bulunmaktadır.
- ❖ Uzun süreli, karmaşık ve büyük kayıtlar için geniş bir kapasiteye ihtiyaç duyulmaktadır.
- ❖ Öykü şeklindeki verilerde, bilgisayar kullanıcıları kodlama sistemi kullanır (13).

Elektronik sağlık kaydı verileri dispanserler, hastaneler, eczaneler, teşhis laboratuvarları vb. gibi birbirine bağlı çeşitli siteler arasında paylaşılmaktadır. Verilerin çok sayıda yerde paylaşılması, bakım, destek, güvenlik, dakiklik ve izleme ihtiyaçları gibi temel ihtiyaçları belirleyerek esnek ve etkili hasta tedavisi sağlamaktadır. Sağlık profesyonellerini (doktorlar, hemşireler vb.) semptomlara dayalı doğru kararlar verme de desteklemektedir (97,98).

Kurumun verimliliğini arttırmada, insan kaynaklı hataların azaltılmasında, maliyetlerin düşürülmesinde, hasta memnuniyetini sağlamada bilgi ve teknolojinin getirdiklerinin etkili olduğu görülmektedir (15). Elektronik sağlık kaydı (EKS), sağlık hizmeti alanların, aldıkları hizmet kayıtlarının, şimdi, geçmişte, gelecekte, her türlü idari ve tıbbi verilerinin elektronik sistemler kullanılarak kaydedilmesi, saklanması, iletilen, ulaşılan, bağlantı kurulan ve işlenen her türlü bilgi olarak tanımlanabilir. Elektronik sağlık kayıtları; insanların kişiye özel, mahrem ve değerli bilgilerinden oluşmaktadır (99).

Dijital algoritmaları ve dijital kayıtları içeren dijital sağlık teknolojisi, sağlık hizmetlerinin sunulma şeklini değiştirmektedir. Bakımevlerinde çalışan hemşireler ile yapılan bir çalışmada katılımcı hemşireler, personelin zamanını boşa çıkarma, bakım kalitesini iyileştirme ve personelin işe alınması ve tutulması üzerinde olumlu etkileri olan dijital sağlık teknolojisi yeniliklerinin bakımevlerinde etkin uygulanması gerektiğini belirtmişlerdir (34).

Sağlık hizmeti sunumu hasta merkezli hizmetlere doğru değiştikçe, kişisel sağlık kayıtları kullanıcılar ve sağlayıcılar için vazgeçilmez bir platform haline gelmektedir. Tayvan Hükümeti'nin web tabanlı bir elektronik tıbbi kayıt deposu olan "My health bank" uygulaması üzerine Rau ve ark. tarafından 2017 yılında, web tabanlı davetiye ile Facebook üzerinden anket dağıtılmış ve bu anketin sonucunda;

- Karmaşık işlevler yerine insanlar sadece tıbbi ziyaretlerini, sağlık muayenelerini ve yaşam davranış kayıtlarını entegre etmelerini ve yönetmelerini sağlayacak bir platforma sahip olmak istediklerini;
- Kişisel sağlık kayıtlarının başkalarıyla paylaşılıp paylaşılmadığının umurlarında olmadığını ve
- Katılımcıların çoğunun, sistem güvenliği tasarımının önemli olmadığını düşünmekte olduğunu, aynı zamanda mevcut güvenlik tasarımından memnun hissetmediklerini belirtmişlerdir (96).

Norveç'te kâğıt bazlı tıbbi kayıtların tarandığı ve ortadan kaldırıldığı bir hastanede, hastane bilgi sisteminin performansı ve kullanıcı memnuniyeti üzerine yapılan çalışmaya göre; tıbbi sekreterlerin, hastane bilgi sistemini hemşirelerden ve doktorlardan çok daha fazla kullandığı ve elektronik hastane bilgi sisteminin işlerini büyük ölçüde basitleştirdiği belirtilmektedir. Elektronik ortama taşınan verilerin öncelikle tıbbi sekreterlere kolaylık sağlasa da hemşire ve doktorların çalışmalarını da kolaylaştırdığı dolayısıyla kullanıcı memnuniyeti konusunda olumlu yanıtlar alındığı ifade edilmektedir (100).

2.7.1. Elektronik Sağlık Kayıtlarında Hemşirenin Rolü

Sağlık profesyonelleri arasında, sağlık sisteminde ve hasta bakımında hemşireler ve doktorlar en önemli role sahiptir. Sayısal olarak çoğunlukta olan

hemşireler, hastaya bakım verme, bakım gereksinimlerini belirleme, uygulamaları planlama, ne zaman, nerede, hangi malzemenin kullanılacağına karar verme gibi durumlarda, sağlık teknolojilerini yoğun şekilde kullanmaktadır. Hastaların verilerini toplayan, topladıkları verileri elektronik ortama aktaran hemşirelerin teknolojiyi kabul ve kullanımı oldukça önemlidir (101). Birleşik Arap Emirlikleri'nde yapılan bir çalışmada, hemşirelerin elektronik sağlık kayıtlarındaki hastaların verileri üzerinde kontrol sahibi oldukları, kurumların hasta bilgilerinde hasta mahremiyetine dikkat ettikleri ve gerekmedikçe verileri açıklamadıkları sonucuna ulaşıldığı görülmektedir. (18).

Bir meslek olarak hemşirelik, hasta bakımı ve sağlık hizmetleri zincirinde önemli bir halkadır. Çünkü hemşireler genellikle hasta bakımı ve sağlık hizmetlerinin sunumunda hem koordinatör hem de bakım verici olarak yer almaktadır (102). Hemşireler hastanın fiziksel, psikolojik ve sosyal ihtiyaçları da dâhil olmak üzere hastayla ilgilenir. Sağlık profesyonelleri arasında hemşireler sayısal olarak çoğunlukta olmaları ve çalışmalarının gereği olarak, elektronik sağlık kayıt sistemleriyle en çok etkileşime de onlar girmektedir. Hemşirelerin elektronik sağlık kayıtlarında birçok yetkisi bulunmaktadır. Hemşirelik tanıları koyarlar (103), doktor istemlerini kontrol ederler (104), hemşirelik bakım planları yazarlar (105), yaşamsal bulguları kaydederler ve diğer rollerinin yanı sıra bazen doktor istemlerini yazıya dökerler (106). Hasta bakımında aktif rolü olan hemşireler elektronik sağlık kayıtlarında; laboratuvar, radyoloji ve diğer test sonuçları, mevcut ve geçmiş ilaçları görüntüleme, ilaçların son kullanım tarihleri, ilaç etkileşimleri, ilaç alerjileri, normal aralığın dışındaki test sonuçları, klinik kılavuzlar, laboratuvar, radyoloji ve eczane istemleri (barkodlandırma), hasta ile ilgili tıbbi sorunların listelenmesi, hastaya özel alerjilerin tanımlanması, hasta taburculuğu talimatlarının belgelendirilmesi ve hasta sevkini yönetme gibi pek çok işlemde yetki sahibidir (107).

Top ve ark. (2011) tarafından yapılan çalışmada, hemşirelerin, elektronik sağlık kayıtlarının hemşire iş akışını ve performansını birçok yönden etkilediğini algıladıkları belirtilmektedir. Hemşireler, genel olarak, elektronik sağlık kayıtlarının hemşirelik işlerini kolaylaştırdığını, hasta bakımı ile ilgili kararları verme yeteneklerini geliştirdiğini, hasta bilgilerine daha iyi erişim sağlamalarına ve hasta bakım ekibinin diğer üyeleriyle iletişim kurmak için daha az zaman harcamalarına izin

verdiğini düşünmektedir (35). Elektronik sağlık kayıt sistemleri, özellikle hemşirelerin hasta bakım planı oluşturmasında çeşitli yararlar sağlamaktadır. Bu yararlarından bazıları şu şekilde sıralanmaktadır (35,108):

- Hastaya ait bilgiler tek bir numara ile ilişkilendirilir,
- Sağlık kurumundaki elektronik sağlık kayıt sistemine girilen hasta bilgilerine, sağlık kurumunun her yerinden erişimini mümkün kılar,
- Hastaların sağlık bakım planının yazılmasına ilişkin (kağıt, dosya vb.) yükü azaltır aynı zamanda hataları en aza indirerek veri kaybını önlemektedir,
- Elektronik sağlık kayıtları üzerinden hasta verilerini girerek, hemşirelerin klinikte hastalarla ilgili kolay karar vermelerine yardımcı olur,
- Bilgisayar ortamına aktarılan formlarla hasta bakım planlarını standart hale getirmektedir,
- Sağlık kurumunda çalışan tüm personel arasındaki bilgilerin doğru aktarılmasına yardımcı olur,
- Hasta için uygulanan sağlık hizmetleri sunumunun doğru kaydedilmesine ve ücretlendirilmesine yardımcı olur,
- Veri tabanı oluşturarak, hasta kayıtlarının doğru ve düzenli olarak tutulmasını sağlar. Böylelikle istatistiksel değerlendirmeler ve araştırmalar için veri oluşturur,
- Hemşirelere yaptıkları işle ilgili olarak zorunlu hatırlatmalarda bulunur. Ayrıca yapılan hasta takibi için bir rehber ve bir öğrenme aracı olarak kullanılır (33).

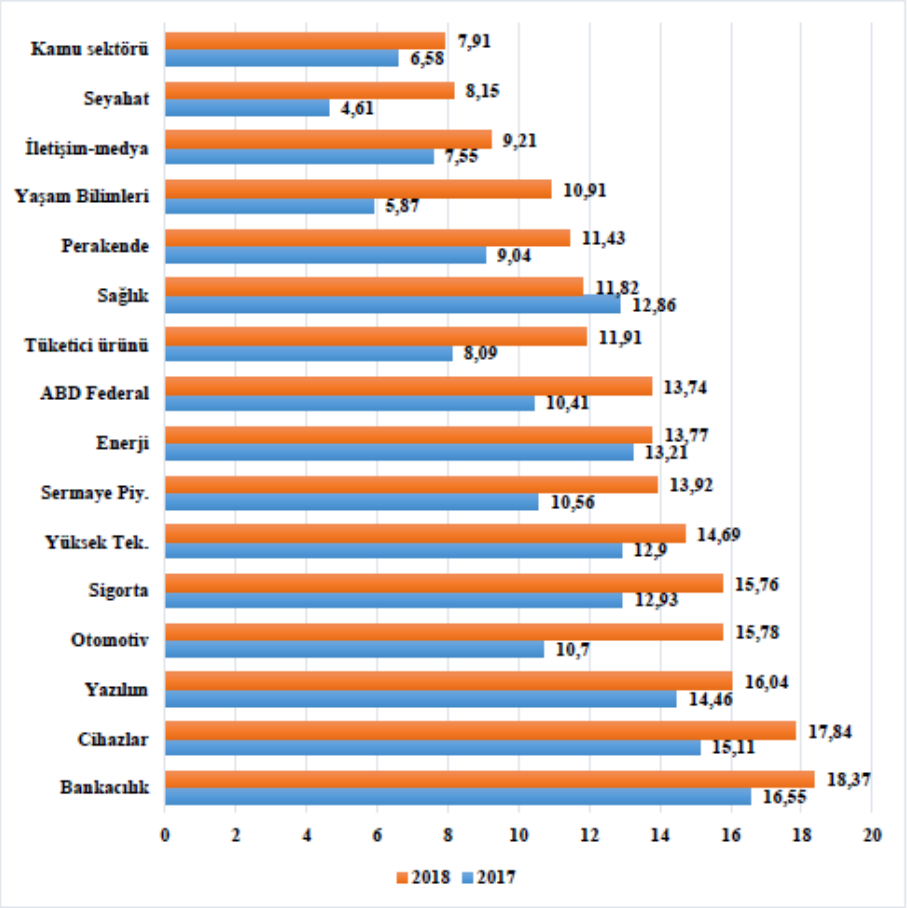
Elektronik sağlık kayıtları; kişisel sağlık kayıtları, test sonuçları, anamnez, muayene, doktor istemi, bakım planı ve epikriz gibi tıbbi bilgilerin yanı sıra hastaya ilişkin kullanılan fatura ve malzemeler gibi tıbbi olmayan verileri de içermektedir (108). Şanlıurfa'da kamu ve özel hastanelerde çalışan hemşirelerin elektronik tıbbi kayıtlara ilişkin görüşlerini belirlemek için yapılan bir çalışmada; elektronik tıbbi kayıt kullanımı, kalitesi ve tatmini boyutlarında özel hastanede çalışan hemşirelerin 3 boyutta da daha yüksek değerlendirmede bulundukları belirtilmektedir. Özel hastanelerde çalışan hemşirelerin, kamu hastanelerinde çalışan hemşirelere göre kayıt tutma konusunda daha dikkatli oldukları sonucuna ulaşıldığı belirtilmektedir. Bu

sonucun, özel hastanelerde çalışan hemşirelerin, faturalandırmadan dolayı tıbbi kayıt kullanımına daha çok özen göstermelerinden kaynaklandığı düşünülmektedir (33).

2.7.2. Elektronik Sağlık Kayıtlarında Bilgi Güvenliği

Veri gözetleme ve kimlik hırsızlığı çağında, elektronik sağlık kayıtlarında güvenlik ve mahremiyet endişesi olması oldukça mümkündür (21). Hastane masaüstü bilgisayarları, özellikle gizlilikteki olası bir ihlal kaynağı olarak görülmektedir. Masaüstü ekranlarında depolanan (devir teslim, sevk mektupları, personel hastalık izni listeleri, denetimler ve hemşirelik raporları dâhil) hasta veya personelin gizli bilgilerine kolayca erişilebilmektedir (109).

Bilgi Güvenlik endişelerini gidermek ve yüksek kaliteli sağlık hizmetleri sunmak için, belirli bir düzenlemeye uygun olarak tanımlanması ve uygulanması gereken belirli politikalar ve yönetmelikler gereklidir. Sağlık kuruluşları tarafından uygun sistem dokümantasyonu sağlanması gerekmektedir (110). T.C. Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi'nin 4. Maddesinin f) bendinde "*Bilgi Güvenliği: Bilgi ve bilgi işleme tesislerinin emniyetli ve güvenilir olarak kullanılabilmesi, bütünlüğünün ve gizliliğinin muhafazası ve yetkisiz şahısların bilgiye ulaşmaları halinde tespit edilmelerine yönelik tedbirlerin tümü"* olarak yer almaktadır (111).



Şekil 2.2. Sektörlere göre 2017-2018 yılları ortalama siber suç maliyeti (milyon $) (6).

Şekil 2.2.'de sektörlere göre yıllık ortalama siber suçların maliyetleri yer almaktadır. Siber saldırılar nedeniyle en yüksek maliyetin bankacılık, en az maliyete sahip saldırıların ise kamu sektöründe olduğu görülmektedir. 2017 ve 2018 yıllarına bakıldığında sağlık sektörüne yapılan siber saldırıların maliyetlerinde bir azalma olması ilgi çekici bir durumdur. Sağlık sektöründe, bilimsel gelişmeler ve teknolojiye daha hızlı uyum sağlanması dolayısıyla, siber güvenlik açısından alınması gereken önlemlere hız verildiği anlaşılmaktadır (6).

Doktorlar ve hemşireler gibi hastaların takip ve tedavisindeki rolü dolayısıyla elektronik sağlık kayıtlarına erişmesi gereken klinik kullanıcılar için, tedavi sağlamak ve klinik kararları verebilmek açısından, hasta bilgilerinin erişilebilirliği çok önemlidir ve sürekli bir gereklilik arz etmektedir (25,112). Kullanıcılar, gizlilik koruma politikalarını ihlal etse bile gerekli bilgilere sürekli olarak erişmek için bazen parolaları

veya bilgisayar ekranlarını birbirleriyle paylaşarak hesaplarına da ortak erişim sağlamaktadırlar. Hastanelerde çalışan çoğu bilgi işlem personelinin sağlık alanında eğitimli olmadığı belirtilmektedir. Bu yüzden hastanedeki sağlık personelinin çalışma uygulamalarının yönü, bilgi işlem personelinin deneyimi veya bilgisinin ötesindedir. Kullanıcılar, elektronik sağlık kayıtları sınırlamalarını gidermek için gizlilikten ödün vermeyen geçici çözümleri kullanmaktadır. Bilgi işlem personelinin, elektronik sağlık kayıtları kullanıcılarının gizlilik yönetimi uygulamalarını anlamaları sınırlıdır (112).

Bilgi güvenliğine ilişkin yaşanan veri ihlallerine rağmen insanlar, kişisel sağlık verilerinin güvenli olarak sağlık sistemlerinde korunduğunu düşünmektedir. Duyulan güven düzeyi sıralamasına bakıldığında 1. sırada sağlık sistemlerinin yer aldığı, sonrasında işverenler ve ardından bankaların veri tabanlarının geldiği görülmektedir. İnsanlar verilerini paylaşma konusunda en çok sigorta şirketlerine karşı şüphe duyduğu belirtilmektedir (16).

Kanada'da, hasta güvenliğini artırmak amacıyla ilaç yan etki (advers) bildirimlerini iletmede bilgi ve iletişim teknolojilerini kullanırken hastaların ve klinisyenlerin veri koruma hakkındaki görüşlerini incelemek amacıyla bir çalışma yapıldığı görülmektedir. Katılımcıların gizlilik tercihlerine bakıldığında, klinisyenler arasında bilgi paylaşımını uygun buldukları anlaşılmaktadır. Ancak katılımcılar, tedavi sürecinde yer almayan (örneğin sigorta şirketleri) veya farklı kiniklerde çalışıp hastanın bakımında rolü olmayanlar ile bilgilerinin paylaşılması ve bilgilerine erişilmesi konusunda dikkatli olduklarını belirtmişlerdir (68).

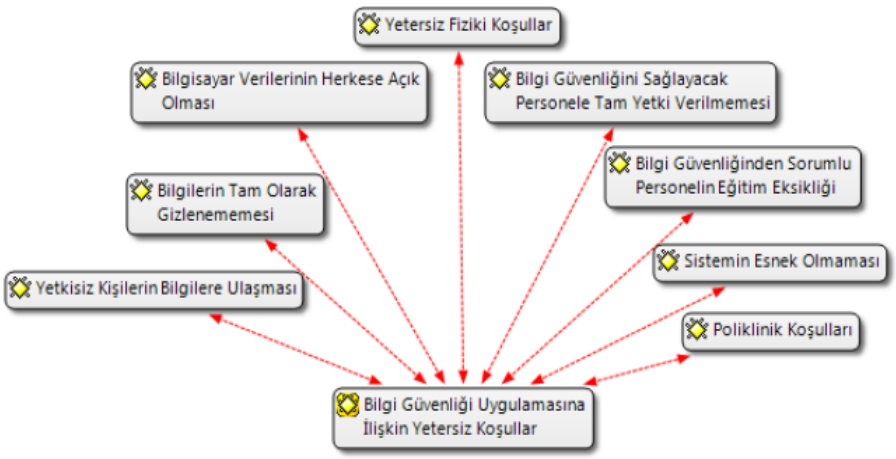
2.7.3. Elektronik Sağlık Kayıtlarında Bilgi Güvenliğini Etkileyen Faktörler

Sağlık personelinin, kuruluşun hayati bilgilerini korumak ve sistemi acemi bir hatayla tehlikeye atmaktan kaçınmak için rollerinin farkında olması önemlidir. Sağlık kuruluşu, çalışanlarının bilgi sistemden anlama düzeylerini artırmak için bir dizi uygun eğitim yapmaktan sorumludur. Kuruluş içindeki bir kişinin yaptığı;

- Virüs bulaşmış veya kötü amaçlı yazılım içeren bir flash bellek getirmek,
- Sağlık bilgisayarlarından birinde kötü amaçlı yazılım veya virüs içeren bir e-postanın açılması,

❖ Yetkisiz birinin niyetini bilmeden kısıtlı bir alana girmesine izin vermek gibi basit bir hata, tüm sistemi tehlikeye atabilir (21).

Hastanelerde kullanılan bilişim sistemlerindeki yazılım hatalarının, süreci zorlaştırdığı bilinmektedir. Bu yüzden hasta verileri üzerinde istenmeyen işlemlerin yapılması ihtimal dâhilindedir (78). Şifreleme ve parola koruması, kişisel sağlık kayıtlarının güvenliğini ve gizliliğini garanti etmenin en iyi yoludur, ancak kötü sistemler veya kötü seçilmiş parolalar söz konusu olduğunda tatmin edici bir sonuç mümkün olmamaktadır (21). Bilgi güvenliği yönetimi sürecinde planlama yapılırken kurumsal ve sektörel dinamikler göz önüne alınmalıdır. Örnek olarak, sağlık sektöründe yapılan çalışmalarda, sağlık çalışanlarının; değişime karşı korku, kuşku, inanç, motivasyon, kişisel gelişim isteği gibi sebeplerle kurulmaya çalışılan yeni sistemlere karşı direnç gösterdikleri belirtilmektedir. Bununla beraber, sağlık sektöründe bilgi güvenliğine ilişkin çalışmalarda, hastanelerde sağlık personelinin otomasyon sistemlerine erişim şifrelerini sıklıkla diğer çalışanlar ile paylaştığı, bunun da işlemleri aslında kimin yaptığının bulunmasını zorlaştırdığı ortaya koyulmaktadır (25,113).



Şekil 2.3. Bilgi güvenliği uygulamasında yetersiz koşullar (41).

Baran ve ark. (2019) tarafından yapılan çalışmada katılımcıların Bilgi Güvenliği Uygulamasında Yetersiz Koşullara İlişkin Görüşlerine ilişkin Şekil 2.3.'teki gruplandırmada; yetersiz fiziki koşullara, bilgi güvenliğinden sorumlu personelin eğitim eksikliğine, bilgilerin yeterince gizlenemediğine ve yetkisiz kişilerin

erişebildiklerine yer verilmiştir. Ayrıca, bazı durumlarda, hastaların başka birinin kimlik bilgileri ile muayene olması durumunun yaşandığı belirtilmektedir (41).

Bilgi Güvenlik sistemi kurulur kurulmaz denetim işlevi bir zorunluluktur. Yöneticilerin ve kullanıcıların kişisel sağlık kaydı verilerine erişim listesini gözden geçirebilmeleri için denetim gereklidir. Bu şekilde herhangi bir yasa dışı veya yetkisiz ihlal kolayca tespit edilebilir ve buna göre işlem yapılabilir. Mahremiyet açısından unutulmaması gereken asıl nokta ise hastaların, bir kişisel sağlık kaydı sistemi içinde bulunan veya bu sistem tarafından erişilebilen verilerin, hak sahibi olduğu vurgulanmaktadır. Böyle bir sistemde, veri sahibi, verilerin herhangi birine veya tümüne erişime izin verme veya reddetme hakkına sahip olduğu bilinmektedir (21).

İdeal olarak, elektronik sağlık kayıtları gibi teknolojiler, hasta bakımını iyileştirecek araçlar olarak kullanılmaktadır. Ancak, teknolojinin ve içinde depolanan verilerin her zaman doğru olmadığını bilmek önemlidir. Örneğin, bir hastanın durumuyla ilgili yanlış bilgiler, kullanıcı hatası da dâhil olmak üzere çeşitli nedenlerle elektronik sağlık kayıt sistemine girilebilir. Bu hatalı bilgiye “dirty data” yani "kirli veri" denmektedir (37).

2.7.4. Sağlık Çalışanlarının Bilgi Güvenliği Kültürü

Sağlık bilgi güvenliği farkındalığının geliştirilmesi için;

- Genel bilgi güvenliği farkındalığı,
- Sağlık bilgi güvenliği yasa ve yönetmelikleri farkındalığı
- Ceza türleri ve sağlık bilgi güvenliği ihlalleri farkındalığı şeklindeki üç öğrenme bileşeni oldukça önemlidir (36).

Tıbbi mümessiller, hastalar, doktorlar ve tıbbi asistanlar gibi sağlık bilgisi alışverişinde yer alan tüm paydaşların, sağlık bakım uygulamalarını etkileyen önemli rolleri olduğu için aynı güvenlik seviyesini izlemeleri önemlidir (21). Sağlık hizmeti sunumunda çalışanlar içinde hastalarla en çok karşılaşan ve en fazla paylaşımı olanlar hemşirelerdir. Hemşireler, yetiştikleri kültürün dışındaki yerlerde çalışmakta veya değişik inanç ve tutuma sahip kişilere bütüncül hemşirelik bakımının gereği olarak hizmet vermektedir (114). Hemşireler birçok yönden hastanın yaşamı üzerinde

etkilidir ve güvenli hemşirelik bakımı sağlamak için politika ve prosedürlere uyulması gerekmektedir (37).

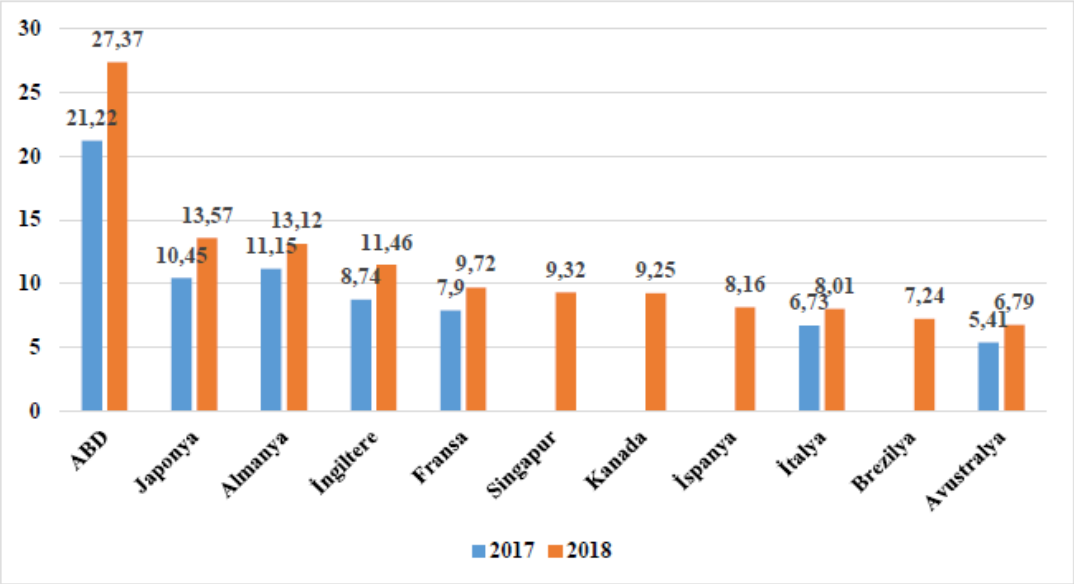
Günümüz dijital dünyasında, hasta verilerinin ve sistemlerinin kasıtlı olarak kurcalanması riskinin de farkında olmak gerekmektedir. Yeni bir kavram olarak karşımıza çıkan bilişim hemşirelerinin, veri ve sistemlerin bütünlüğü ve güvenliği ile ilgili olası tehditleri ve sorunları tespit edebilmesi beklenmektedir. Bilişim hemşiresi, özünde hasta verilerinin sorumlu bir temsilcisidir. Elektronik sağlık kayıt sistemi veya içindeki verilerle ilgili potansiyel bir tehdit veya sorun tespit ederse, işverenin politika ve prosedürleri doğrultusunda uygun irtibat noktası ile ivedilikle iletişime geçmelidir. Bilişim hemşiresi böylece klinik ve bilgi teknolojisi dünyaları arasında bir bağlantı görevi görür (37).

Hemşirelerin, bilişim teknolojilerinin yerleşik uygulama kalıplarına ilişkin bir rahatsızlık duydukları ve hasta bakımında bilişim teknolojilerini dikkat dağıtıcı buldukları belirtilmektedir. Bilgi teknolojisinin faydalarının anlaşılamamış olması hemşirelikte bilgi teknolojisinin kabul edilmesindeki ana engellerden biridir. Klinik alanda hemşireler hem hasta bakımı hem de günlük işlerinde bilgi teknolojisine girme konusunda baskı hissetmektedir (115).

Hemşirelik eğitimi programlarının, elektronik sağlık kayıtlarını kullanan hemşirelik fakültesi üyelerinin deneyimlerini ve algılarını araştırmak ve bu teknolojinin başarılı bir şekilde uygulanmasında etkili faktörleri belirlemek amacıyla Singapur'da Kowitlawakul ve ark. (2014) tarafından yapılan çalışmada, katılımcılar bu teknolojiyi, kullanıcılar için hem değerli hem de zorlukları olmasına rağmen yenilikçi bir teknoloji olarak algıladıkları belirtilmektedir. Bulgular, elektronik sağlık kayıtlarının hemşirelik eğitimi müfredatına entegrasyonunun, öğretim üyelerinin yeni teknolojiye ilişkin deneyimlerinin yanı sıra algılarına da bağlı olduğunu göstermektedir. Hemşirelerin hasta bakımı sağlamada elektronik hemşirelik belgelerinin kullanımı konusunda özellikle lisans düzeyinde eğitilmeleri gerekmektedir (116).

2.8. Siber Saldırı

Bilgisayar, bilgisayar ağları ve kullanıcılar tarafından oluşturulan sanal topluluğun imkânlarını kullanarak bilgi çalmak, değiştirmek bilişim sistemlerinde tahribata yol açmak veya aksatmaya neden olmak şeklindeki her türlü girişim, siber saldırı olarak tanımlanmaktadır. Günümüzde bilişim sistemlerinin getirdiği kolaylıkların yanı sıra bilgi güvenliğinin de önemi artmaktadır. Geçtiğimiz yüzyılda siber saldırılardan kaynaklı ciddi ekonomik zararlar oluştuğu belirtilmektedir. Bunu keşfeden devletler geliştirdikleri siber savunma stratejileriyle savunma bütçe ve strateji eylem planlarında siber güvenliğe yer vermeye başlamışlardır. Son yıllarda teknolojik adaptasyonun artışıyla beraber siber saldırıların ekonomik boyutu giderek şiddetini arttırmakta ve siber savaşları yol açmaktadır (53).



Şekil 2.4. Ülkelere göre 2017-2018 yılları siber suç maliyetleri (milyon $) (6).

Şekil 2.4.'te ülkelere göre 2017-2018 yıllarındaki siber suç maliyetlerine yer verilmektedir. ABD'nin siber suçlarla maliyette ilk sırada yer alması dikkat çekmekte ve 2017 yılı ile 2018 yılı arasındaki siber suç maliyeti farkına bakıldığında ciddi bir artış olduğu görülmektedir. Siyasi ve ekonomik yönden ilgi çekmesi, büyük bir ülke olması ve bilişim teknolojilerindeki entegrasyon gibi birçok faktör bu durumda rol

oynamaktadır. Asıl göze çarpan nokta ise Şekil 2.4.'te yer alan ülkelerde siber suç maliyetlerinin hızlı bir artış göstermiş olmasıdır (6).

Virüs koruma programları ve güvenlik duvarları, verileri siber suçlardan ve diğer tehditlerden korumayı amaçlar, ancak tüm kötü niyetli etkinlikleri engelleyemezler. Güvenliğe veya verilerin bütünlüğüne yönelik algılanan herhangi bir tehdit, mümkün olan en kısa sürede kuruluş içindeki doğru iletişim noktasına bildirilmelidir. Algılanan anomali, yazılım veya veritabanı arızası gibi masum bir nedenden kaynaklanabilir ya da siber suç faaliyetleri gibi kötü bir şeyden de kaynaklanıyor olabilir. Potansiyel olarak şüpheli gösterge örnekleri şunları içerir:

- Alışılmadık derecede yavaş veya yanıt vermeyen bilgisayar
- Olağandışı ağ etkinliği
- Düşük bellek
- Düşük disk alanı
- Mavi "ölüm ekranı"
- Sık sabit disk sürücüsü etkinliği
- Değiştirilmiş kayıtlar/kayıtlara olağandışı erişim
- Beklenmedik web sitelerine yönlendirme
- Kilitli bilgisayar/cihaz (erişim reddedildi)
- Devre dışı bırakılmış uygulamalar (antivirüs programı gibi)
- Gönderilenler klasöründeki sizin tarafınızdan gönderilmeyen e-postalar
- Hassas bilgileri ortaya çıkaran ve/veya garip ekler/bağlantılar içeren e-postalar.

Beklenmeyen veya şüpheli görünen e-posta iletilerindeki ekleri açarken veya bağlantılara tıklarken dikkatli olunması önemlidir. Teknolojinin kusursuz olmadığı gibi %100 doğru ve güvenli olmadığı da bilinmektedir (37).

Sağlık teknolojisinin benimsenmesi zordur ve planlama ve uygulama süresi gerektirir. Sağlık kuruluşları, tehditlere ayak uyduramadığı için modern eğilimlere ve tehditlere karşı güçsüz kalmaktadır (22). Siber güvenlik olayları, genel olarak sağlık sektörü ve özellikle hastaneler için büyüyen bir tehdittir (83). Kişisel sağlık bilgilerinin kullanımında gizliliğin korunması ve şeffaflığın teşvik edilmesi, güvenin sürdürülmesi için gereklidir (48). Ancak sağlık sektörü, ana paydaşını (yani hastaları) korumada diğer sektörlerin gerisinde kalmaktadır. Bu nedenle hastanelerin sistemlerini korumak için önemli miktarda sermaye ve çaba harcaması gerekmektedir. Bir ülkenin hastane

altyapısının siber güvenlik açığı, tüm hastanelerin güvenlik açıklarından etkilenir. Bu büyük sistemde, kaynak kullanılabilirliğindeki çeşitliliği azaltmak, tüm sistemi daha az savunmasız hale getirir. Siber güvenlik için düşük kaynaklara sahip birkaç hastane, tüm sağlık hizmetleri altyapısını tehdit eder. Başka bir deyişle, endüstriyi siber suçlular için daha az çekici hale getirmek için hastanelerin birlikte hareket etmesi gerekmektedir. Günümüzde, politikalar veri güvenliğini değil, çoğunlukla veri gizliliğini ele almaktadır. Bu nedenle, politika yapıcıların yalnızca siber güvenlik yeteneklerinin hedef seviyesini yükseltmekle kalmayıp aynı zamanda tüm sağlık sistemi genelinde kaynak kullanılabilirliğindeki değişkenliği azaltan politikalar getirmesi önemlidir (83).

Kişisel sağlık bilgileri, mağdurların tıbbi durumlarından kar elde etmek ve sahte sigorta talepleri yapmak için kullanılabilir ve tıbbi ekipmanın satın alınmasına ve yeniden satılmasına izin vererek veri gizliliğini tehdit eder. Veri kullanılabilirliği, kötü amaçlı yazılım saldırıları nedeniyle tehlikeye girebilir ve bu da kritik hastane prosedürleri için sorunlara neden olabilir. Kişisel sağlık bilgilerinde veri güvenliğinin temel amacı hasta güvenliği ve mahremiyetidir (117). Veri güvenliği, hastaların güvenini artırmak için önemlidir (118,119) ve sağlık tesisleri arasında iletişimi ve standardizasyonu kolaylaştıran sağlık sevk sistemlerinin kullanıcı tarafından kabulü için etkili bir faktördür (120). Veri güvenliği çok önemli olduğundan, bir kuruluşun bilgi güvenliğini etkin bir şekilde yönetmesi gerekir (29).

Siber saldırıların başarılı olması durumunda, hastane işlemlerinin olumsuz etkileneceği, klinik hizmetlere erişimin gecikeceği ve önemli ekonomik kayıplara yol açacağı bilinmektedir. Tüm bunların, hâlihazırda olağanüstü ekonomik ve klinik baskı altında olan kuruluşlar için yıkıcı sonuçlar doğuracağı belirtilmektedir (17).

2.9.Veri İhlalleri

Veri koruma kurallarının ihlal edilmesi durumunda ulusal veri koruma kurulları düzeltici önlem alma ve idari para cezası uygulama yetkisine sahip olmaktadır. Güçlü bir yaptırım etkisi sağlayan GVKT ile belirli veri ihlallerinde yüksek miktarda verilen para cezalarında kademeli şekilde artış olduğu belirtilmektedir (62).

Türkiye'de 24.03.2016 tarih ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'nun yayımlanmasının ardından her kurum ve kuruluş bilgi güvenliğine ilişkin düzenlemeler ile veri ihlallerinin önüne geçmeye çalışmaktadır. Veri ihlali oluşması halinde, Kişisel Verilerin Korunması Kanunu ile 2016 yılında kurulan Kişisel Verileri Koruma Kurumuna, 72 saat içinde bildirim yapılması gerekmektedir. Kişisel Verileri Koruma Kurumuna bildirilen veri ihlalleri, Kişisel Verileri Koruma Kurulu tarafından kanun kapsamında değerlendirilmekte ve kurulda alınan karar özetleri web sayfasında ilan edilmektedir (10).

3. MATERYAL VE YÖNTEM

3.1. Araştırmanın Şekli

Elektronik sağlık kayıtları kullanımında hemşirelerin bilgi güvenliği farkındalık düzeylerini belirlemek amacıyla yapılan tanımlayıcı nitelikte bir araştırmadır.

3.2. Araştırmanın Yapıldığı Yer ve Özellikleri

Bu araştırma Ankara ilindeki SBÜ Etlik Zübeyde Hanım Kadın Hastalıkları Eğitim ve Araştırma Hastanesi ile SBÜ Dr. Abdurrahman Yurtaslan Ankara Onkoloji Eğitim ve Araştırma Hastanesinde yapılmıştır.

SBÜ Etlik Zübeyde Hanım Kadın Hastalıkları Eğitim ve Araştırma Hastanesi 429 yatak kapasitesi ile Ankara ili Keçiören ilçesinde hizmet vermekte olup bünyesinde Genetik Merkezi, Perinatal Merkezi, ÜYTE Merkezi, Kemoterapi Merkezi gibi özellikli hizmetler bulunmaktadır. Bu hastanede 324 hemşire görev yapmaktadır.

SBÜ Dr. Abdurrahman Yurtaslan Ankara Onkoloji Eğitim ve Araştırma Hastanesi 500 Yatak Kapasitesi ile Ankara ili Yenimahalle ilçesinde hizmet vermekte olup bünyesinde Kemik İliği Nakil Merkezi (Erişkin), Kemoterapi Merkezi, Uyku Laboratuvarı, Tıbbi Genetik, Aferez gibi özellikli hizmetler bulunmaktadır. Bu hastanede 483 hemşire görev yapmaktadır.

3.3. Araştırmanın Evren ve Örneklemi

3.3.1. Araştırmanın Evreni

Araştırmanın evrenini, Ankara ilindeki SBÜ Etlik Zübeyde Hanım Kadın Hastalıkları Eğitim ve Araştırma Hastanesi ile SBÜ Dr. Abdurrahman Yurtaslan Ankara Onkoloji Eğitim ve Araştırma Hastanesinde çalışan toplam 807 hemşire oluşturmaktadır. Toplam hemşire sayısı, aktif çalışan (ücretsiz izin, doğum izni,

görevlendirme vb. nedenlerle çalışmayan hemşirelerin dâhil edilmemesi) hemşireler üzerinden hesaplanmıştır.

3.3.2. Araştırmanın Örneklemi

Örneklem seçimine gidildiğinde bu evren üzerinden yapılan örneklem hesabında %5 örneklem hatası %5 anlamlılık düzeyinde 261 sağlık çalışanı ile çalışılması yeterli bulunmuştur. Araştırma 266 hemşire ile tamamlanmıştır.

Araştırmaya dahil edilme kriterleri;

- ❖ Çalışmaya katılmaya gönüllü olma

Araştırmaya dahil edilmeme kriterleri;

- ❖ Çalışmaya katılmayı kabul etmeme
- ❖ Ücretsiz izin, doğum izni, görevlendirme vb. olan hemşireler

3.4. Veri Toplama Araçları

Araştırmamızda veri toplanma aracı olarak "Sosyo-Demografik Veri Formu" ve "Bilgi Güvenliği Ölçeği" kullanılmıştır.

3.4.1. Sosyo-Demografik Veri Formu

Araştırma için kullanılan Sosyo-Demografik Veri Formu (EK-2), literatür taraması yapılarak araştırmacı tarafından oluşturulmuştur (4,27,51,109,115,121) Sosyo-Demografik Veri Formu; hemşirelerin yaş, cinsiyet, medeni durum, eğitim durumu, meslekte görev süresi, bilgisayar ve internet kullanım süresi gibi tanımlayıcı özelliklerini belirlemek amacıyla yöneltilen 10 sorudan oluşmaktadır.

3.4.2. Bilgi Güvenliği Ölçeği

Upfold ve Sewry (2005) tarafından geliştirilen ölçek sağlık sektörü faaliyet alanı dışında, Küçük ve Orta Ölçekli İşletmelerin (KOBİ'ler) kurumsal bilgi güvenliği farkındalık düzeyini belirlemek amacıyla kullanılmıştır (122). Kılıç Aksu (2014) tarafından ölçeğin Türkçe geçerlik ve güvenirliği çalışması özel hastanelerde yapılmıştır (EK-3) (7). Ölçeğin puanlama yöntemi 5'li Likert Skalası (1: kesinlikle katılmıyorum, 2: katılmıyorum, 3: orta derecede katılıyorum, 4: katılıyorum, 5:

kesinlikle katılıyorum) şeklinde olup orijinal ölçekteki gibidir. Anket sorularına verilen yanıtlarda ortalama değerin 1'e yaklaşması elektronik sağlık kayıtlarının kullanımı konusunda hemşirelerin bilgi güvenliği farkındalık düzeylerinin düşük olduğu, ortalama değerin 5'e yaklaşması ise elektronik sağlık kayıtlarının kullanımı konusunda hemşirelerin bilgi güvenliği farkındalık düzeylerinin yüksek olduğu şeklinde ifade edilmektedir. Ölçekte bulunan 4 soru diğer sorular ile uyumluluk sağlaması için olumlu hale getirilmiştir. Bilgi güvenliği ile ilgili 42 sorudan oluşmaktadır. Bilgi Güvenliği Ölçeği, güvenlik politikası, örgütsel güvenlik, güvenlik uygulamaları, erişim ve yetkilendirme ile hizmet sunumu alt boyutları ile değerlendirilmektedir (7). 27 maddeden oluşan Bilgi Güvenliği Ölçeğinin Cronbach Alfa güvenirlik katsayısı 0.959 olarak hesaplanmıştır.

- **Güvenlik Politikası Alt Boyutu:** Bilgi güvenliğine ilişkin eğitimler, politikalar ve çalışanların sorumluluklarına dair 4 maddeden oluşmaktadır. Cronbach Alfa güvenirlik katsayısı 0.869 olarak hesaplanmıştır.
  - ❖ Çalışanlar bilgi güvenliği politikalardan haberdardır.
  - ❖ Hastanede, bilgi güvenliğine ilişkin yazılı politikalar vardır.
  - ❖ Hastanede bilgi güvenliğinin sağlanması için görevler ve sorumluluklar net olarak belirlenmiştir.
  - ❖ Tüm personele yeterli ve uygun bilgi güvenliği eğitimi verilmektedir.

- **Örgütsel Güvenlik Alt Boyutu:** Yönetici ve çalışanların bilgi güvenliğinin sağlanmasına ilişkin sorumluluklarına dair 5 maddeden oluşmaktadır. Cronbach Alfa güvenirlik katsayısı 0.867 olarak hesaplanmıştır.
  - ❖ Yöneticiler bilgi güvenliğinin uygulanması konusunda sorumluluk sahibidirler.
  - ❖ Hastanedeki yöneticiler bilgi güvenliğine gereken özeni gösterir.
  - ❖ Hastane içinde bilgi güvenliği konusunda bir uzman bulunmaktadır.
  - ❖ Bilgi güvenliğinin sağlanması için çalışanlar gerekli özeni gösterir.
  - ❖ Çalışanlar bilgi sisteminde izin verilen ve onaylanmayan uygulamalar konusunda yeterince bilgilidir.

- **Güvenlik Uygulamaları Alt Boyutu:** Yetkisiz erişim, veri ihlali gibi durumlarda gerekli denetim mekanizmaları ve yaptırımlar ile mevcut bilgilerin

korunması süreçlerine dair 5 maddeden oluşmaktadır. Cronbach Alfa güvenirlik katsayısı 0.828 olarak hesaplanmıştır.

- ❖ Güvenlik politikalarımızı ve süreçlerimizi ihlal eden çalışanlarımıza yönelik disiplin uygulamaları vardır.
- ❖ Çalışanlar kendi çalışma alanlarından uzaklaştığında, bilgisayarlarını daima güvenli şekilde bırakmaları konusunda eğitilmiştir.
- ❖ Çalışanlar, güvenlik ihlali olaylarının derhal yönetime bildirilmesi gerektiğinden haberdardır.
- ❖ Bilgi güvenliği uzmanı bulunmadığında dışarıdan danışmanlık hizmeti alınmaktadır.
- ❖ Sistem arızası, çökmesi ya da hırsızlık gibi durumlarda, veri yedeklerimiz işimizde kesintiye yol açmayacak şekilde bilgilerimizi geri kazanmamızı sağlar.

- **Erişim ve Yetkilendirme Alt Boyutu:** Katılımcıların, HBYS' de yetki sınırlamaları, kullanıcı hesaplarının tanımlanması, prosedürlerin belirlenmesi ve erişim yetkilerine dair 9 maddeden oluşmaktadır. Cronbach Alfa güvenirlik katsayısı 0.912 olarak hesaplanmıştır.

- ❖ Çalışanlar, kendi kullanıcı hesaplarıyla yetkilendirilip tanımlamaları yapılmadan, sistemlerimizde oturum açamaz/ sistemlerimize erişim sağlayamazlar.
- ❖ Bilgi işlem uygulamaları sadece yetkilendirilmiş iş amaçları doğrultusunda kullanılır.
- ❖ Hastanede, kullanıcıların hangi verilere erişebileceğini belirleyen bir yetkilendirme prosedürü vardır.
- ❖ Halka açık ağlara bağlı olmasına rağmen, sistemlerimiz internet hizmeti sağlayıcısının güvenliği ve/veya kendi güvenlik sistemlerimiz tarafından yeterince korunmaktadır.
- ❖ Sistemlerimiz herhangi bir sorun oluşması beklenmeden, önceden oluşturulmuş bir plan doğrultusunda güncellenmektedir.
- ❖ Anti-virüs sistemimiz günceldir ve bir virüs saldırısı durumunda, sistemlerimizi mümkün olan en iyi şekilde korumaktadır.

- ❖ Bir güvenlik ihlalinin meydana gelmesi durumunda, yapılacaklar ve yardım için kimin aranacağı bilinmektedir.
- ❖ Şifre değiştirme sıklığını belirleyen ve şifre karmaşıklığını engelleyen bir şifre yönetim sistemi bulunmaktadır.
- ❖ Kullanıcıların sistemlerimizde oturum açmalarına yetki verecek uygun mekanizmalar bulunmaktadır.

- **Hizmet Sunumu Alt Boyutu:** Bilgi güvenliği süreçleri ve iş akışına ilişkin hastalara sunulan hizmet kalitesine dair 4 maddeden oluşmaktadır. Cronbach Alfa güvenirlik katsayısı 0.847 olarak hesaplanmıştır.

- ❖ Bilgisayar kullanımı ile iş akışında olan değişimler bilgi güvenliğine gereken önemi vermeyi engellemez.
- ❖ Bilgi güvenliği süreçleri, hizmet kalitesini olumsuz yönde etkilemez.
- ❖ Bilgi güvenliği gün içinde yaptığımız işleri düşününce öncelikli bir konudur.
- ❖ Hastanedeki iş yükünün fazla olması, bilgi güvenliğine gereken önemin verilmesini engellememektedir.

3.5. Araştırmanın Uygulanması

Araştırma 20 Eylül-20 Ekim 2021 tarihleri arasında 266 (%101.9) hemşire ile tamamlanmıştır. Anket çalışması sırasında, anketi doldurmayı kabul etmeyen, ankette yer alan soruları eksik dolduran hemşireler araştırma kapsamı dışında bırakılmıştır. Pandemi nedeniyle araştırma için kullanılacak veri toplama araçları, online olarak uygulayabilmek için Google Formlar vasıtasıyla internet ortamına aktarılmıştır. İlgili hastanelerin Sağlık Bakım Hizmetleri Müdürleri ile Google Formlar üzerinde oluşturulan anketin bağlantı adresi çevrimiçi olarak paylaşılarak Sağlık Bakım Hizmetleri Müdürleri tarafından hemşirelere iletilmiştir. Hemşirelerin çalışmaya katılım için, online sistemde sunulan bilgilendirilmiş onam formunu okuyup araştırmaya katılmayı onayladıklarına dair ilgili kutucuğu işaretlemesi gerekmektedir. Bu işaretleme katılımcıların onam imzaları yerine geçmektedir. Katılımcılar onam formunun sonundaki "araştırmaya katılmayı kabul ettiklerine dair" ilgili kutucuğu işaretlemedikleri takdirde onay vermemiş sayılırlar ve bu durumda araştırmaya devam

edilmez. Ayrıca anketi doldurmayı yarıda bıraktıkları takdirde çalışmadan çekilebilmeleri mümkündür.

3.6. Araştırmanın Sınırlılıkları

Araştırmanın sadece iki merkezde yapılmış olması araştırmamızın sınırlılıklarını oluşturmaktadır.

3.7. Verilerin Değerlendirilmesi

Araştırma verilerinin analizleri IBM SPSS Statistics 26 paket programı üzerinden yapılmıştır. Araştırma verileri değerlendirilirken kategorik değişkenler için sayı ve yüzde, sayısal değişkenler için ise tanımlayıcı istatistikler (ortalama, standart sapma) verilmiştir. Sayısal değişkenlerin normallik varsayımı Kolmogorov Smirnov normallik testi ile incelenmiş ve normal dağıldığı görülmüştür. Bu nedenle çalışmada parametrik olan istatistiksel yöntemlerden yararlanılmıştır.

İki bağımsız grup arasındaki farklılıklar Bağımsız Örneklem T Testi ile incelenmiştir. İkiden fazla bağımsız grup arasındaki farklılıklar ise Tek Yönlü Varyans Analizi (ANOVA) ile kontrol edilmiştir. Tek Yönlü Varyans Analizi (ANOVA) sonucunda farklılık çıkması durumunda farklılığın hangi gruptan kaynaklandığını tespit etmek için Tukey testi kullanılmıştır. Analizlerde istatistiksel anlamlılık 0.05 düzeyinden yorumlanmıştır.

3.8. Araştırmanın Etik Boyutu

Araştırmayı yapabilmek için Ankara Yıldırım Beyazıt Üniversitesi Etik Kurulu'ndan onay alınmıştır (EK-1). Ölçeklerin kullanımı için araştırmacıdan e-posta ile izin alınmıştır (EK-4). Ankara Yıldırım Beyazıt Üniversitesi Sağlık Bilimleri Enstitüsünden gönderilen resmi yazıyla SBÜ Etlik Zübeyde Hanım Kadın Hastalıkları Eğitim ve Araştırma Hastanesi ile SBÜ Dr. Abdurrahman Yurtaslan Ankara Onkoloji Eğitim ve Araştırma Hastanesinden araştırma için izin alınmıştır (EK-5, EK-6). Araştırmaya katılım gönüllülük esasına dayalı olup online anket, araştırmanın neden ve nasıl yapılacağına ilişkin bilgi verildikten sonra bilgilendirilmiş onam formunu kabul eden hemşireler ile yapılmıştır (EK-7).

4. BULGULAR

Araştırmaya katılan hemşirelerin elektronik sağlık kayıtları kullanımında bilgi güvenliği farkındalık düzeylerini belirlemek üzere; sosyo-demografik verilerine ilişkin bulgular ve Bilgi Güvenliği Ölçeğinin güvenlik politikası, örgütsel güvenlik, güvenlik uygulamaları, erişim ve yetkilendirme ile hizmet sunumu alt boyutları birlikte değerlendirilmiştir.

Tablo 4.1. Araştırmaya katılanların hemşirelerin kişisel bilgilerine ilişkin dağılım (n=266).

	Sayı	**Yüzde**
Çalışılan Kurum		
Etlik Zübeyde Hanım Kadın Hastalıkları EAH	118	44.4
Dr. Abdurrahman Yurtaslan Onkoloji EAH	148	55.6
Cinsiyet		
Erkek	35	13.2
Kadın	231	86.8
Medeni Durum		
Bekar	101	38.0
Evli	165	62.0
Yaş		
18-26 Yaş	94	35.3
27-40 Yaş	83	31.2
41 ve Üzeri Yaş	89	33.5
Eğitim Durumu		
Sağlık Meslek Lisesi	21	7.9
Ön Lisans	27	10.2
Lisans	191	71.8
Lisansüstü	27	10.2
Meslekteki Görev Süresi		
1 Yıldan Az	26	9.8
1-5 Yıl	83	31.2
6-10 Yıl	23	8.6
11-20 Yıl	59	22.2
20 Yıl ve Üzeri	75	28.2
Günlük Bilgisayar Kullanım Süresi		
Hiç Kullanmıyor	60	22.6
1-2 Saat	123	46.2
3-4 Saat	36	13.5
4 Saatten Fazla	47	17.7
Günlük İnternet Kullanım Süresi		
Hiç Kullanmıyor	1	0.4
1-2 Saat	79	29.7
3-4 Saat	83	31.2
4 Saatten Fazla	103	38.7

Tablo 4.1 incelendiğinde araştırmaya katılan hemşirelerin %44.4'ü Sağlık Bilimleri Üniversitesi Etlik Zübeyde Hanım Kadın Hastalıkları Eğitim ve Araştırma Hastanesinde görev yapmakta iken %55.6'sı ise Sağlık Bilimleri Üniversitesi

Dr.Abdurrahman Yurtaslan Ankara Onkoloji Eğitim ve Araştırma Hastanesinde çalışmaktadır. Hemşirelerin %27.4'ü Kadın Doğum Kliniklerinde görev yapmakta iken %1.5'i Psikiyatri Klinikler, %12.4'i Onkoloji Klinikler ve %58.6'sı ise diğer kliniklerde (KBB, Ortopedi, Beyin Cerrahi, Genel Cerrahi Klinikleri ile Yenidoğan YB, Ameliyathane ve Poliklinikler) görev yapmaktadır. Araştırmaya katılan hemşirelerin %86.8'i kadın %13.2'si erkektir. Araştırmaya katılan hemşirelerin %35.3'ü 18-26 yaş grubunda iken %31.2'si 27-40 ve %33.5'i ise 41 ve üzeri yaş grubundadır. Hemşirelerin %7.9'unun eğitim durumu sağlık meslek lisesi iken %10.2'sinin önlisans, %71.8'inin lisans ve %10.2'sinin ise lisansüstüdür.

Araştırmaya katılan hemşirelerin %9.8'inin meslekteki görev süresi 1 yıldan az iken %31.2'sinin 1-5 yıl, %8.6'sının 6-10 yıl, %22.2'sinin 11-20 yıl ve %28.2'sinin ise 20 yıl ve üstüdür.

Hemşirelerin tamamı teknolojik cihaza (akıllı telefon, tablet, laptop vb.) sahiptir. Araştırmaya katılan hemşirelerin %22.6'sı günlük hiç bilgisayar kullanmamakta iken %46.2'si 1-2 saat, %13.5'i 3-4 saat ve %17.7'si ise 4 saatten fazla bilgisayar kullanmaktadır. Hemşirelerin %0.4'ü günlük internet kullanmamakta iken %29.7'si 1-2 saat, %31.2'si 3-4 saat ve %38.7'si 4 saatten fazla internet kullanmaktadır.

Tablo 4.2. Araştırmaya katılan hemşirelerin HBYS kullanımında erişimlerin denetimi konusundaki görüşlerine ilişkin dağılım.

	Sayı	**Yüzde**
HBYS Üzerinden Hasta Verilerine Erişimi Denetleyen Birim		
Bilgi İşlem	128	48.1
Hastane Yönetimi	66	24.8
Kalite	8	3
Bakanlık	5	1.9
Cevaplamayan	59	22.2

Tablo 4.2 incelendiğinde araştırmaya katılan hemşirelerin %48.1'i HBYS üzerinden hasta verilerine erişimi Bilgi İşlem biriminin denetlediğini %24.8'ü Hastane Yönetiminin denetlediğini belirtmiştir. Hemşirelerin %22.2'si ise soruyu yanıtsız bırakmıştır.

Tablo 4.3. Araştırmaya katılan hemşirelerin HBYS kullanımlarına ilişkin dağılım.

	Sayı	**Yüzde**
***Hastanede Kolaylıkla Erişilebilen Bilgiler**		
Hastaya Ait Bilgiler	249	93.6
Çalışanlara Ait Bilgiler	41	15.4
Hastaneye Ait Mali Bilgiler	11	4.1
Yönetimsel Raporlar	15	5.6
Süreçsel Raporlar	19	7.1
Kurum Prosedürleri	114	42.9
Sigorta Şirketi Bilgileri	4	1.5
Sosyal Güvence Bilgileri	45	16.9
Diğer	38	14.3
Tablo		
***Hastanede Günlük Çalışma Düzeninde Kullanılan Bilgiler**		
Hastaya Ait Bilgiler	245	92.1
Çalışanlara Ait Bilgiler	42	15.8
Hastaneye Ait Mali Bilgiler	17	6.4
Yönetimsel Raporlar	19	7.1
Süreçsel Raporlar	28	10.5
Kurum Prosedürleri	112	42.1
Sigorta Şirketi Bilgileri	5	1.9
Sosyal Güvence Bilgileri	35	13.2
Diğer	44	16.5
***Hastanede Koruma Altında Olan Bilgiler**		
Hastaya Ait Bilgiler	194	72.9
Çalışanlara Ait Bilgiler	214	80.5
Hastaneye Ait Mali Bilgiler	189	71.1
Yönetimsel Raporlar	184	69.2
Süreçsel Raporlar	115	43.2
Kurum Prosedürleri	100	37.6
Sigorta Şirketi Bilgileri	127	47.7
Sosyal Güvence Bilgileri	118	44.4
Diğer	34	12.8

* Bu sorularda katılımcılar tarafından birden fazla seçenek işaretlenmiştir.

Tablo 4.3 incelendiğinde araştırmaya katılan hemşirelerin hastalara ilişkin kolaylıkla erişebildiği bilgiler incelendiğinde %93.6'sı hastaya ait bilgiler cevabı vermiş iken kurum prosedürleri cevabı verenlerin oranı %42.9'dur.

Hastanede günlük çalışma düzeninde kullanılan bilgiler incelendiğinde %92,1'i hastaya ait bilgiler cevabı vermiş iken %42.1'i kurum prosedürleri cevabını vermiştir. Hastanede koruma altında olan bilgiler sorusunda çoğunlukla verilen ilk 3 cevap sırasıyla %80.5 ile çalışanlara ait bilgiler, %72.9 ile hastaya ait bilgiler ve %71.1 ile ise hastaya ait bilgilerdir.

Araştırmaya katılan hemşirelerin %25.2'si bilgi güvenliği sorunlarının nedenini "İhmal, Dikkatsizlik ve Önemsememe" olarak ifade etmiş iken %23.6'sı "Eğitim Yetersizliği" olarak ifade etmiştir. Diğer nedenler arasında ekranların açık bırakılması, şifre paylaşımı, bilgi güvenliğine yeterince önem verilmeyişi ve denetim eksikliği gösterilmiştir. Hemşirelerin %90.6'sı, bilgi güvenliği ile ilgili yaşanan kazaların ve nedenlerinin sistem kullanıcılarına duyurulmasını istemektedir.

Tablo 4.4. Araştırmaya katılan hemşirelerin hastadan onam alma durumlarına ilişkin dağılım.

	Sayı	Yüzde
Hastaya Ait Olan Bilgilerin Paylaşımı İçin Hastadan Onam Formu Alma		
Evet	211	79,3
Hayır	55	20,7

Tablo 4.4 incelendiğinde araştırmaya katılan hemşirelerin %79.3'ü, hastaya ait olan bilgilerin paylaşımı için hastadan onam formu alındığını belirtmektedir. Hemşirelerin %20.7'si ise hastaya ait olan bilgilerin paylaşımı için hastadan onam formu alınmadığını ifade etmektedir.

Tablo 4.5. Araştırmaya katılan hemşirelerin bilgi güvenliği uygulamalarına ilişkin dağılım.

	Sayı	Yüzde
***Bilgi Güvenliğinin Sağlanması İçin Sisteme Girişte Kullanılan Kimlik Belirleme Yöntemi**		
Kullanıcı Adı	256	96.2
Şifre	255	95.9
Akıllı Kart	14	5.3
Parmak İzi	1	0.4
Diğer	3	1.1
***Kullanılan Şifre Yapıları**		
1234...	23	8.6
8765...	6	2.3
Kullanıcı Adı ve Şifrenin Aynı Olması	20	7.5
Şifrede Kişisel İsim Kullanımı	59	22.2
Şifrede Bölüm Adı Kullanımı	16	6.0
Şifrede Hastane Adı Kullanımı	22	8.3
Sayı ve Harfin Bir Arada Kullanımı	204	76.7
Diğer	33	12.4
***Hastane Bilgi Yönetim Sisteminde Hastaya Ait Bilgiler İçin Yapılabilen İşlemler**		
Okuma	242	91.0
Yazma	132	49.6
Silme	31	11.7
Gönderme	31	11.7
Değiştirme	32	12.0
Kopyalama	26	9.8
Ekleme	58	21.8
Diğer	29	10.9
***Hastaya Ait Ulaşılabilen Bilgiler**		
Kimlik Bilgileri	241	90.6
İletişim Bilgileri	237	89.1
Hastalık Bilgileri	222	83.5
Tıbbi Raporlar	164	61.7
Tetkik Sonuçları	225	84.6
Önceden Aldığı Tıbbi Hizmetlere Ait Bilgiler	84	31.6
Ödeme Bilgileri	30	11.3
Sigorta Bilgileri	76	28.6
Diğer	21	7.9
***Hastane Bilgi Yönetim Sistemini Kullanırken Bilgi Güvenliğini Arttırmak İçin Alınması Gereken Önlemler**		
Anti-Virüs Programlarının Kullanımı	186	69.9
Yazılım ve Donanımın İhtiyaca Göre Güncellenmesi	167	62.8
Şifre Kullanımı	182	68.4
Bilgisayarlarda Kişisel USB Kullanımının Engellenmesi	87	32.7
Bilgisayarı Çalışanlar Dışında Kimsenin Kullanmasına İzin Verilmemesi	152	57.1
Çalışanın Birimden Ayrılırken Mutlaka Bilgisayarını Kapatması	146	54.9
Şifrenin Kesinlikle Paylaşılmaması	178	66.9
Şifrenin Uygun Kalitede Seçiminin Sağlanması	141	53.0
Diğer	18	6.8

* Bu sorularda katılımcılar tarafından birden fazla seçenek işaretlenmiştir.

Tablo 4.5 incelendiğinde bilgi güvenliğinin sağlanması için sisteme girişte kullanılan kimlik belirleme yöntemlerine verilen cevaplar incelendiğinde kullanıcı adı cevabı verenlerin oranı %96.2 iken şifre cevabı verenlerin oranı ise %95.9'dur.

Hemşirelerin kullandıkları şifre yapılarına verdikleri cevaplar incelendiğinde en çok verilen 3 cevap %76.7 ile sayı ve harfin bir arada kullanılması, %22.2 ile şifrede kişisel isim kullanımı ve %12.4 ile ise diğer yapılardır.

Hastane bilgi yönetim sisteminde hastaya ait bilgiler için yapılabilen işlemler için verilen cevaplar incelendiğinde en çok verilen 3 cevap sırasıyla %91 ile okuma, %49.6 ile yazma ve %21.8 ile ise de eklemedir.

Hastaya ait ulaşılabilen bilgiler incelendiğinde en çok verilen 4 cevap sırasıyla %90.6 ile kimlik bilgileri, %89.1 ile iletişim bilgileri, %84.6 ile tetkik sonuçları ve %83.5 ile ise hastalık bilgilerdir. Hastanın tıbbi tedavisinde kullanılmayan ödeme ve sigorta bilgilerine de erişim sağlanabildiğini görülmektedir.

Hastane bilgi yönetim sistemini kullanırken bilgi güvenliğini arttırmak için alınması gereken önlemlere verilen cevaplar incelendiğinde parametreler arasında birbirine yakın oranlar olduğu görülmektedir. En çok verilen 4 cevap sırasıyla %69.9 ile anti-virüs programlarının kullanımı, %68.4 ile şifre kullanımı, %66.9 ile şifrenin kesinlikle paylaşılmaması ve %62.8 ile yazılım ve donanımın ihtiyaca göre güncellenmesidir.

Tablo 4.6. Araştırmaya katılan hemşirelerin bilgi güvenliği konusunda farkındalık uygulamaları tercihlerine ilişkin dağılım.

	Sayı	Yüzde
Kurumdaki Bilgi Güvenliği Farkındalığını Artırmak İçin Yapılabilecek Uygulamalar		
Eğitici Posterlerin Hazırlanması		
1.Öncelik	100	53.2
2.Öncelik	29	15.4
3.Öncelik	36	19.1
4.Öncelik	22	11.7
5.Öncelik	1	0.5
SMS ile Hatırlatıcı Mesaj Gönderilmesi		
1.Öncelik	82	41.8
2.Öncelik	76	38.8
3.Öncelik	23	11.7
4.Öncelik	14	7.1
5.Öncelik	1	0.5
Hastane Bilgi Yönetim Sistemi Üzerinden Hatırlatıcı E-Posta Gönderilmesi		
1.Öncelik	18	10.6
2.Öncelik	49	28.8
3.Öncelik	79	46.5
4.Öncelik	24	14.1
5.Öncelik	0	0.0
E-Konferans Düzenlenmesi		
1.Öncelik	37	22.4
2.Öncelik	25	15.2
3.Öncelik	19	11.5
4.Öncelik	83	50.3
5.Öncelik	1	0.6
Diğer		
1.Öncelik	1	2.0
2.Öncelik	1	2.0
3.Öncelik	0	0.0
4.Öncelik	2	4.0
5.Öncelik	46	92.0

Tablo 4.6 incelendiğinde hemşirelerin kurumdaki bilgi güvenliği farkındalığını arttırmak için yapılabilecek uygulamaları önem derecesine göre sıralamaları incelendiğinde eğitici posterlerin hazırlanmasını %53.2'si 1.öncelik olarak seçmiş iken SMS ile hatırlatıcı mesaj gönderilmesi %41.8 ile 1. öncelik, hastane bilgi yönetim sistemi üzerinden hatırlatıcı e-posta gönderilmesi %46.5 ile 3.öncelik, e-konferans düzenlenmesi %50.3 ile 4.öncelik ve diğer uygulamalar ise %92 ile 5.öncelik olarak işaretlenmiştir.

Tablo 4.7. Araştırmaya katılan hemşirelerin bilgi güvenliği kazaları konusunda bilgilendirilmek için uygulama tercihlerine ilişkin dağılım.

	Sayı	Yüzde
Bilgi Güvenliği ile İlgili Yaşanan Kazaların ve Nedenlerinin Sistem Kullanıcılarına Duyurulması İçin Kullanılacak Kanallar		
SMS ile Gönderilmesini İsterim		
1.Öncelik	219	90.1
2.Öncelik	16	6.6
3.Öncelik	2	0.8
4.Öncelik	6	2.5
E-Posta ile Gönderilmesini İsterim		
1.Öncelik	17	10.9
2.Öncelik	116	74.4
3.Öncelik	22	14.1
4.Öncelik	1	0.6
E-Konferans ile Bildirilmesini İsterim		
1.Öncelik	15	11.6
2.Öncelik	18	14.0
3.Öncelik	86	66.7
4.Öncelik	10	7.8
Haber Verilmesini İstemem		
1.Öncelik	8	10.0
2.Öncelik	6	7.5
3.Öncelik	11	13.8
4.Öncelik	55	68.8
	Ort±SS	**Min-Mak**
Hastanedeki Bilgi Güvenliğini Değerlendirme	68.3±19.28	0-100

Tablo 4.7 incelendiğinde hemşirelerin bilgi güvenliği ile ilgili yaşanan kazaların ve nedenlerinin sistem kullanıcılarına duyurulması için kullanılacak kanalları önem derecelerine göre sıralamaları incelendiğinde SMS ile gönderilmesini isterim cevabı %90.1 ile 1.öncelik, E-posta ile gönderilmesini isterim %74.4 ile 2.öncelik, E-konferans ile bildirilmesini isterim %66.7 ile 3.öncelik ve haber verilmesini istemem ise %68.8 ile 4.öncelik olarak işaretlenmiştir. Hemşirelerin hastane bilgi güvenliğini değerlendirme düzeylerinin 0-100 puan arasında 68.3±19.28 olduğu görülmüştür.

Tablo 4.8. Bilgi Güvenliği Ölçeği ve Alt Boyutlarına ilişkin tanımlayıcı istatistikler.

	Ortalama	Standart Sapma	Minimum	Maksimum
Bilgi Güvenliği Ölçeği Toplam Puanı	**3.73**	**0.72**	**1.51**	**5.00**
Güvenlik Politikası Alt Boyutu	3.64	0.88	1.25	5.00
Örgütsel Güvenlik Alt Boyutu	3.70	0.80	1.20	5.00
Güvenlik Uygulamaları Alt Boyutu	3.61	0.84	1.00	5.00
Erişim ve Yetkilendirme Alt Boyutu	3.86	0.77	1.89	5.00
Hizmet Sunumu Alt Boyutu	3.86	0.91	1.00	5.00

Tablo 4.8 incelendiğinde hemşirelerin, Bilgi Güvenliği Ölçeği puanları ortalaması 3.73±0.72 iken Güvenlik Politikası alt boyutu 3.64±0.88, Örgütsel Güvenlik alt boyutu 3.70±0.80, Güvenlik Uygulamaları alt boyutu 3.61±0.84, Erişim ve Yetkilendirme alt boyutu 3.86±0.77 ve Hizmet Sunumu alt boyutu ise 3.86±0.91'dir.

Tablo 4.9. Günlük bilgisayar kullanım sürelerine göre Bilgi Güvenliği Ölçeği puanlarının farklılıklarının incelenmesi.

	Günlük Bilgisayar Kullanım Süresi	Ortalama	Standart Sapma	F	p
Bilgi Güvenliği Ölçeği Toplam Puanı	1)Hiç Kullanmıyor (n=60)	3.54	0.70	3.726	**0.012* Fark:1-4**
	2)1-2 Saat (n=123)	3.70	0.73		
	3) 3-4 Saat (n=36)	3.92	0.55		
	4) 4 Saatten Fazla (n=47)	3.94	0.79		
Güvenlik Politikası Alt Boyutu	1)Hiç Kullanmıyor (n=60)	3.50	0.83	2.468	0.063
	2)1-2 Saat (n=123)	3.58	0.89		
	3) 3-4 Saat (n=36)	3.86	0.71		
	4) 4 Saatten Fazla (n=47)	3.85	0.99		
Örgütsel Güvenlik Alt Boyutu	1)Hiç Kullanmıyor (n=60)	3.54	0.79	1.858	0.137
	2)1-2 Saat (n=123)	3.68	0.81		
	3) 3-4 Saat (n=36)	3.85	0.65		
	4) 4 Saatten Fazla (n=47)	3.86	0.86		
Güvenlik Uygulamaları Alt Boyutu	1)Hiç Kullanmıyor (n=60)	3.44	0.83	1.836	0.141
	2)1-2 Saat (n=123)	3.60	0.82		
	3) 3-4 Saat (n=36)	3.72	0.69		
	4) 4 Saatten Fazla (n=47)	3.79	0.97		
Erişim ve Yetkilendirme Alt Boyutu	1)Hiç Kullanmıyor (n=60)	3.64	0.77	3.887	**0.010* Fark: 1-3,4**
	2)1-2 Saat (n=123)	3.82	0.72		
	3) 3-4 Saat (n=36)	4.07	0.76		
	4) 4 Saatten Fazla (n=47)	4.06	0.81		
Hizmet Sunumu Alt Boyutu	1)Hiç Kullanmıyor (n=60)	3.58	0.81	4.320	**0.005* Fark: 1-3,4**
	2)1-2 Saat (n=123)	3.82	0.98		
	3) 3-4 Saat (n=36)	4.08	0.77		
	4) 4 Saatten Fazla (n=47)	4.13	0.85		

*F:Tek Yönlü Varyans Analizi (ANOVA) Fark:Tukey Testi *:p<0.05*

Tablo 4.9 incelendiğinde uygulanan Tek Yönlü Varyans Analizleri sonucunda araştırmaya katılan hemşirelerin günlük bilgisayar kullanım sürelerine göre Güvenlik Politikası alt boyutu, Örgütsel Güvenlik alt boyutu, Erişim ve Yetkilendirme alt boyutu puanları istatistiksel olarak anlamlı farklılık göstermemekte ($p>0.05$) iken Bilgi Güvenliği Ölçeği, Erişim ve Yetkilendirme alt boyutu ve Hizmet Sunumu alt boyutu puanları istatistiksel olarak anlamlı farklılık göstermektedir ($p<0.05$). Buna göre günlük 4 saatten fazla bilgisayar kullanan hemşirelerin Bilgi Güvenliği Ölçeği puanları hiç bilgisayar kullanmayan hemşirelerden anlamlı derecede daha fazladır. Hiç bilgisayar kullanmayan hemşirelerin Erişim ve Yetkilendirme alt boyutu puanları günlük 3-4 saat ve 4 saatten fazla bilgisayar kullanan hemşirelerden anlamlı derecede daha azdır. Hiç bilgisayar kullanmayan hemşirelerin Hizmet Sunumu alt boyutu puanları günlük 3-4 saat ve 4 saatten fazla bilgisayar kullanan hemşirelerden anlamlı derecede daha azdır.

Tablo 4.10. Günlük internet kullanım süresine göre Bilgi Güvenliği Ölçeği puanlarının farklılıklarının incelenmesi.

	Günlük İnternet Kullanım Süresi	**Ortalama**	**Standart Sapma**	**F**	**p**
Bilgi Güvenliği Ölçeği Toplam Puanı	1)1-2 Saat	3.78	0.69	0.534	0.587
	2)3-4 Saat	3.67	0.77		
	3)4 Saatten Fazla	3.76	0.71		
Güvenlik Politikası Alt Boyutu	1)1-2 Saat	3.67	0.86	0.270	0.764
	2)3-4 Saat	3.59	0.90		
	3)4 Saatten Fazla	3.68	0.88		
Örgütsel Güvenlik Alt Boyutu	1)1-2 Saat	3.76	0.75	0.805	0.448
	2)3-4 Saat	3.61	0.87		
	3)4 Saatten Fazla	3.74	0.78		
Güvenlik Uygulamaları Alt Boyutu	1)1-2 Saat	3.63	0.79	0.430	0.651
	2)3-4 Saat	3.54	0.88		
	3)4 Saatten Fazla	3.65	0.85		
Erişim ve Yetkilendirme Alt Boyutu	1)1-2 Saat	3.94	0.75	0.804	0.449
	2)3-4 Saat	3.79	0.80		
	3)4 Saatten Fazla	3.85	0.76		
Hizmet Sunumu Alt Boyutu	1)1-2 Saat	3.91	0.94	0.179	0.836
	2)3-4 Saat	3.82	0.92		
	3)4 Saatten Fazla	3.86	0.89		

F:Tek Yönlü Varyans Analizi (ANOVA)

Tablo 4.10 incelendiğinde uygulanan Tek Yönlü Varyans Analizleri sonucunda araştırmaya katılan hemşirelerin günlük internet kullanım sürelerine göre Bilgi Güvenliği Ölçeği ve alt boyut puanları istatistiksel olarak anlamlı farklılık göstermemektedir (p>0.05).

Tablo 4.11. Cinsiyete göre Bilgi Güvenliği Ölçeği puanlarının farklılıklarının incelenmesi.

	Cinsiyet	**Ortalama**	**Standart Sapma**	**t**	**p**
Bilgi Güvenliği Ölçeği Toplam Puanı	Erkek (n=35)	3.50	0.76	2.049	**0.041***
	Kadın (n=231)	3.77	0.71		
Güvenlik Politikası Alt Boyutu	Erkek (n=35)	3.39	0.99	-1.830	0.068
	Kadın (n=231)	3.68	0.86		
Örgütsel Güvenlik Alt Boyutu	Erkek (n=35)	3.45	0.82	2.053	**0.041**
	Kadın (n=231)	3.74	0.79		
Güvenlik Uygulamaları Alt Boyutu	Erkek (n=35)	3.42	0.86	-1.481	0.140
	Kadın (n=231)	3.64	0.83		
Erişim ve Yetkilendirme Alt Boyutu	Erkek (n=35)	3.63	0.80	-1.899	0.059
	Kadın (n=231)	3.89	0.76		
Hizmet Sunumu Alt Boyutu	Erkek (n=35)	3.63	1.00	-1.584	0.114
	Kadın (n=231)	3.89	0.89		

*t.Bağımsız Örneklem T Testi *:p<0.05*

Tablo 4.11 incelendiğinde uygulanan Bağımsız Örneklem t Testleri sonucunda araştırmaya katılan hemşirelerin cinsiyetlerine göre Güvenlik Politikası, Örgütsel Güvenlik, Güvenlik Uygulamaları, Erişim ve Yetkilendirme, Hizmet Sunumu alt boyutları puanları istatistiksel olarak anlamlı farklılık göstermemekte (p>0.05) iken Bilgi Güvenliği Ölçeği puanları istatistiksel olarak anlamlı farklılık göstermektedir (p<0.05). Buna göre kadınların Bilgi Güvenliği Ölçeği puanları erkeklerden anlamlı derecede daha fazladır.

Bağımsız Örneklem t Testleri sonucunda araştırmaya katılan hemşirelerin medeni durumlarına göre Bilgi Güvenliği Ölçeği ve alt boyut puanları istatistiksel olarak anlamlı farklılık göstermemektedir (p>0.05).

Tablo 4.12. Yaşa göre Bilgi Güvenliği Ölçeği puanlarının farklılıklarının incelenmesi.

	Yaş	Ortalama	Standart Sapma	F	p
Bilgi Güvenliği Ölçeği Toplam Puanı	1)18-26 Yaş(n=94)	3.74	0.74	4.426	**0.013* Fark: 2-3**
	2)27-40 Yaş (n=83)	3.56	0.72		
	3)41 ve Üzeri Yaş (n=89)	3.88	0.68		
Güvenlik Politikası Alt Boyutu	1)18-26 Yaş(n=94)	3.62	0.92	2.108	0.124
	2)27-40 Yaş (n=83)	3.52	0.85		
	3)41 ve Üzeri Yaş (n=89)	3.79	0.84		
Örgütsel Güvenlik Alt Boyutu	1)18-26 Yaş(n=94)	3.76	0.83	2.944	0.054
	2)27-40 Yaş (n=83)	3.53	0.79		
	3)41 ve Üzeri Yaş (n=89)	3.81	0.76		
Güvenlik Uygulamaları Alt Boyutu	1)18-26 Yaş(n=94)	3.74	0.81	3.613	**0.028* Fark: 1-2**
	2)27-40 Yaş (n=83)	3.41	0.86		
	3)41 ve Üzeri Yaş (n=89)	3.66	0.82		
Erişim ve Yetkilendirme Alt Boyutu	1)18-26 Yaş(n=94)	3.84	0.75	6.105	**0.003* Fark: 2-3**
	2)27-40 Yaş (n=83)	3.66	0.79		
	3)41 ve Üzeri Yaş (n=89)	4.06	0.72		
Hizmet Sunumu Alt Boyutu	1)18-26 Yaş(n=94)	3.76	0.94	5,523	**0.004* Fark: 3-1,2**
	2)27-40 Yaş (n=83)	3.69	0.94		
	3)41 ve Üzeri Yaş (n=89)	4.11	0.81		

*F:Tek Yönlü Varyans Analizi (ANOVA) Fark:Tukey Testi *:p<0.05*

Tablo 4.12 incelendiğinde uygulanan Tek Yönlü Varyans Analizleri sonucunda araştırmaya katılan hemşirelerin yaşlarına göre Güvenlik Politikası alt boyutu, Örgütsel Güvenlik alt boyutu, puanları istatistiksel olarak anlamlı farklılık göstermemekte ($p>0.05$) iken Bilgi Güvenliği Ölçeği, Güvenlik Uygulamaları alt boyutu, Erişim ve Yetkilendirme alt boyutu ve Hizmet Sunumu alt boyutu puanları istatistiksel olarak anlamlı farklılık göstermektedir ($p<0.05$). Buna göre 41 ve üzeri yaş grubundaki hemşirelerin Bilgi Güvenliği Ölçeği puanları 27-40 yaş grubundaki hemşirelerden anlamlı derecede daha fazladır. 18-26 yaş grubundaki hemşirelerin Güvenlik Uygulamaları alt boyutu puanları 27-40 yaş grubundaki hemşirelerden anlamlı derecede daha fazladır. 41 ve üzeri yaş grubundaki hemşirelerin Güvenlik Uygulamaları alt boyutu puanları 27-40 yaş grubundaki hemşirelerden anlamlı derecede daha fazladır. 41 ve üzeri yaş grubundaki hemşirelerin Hizmet Sunumu alt boyutu puanları 18-26 ve 27-40 yaş grubundaki hemşirelerden anlamlı derecede daha fazladır.

Tablo 4.13. Eğitim durumuna göre Bilgi Güvenliği Ölçeği puanlarının farklılıklarının incelenmesi.

	Eğitim Durumu	Ortalama	Standart Sapma	F	p
Bilgi Güvenliği Ölçeği Toplam Puanı	1) Sağlık Meslek Lisesi (n=21)	3.88	0.74	1.479	0.221
	2) Ön Lisans (n=27)	3.78	0.82		
	3) Lisans (n=191)	3.75	0.71		
	4) Lisansüstü (n=27)	3.48	0.64		
Güvenlik Politikası Alt Boyutu	1) Sağlık Meslek Lisesi (n=21)	3.76	0.92	0.520	0.669
	2) Ön Lisans (n=27)	3.79	0.96		
	3) Lisans (n=191)	3.63	0.87		
	4) Lisansüstü (n=27)	3.54	0.83		
Örgütsel Güvenlik Alt Boyutu	1) Sağlık Meslek Lisesi (n=21)	3.83	0.80	0.919	0.432
	2) Ön Lisans (n=27)	3.76	0.85		
	3) Lisans (n=191)	3.71	0.81		
	4) Lisansüstü (n=27)	3.48	0.65		
Güvenlik Uygulamaları Alt Boyutu	1) Sağlık Meslek Lisesi (n=21)	3.97	0.69	3.541	**0.015* Fark: 1-4**
	2) Ön Lisans (n=27)	3.71	0.94		
	3) Lisans (n=191)	3.61	0.83		
	4) Lisansüstü (n=27)	3.21	0.80		
Erişim ve Yetkilendirme Alt Boyutu	1) Sağlık Meslek Lisesi (n=21)	3.89	0.79	1.049	0.371
	2) Ön Lisans (n=27)	3.95	0.80		
	3) Lisans (n=191)	3.87	0.76		
	4) Lisansüstü (n=27)	3.62	0.72		
Hizmet Sunumu Alt Boyutu	1) Sağlık Meslek Lisesi (n=21)	3.95	0.84	1.561	0.200
	2) Ön Lisans (n=27)	3.71	0.90		
	3) Lisans (n=191)	3.91	0.91		
	4) Lisansüstü (n=27)	3.55	0.97		

*F:Tek Yönlü Varyans Analizi (ANOVA) Fark:Tukey Testi *:p<0.05*

Tablo 4.13 incelendiğinde uygulanan Tek Yönlü Varyans Analizleri sonucunda araştırmaya katılan hemşirelerin eğitim durumlarına göre Bilgi Güvenliği Ölçeği, Güvenlik Politikası alt boyutu, Örgütsel Güvenlik alt boyutu, Erişim ve Yetkilendirme alt boyutu ve Hizmet Sunumu alt boyutu puanları istatistiksel olarak anlamlı farklılık göstermemekte ($p>0.05$) iken Güvenlik Uygulamaları alt boyutu puanları istatistiksel olarak anlamlı farklılık göstermektedir ($p<0.05$). Buna göre eğitim durumu sağlık meslek lisesi olan hemşirelerin Güvenlik Uygulamaları alt boyutu puanları eğitim durumu lisansüstü olan hemşirelerden anlamlı derecede daha fazladır.

Tablo 4.14. Meslekte çalışma süresine göre Bilgi Güvenliği Ölçeği puanlarının farklılıklarının incelenmesi.

	Meslekte Çalışma Süresi	Ortalama	Standart Sapma	F	p
Bilgi Güvenliği Ölçeği Toplam Puanı	1) 1 Yıldan Az (n=26)	3.83	0.65	1.712	0.148
	2) 1-5 Yıl (n=83)	3.65	0.76		
	3) 6-10 Yıl (n=23)	3.55	0.62		
	4) 11-20 Yıl (n=59)	3.69	0.70		
	5) 20 Yıl ve Üzeri (n=75)	3.89	0.73		
Güvenlik Politikası Alt Boyutu	1) 1 Yıldan Az (n=26)	3.69	0.85	1.615	0.171
	2) 1-5 Yıl (n=83)	3.57	0.91		
	3) 6-10 Yıl (n=23)	3.47	0.81		
	4) 11-20 Yıl (n=59)	3.54	0.87		
	5) 20 Yıl ve Üzeri (n=75)	3.85	0.86		
Örgütsel Güvenlik Alt Boyutu	1) 1 Yıldan Az (n=26)	3.95	0.74	1.590	0.177
	2) 1-5 Yıl (n=83)	3.59	0.86		
	3) 6-10 Yıl (n=23)	3.64	0.65		
	4) 11-20 Yıl (n=59)	3.63	0.78		
	5) 20 Yıl ve Üzeri (n=75)	3.82	0.80		
Güvenlik Uygulamaları Alt Boyutu	1) 1 Yıldan Az (n=26)	3.82	0.81	0.761	0.551
	2) 1-5 Yıl (n=83)	3.64	0.87		
	3) 6-10 Yıl (n=23)	3.47	0.62		
	4) 11-20 Yıl (n=59)	3.52	0.84		
	5) 20 Yıl ve Üzeri (n=75)	3.63	0.87		
Erişim ve Yetkilendirme Alt Boyutu	1) 1 Yıldan Az (n=26)	3.95	0.68	3.039	**0.018* Fark: 2-5**
	2) 1-5 Yıl (n=83)	3.72	0.78		
	3) 6-10 Yıl (n=23)	3,60	0,69		
	4) 11-20 Yıl (n=59)	3.83	0.75		
	5) 20 Yıl ve Üzeri (n=75)	4.08	0.77		
Hizmet Sunumu Alt Boyutu	1) 1 Yıldan Az (n=26)	3.73	0.91	2.485	**0.044* Fark 2-5**
	2) 1-5 Yıl (n=83)	3.72	0.93		
	3) 6-10 Yıl (n=23)	3.55	0.93		
	4) 11-20 Yıl (n=59)	3.94	0.85		
	5) 20 Yıl ve Üzeri (n=75)	4.08	0.90		

*F:Tek Yönlü Varyans Analizi (ANOVA) Fark:Tukey Testi *:p<0.05*

Tablo 4.14 incelendiğinde uygulanan Tek Yönlü Varyans Analizleri sonucunda araştırmaya katılan hemşirelerin meslekte çalışma sürelerine göre Bilgi Güvenliği Ölçeği, Güvenlik Politikası alt boyutu, Örgütsel Güvenlik alt boyutu, Güvenlik Uygulamaları alt boyutu puanları istatistiksel olarak anlamlı farklılık göstermemekte ($p>0.05$) iken Erişim ve Yetkilendirme alt boyutu, Hizmet Sunumu alt boyutu puanları istatistiksel olarak anlamlı farklılık göstermektedir ($p<0.05$). Buna göre meslekte çalışma süresi 20 yıl ve üzeri olan hemşirelerin Erişim ve Yetkilendirme

alt boyutu, Hizmet Sunumu alt boyutu puanları meslekte çalışma süresi 1-5 yıl olan hemşirelerden anlamlı derecede daha fazladır.

5. TARTIŞMA

Günümüz bilişim teknolojisinin geldiği bu noktada elektronik sağlık kayıtları sağlık kurumlarının en değerli varlıkları haline gelmiştir. Hastalara ait elektronik sağlık kayıtlarına yetkisiz kişiler tarafından erişilmesi, paylaşılması, ifşa edilmesi hem hasta mahremiyeti hem de yasal açıdan bu bilgilerin güvenliğinin sağlanmasını gerektirmektedir. Bu sebeple hastalarla en sık karşılaşan ve sağlık çalışanları arasında sayısal olarak çoğunlukta olan hemşirelerin (123) elektronik sağlık kayıtları kullanımı oldukça önemlidir.

Araştırmamızda, HBYS üzerinden hasta verilerine erişimi denetleyen birim olarak %48,1 bilgi işlem birimi yanıtı alınmıştır. Bilgi Güvenlik sistemlerinde denetim işlevi bir zorunluluktur. Yöneticilerin ve kullanıcıların kişisel sağlık kaydı verilerine erişim listesini gözden geçirebilmeleri için denetim gereklidir. Böylelikle herhangi bir yasa dışı veya yetkisiz ihlal kolayca tespit edilebilir ve buna göre işlem yapılabilir (21). Sağlık Bakanlığı tarafından düzenlenen politikalar doğrultusunda, bilgi güvenliği yönetim sistemlerinde denetim yetkililerinin belirlenmesi ve kullanıcılar tarafından yetkililerin bilinmesi olası ihlallerin önüne geçmek adına katkı sağlayacaktır.

HBYS'de hastaya ait bilgiler için yapılabilen işlemler için verilen cevaplar incelendiğinde en çok verilen cevaplar %91 ile okuma, %49.6 ile yazma ve %21.8 ile ekleme yetkisi şeklindedir. Hemşirelerin hastaya ait bilgileri değiştirme ve silme yetkilerinin bulunmadığı görülmektedir. Hastaya ait ulaşılabilen bilgiler incelendiğinde ise en çok verilen cevaplar; %90.6 ile kimlik bilgileri, %89.1 ile iletişim bilgileri, %84.6 ile tetkik sonuçları ve %83.5 ile hastalık bilgileri olmuştur. Hastaya ait veriler üzerinde silme, değiştirme, gönderme işlemi yapabildiğini belirten %11.6 oranındaki hemşire, erişim yetkilerinde farklılıklar olduğunu göstermektedir. Hastalara ait verilere kimlerin erişebileceği ve erişen kişinin kaydedilmesi konusunda; HBYS üzerinde yetki matrisi ile kimin, ne zaman, ne biçimde, hangi kanallar ile ulaşım sağlayacağına dair erişimlerin sınırlandırılması ve kontrol edilmesi gerektiği düşünülmektedir.

Araştırmamızda bilgi güvenliğine ilişkin sorunlar arasında; ihmal, dikkatsizlik, eğitimlerin yetersizliği, ekranların açık bırakılması, şifre paylaşımı, yetkisiz erişim ve bilgi güvenliğine yeterince önem verilmediği konuları öne çıkmaktadır. Başdinkçi'nin

çalışmasında kurumlardaki en önemli bilgi güvenliği risk faktörleri; şifrelerin paylaşılması, kötü niyet, hasta bilgilerinin sızdırılması, veri güvenliğinin sağlanamaması, sabotaj ve lisansız yazılım kullanılması olarak görülmektedir. Hastalara ait bilgilerin sızdırılması çok ciddi bir konu olduğundan gereken tedbirlerin alınması önemlidir (40). Gizlilik koruma politikaları ihlal edilmese bile gerekli bilgilere ulaşmak için bilgisayar ekranlarının açık bırakılması ve şifrelerin paylaşılması durumlarına yönelik (112) elektronik sağlık kayıtları kullanıcılarının BGYS kapsamındaki politikaları bilmesi ve uygulaması önemlidir. Çünkü veri ihlali açısından ihmal, kusur veya kasıt içeren herhangi bir olumsuzluk yaşanması halinde, ilgili yasal düzenlemeler kapsamında elektronik sağlık kayıtları üzerinde işlem yapan kişinin bilinmesi ve tespit edilebilmesi gerekmektedir. Şifrelerin paylaşılması ya da ekranların açık bırakılmasının yasal sorumlulukları açısından eğitim programları ile bu konuda farkındalığın sağlanması gerektiği düşünülmektedir.

Bilgi güvenliği sorunlarına yönelik verilen cevaplar arasında araştırmamıza katılan hemşirelerin %23.6'sı, bilgi güvenliğine ilişkin eğitim yetersizliğine değinmiştir. Araştırmamıza katılan hemşirelerin Sağlık Bakanlığı Hizmet İçi Eğitim Yönetmeliği kapsamında hizmet içi eğitim olarak Bilgi Güvenliği eğitimi aldıkları bilinmektedir. Çakırlar ve ark. (2016) tarafından yapılan çalışma sonucunda hemşireler hizmet içi eğitim programlarında teknoloji kullanımına yönelik eğitimlere yer verilmesi yönünde görüş bildirmişlerdir (32). Hemşirelerin bilgi güvenliği politikalarına ilişkin farkındalıklarının, bilgi güvenliği ihlallerine yönelik yaptırımların ciddiyetinin algılanması üzerinde önemli bir etkisi bulunmaktadır (124). Eğitim programlarının, personelin ihtiyaç duyduğu konular doğrultusunda güncellenmesinin, bilgi güvenliği farkındalığını arttırmak adına olumlu bir etki sağlayacağı görülmektedir.

Araştırmamız sonucunda araştırmaya katılan hemşirelerin %79.3'ü hastaya ait olan (kimlik, iletişim, hastalık bilgileri ile tıbbi rapor ve tetkik sonuçları vb.) bilgilerin paylaşımı için hastadan onam formu alındığını belirtirken %20.7'si hastadan onam formu alınmadığını belirtmiştir. Toplama, analiz ve saklama dâhil olmak üzere sağlık verilerinin işlenmesi için onam zorunludur. Onam bireysel mahremiyeti, gizliliği ve özerkliği korumak için önemli bir araçtır. Bu, hem etik kurallar hem de KVKK, GVKT ve HIPAA gibi yasal düzenlemelere tabidir (9,10,125). Onam ile ilgili temel sorun veri

paylaşımı ve veri bağlantısı sırasında ortaya çıkmaktadır (125). Bilişim teknolojisi daha güçlü hale geldikçe ve farklı veri kümelerini birbirine bağlama yeteneği arttıkça, onam alınması için kullanılan kâğıt tabanlı sistemler artık amaca uygun bulunmamaktadır. Özellikle bilimsel araştırmalarda, onam için etik ve yasal gereklilikleri karşılamak ve araştırma ağlarındaki veri akışını sağlamak için yeni yaklaşımlara ihtiyaç duyulmaktadır (126). Çünkü onam, veri toplamada alınan verilerin gelecekteki tüm kullanımlarını kapsamamaktadır (125). Hastaya ait bilgilerin paylaşılması için hastadan onam alınmadığına ilişkin %20.7'lik oran, bireyin mahremiyet ve gizlilik hakkının ihlal edilebileceğini düşündürmektedir. Sigorta şirketleri, medikal firmalar, ilaç şirketleri veya bilimsel araştırmalarda kullanılmak üzere, hastalara ait bilgilerin, hangi gerekçe ile olursa olsun 3. kişilerle paylaşılması bilgi güvenliği açısından dikkat edilmesi gereken bir husustur.

Bilgi güvenliğinin sağlanması için sisteme girişte kullanılan kimlik belirleme yöntemlerine verilen cevaplar incelendiğinde kullanıcı adı cevabı verenlerin oranı %96.2 iken şifre cevabı verenlerin oranı ise %95.9'dur. Hemşirelerin kullandıkları şifre yapılarına verdikleri cevaplar incelendiğinde en çok verilen cevaplar %76.7 ile sayı ve harfin bir arada kullanılması, %22.2 ile şifrede kişisel isim kullanımı ve %12.4 ile ise diğer yapılar olmuştur. Şifreleme ve parola koruması, kişisel sağlık kayıtlarının güvenliğini ve gizliliğini garanti etmenin en iyi yoludur, ancak kötü sistemler veya kötü seçilmiş parolalar söz konusu olduğunda tatmin edici bir sonuç mümkün olmamaktadır (21).

Araştırmamızda HBYS kullanırken bilgi güvenliğini arttırmak için alınması gereken önlemlere verilen cevaplar incelendiğinde en çok verilen 4 cevap sırasıyla %69.9 ile anti-virüs programlarının kullanımı, %68.4 ile şifre kullanımı, %66.9 ile şifrenin kesinlikle paylaşılmaması ve %62.8 ile yazılım ve donanımın ihtiyaca göre güncellenmesi olmuştur. Kurumsal bilgi kaynaklarının farkına vararak, bu kaynaklara her tür denetimsiz erişimi engellemek, risk analizleri yaparak bilginin gizliliğinin ve bütünlüğünün korunması için gerekli idari ve teknik önlemleri almak ve tüm iş süreçlerini bilgi güvenliği politikaları doğrultusunda düzenleyerek bilgi güvenliği yönetimini sağlamak gerekmektedir (21).

Yılmaz ve ark. (2016) çalışmasında, kurumlarda bilgi güvenliği risk faktörlerinden en fazla önlem alınan konular arasında, kilitsiz kapılar, sistem odasına erişim, elektrik kesintileri, mekanik arızalar ve yangın, sel, doğal afetler yer almaktadır (4). En az önlem alınan bilgi güvenliği risk faktörleri ise network ağındaki yoğunluk, sistem uzmanı eksikliği, alt yapı eksikliği ve yazılım ihtiyaçlarının eksik belirlenmesidir. Başdinkçi'nin (2017) çalışmasında %70.9 oranında güçlü şifreler belirlenmekte olduğu ve şifreleri hiç kimseyle paylaşılmadığı belirtilmektedir. Şifre paylaşımını en çok yapan meslek grubunun ise doktorlar olduğu ve şifrelerini diğer sağlık çalışanları ile paylaştıkları sonucu ortaya çıkmıştır (40).

Özaslan (2019) çalışmasında, sağlık kurumlarında, bilgi güvenliğini sağlamada teknik koruma yöntemlerinin yeterli olmayacağı ve asıl etkenin kullanıcı olduğunu belirtmektedir. Bu yüzden donanımsal önlemlerin yanı sıra kullanıcı etkeninin de kurumlar tarafından göz önünde bulundurulması ve önemi açısından farkındalığın arttırılması gerektiğine değinmiştir (38). Keser ve ark. (2015) belirttiği gibi bilgi sistemlerinde bilgi sahibi, bilgi kullanıcısı veya bilgi sistemi yöneticisi olmanın getirdiği sorumluluk ile bilgi güvenliği seviyesi kullanıcılara bağlanmaktadır. Kullanıcıların farkındalığı bilgi güvenliğini sağlama noktasında oldukça kritik bir önem arz etmektedir (27). Box ve ark. (2013) bilgi güvenliği davranışını, bilgi güvenliği kültürünü teşvik eden bir örgütsel davranış olarak görmüştür. Duyguların, tutum ve davranışlara neden olduğunu belirtmiştir. Bu nedenle uyumluluğu sağlamayı amaçlayan Bilgi Güvenliği Farkındalığı ve Bilgi Güvenliği Farkındalığı programlarının, olumlu duyguları motive edecek ve kabullerini sağlayacak şekilde tasarlanması ve sunulmasının bilgi güvenliği davranışını iyileştirmenin etkili bir yolu olduğu vurgulanmaktadır (85).

Filik'in (2020) çalışmasında; tıbbi sekreterlerin, bilgi mahremiyeti ihlal sebepleri içinde yer alan yoğunluk bir tarafa bırakıldığında, bilgisizlik ve dikkatsizlik gibi kişi odaklı etkenler ortaya çıkmaktadır. Kişiye bağlı etkenleri en az seviyeye düşürmek için çalışanlara konu ile ilgili hizmet içi eğitim verilmesi ve çalışanların periyodik performans testleri ile takip edilmesi gibi uygulamalar yapılabilir. Yoğunluk kaynaklı ihlaller konusunda da alt yapının elektronik donanım ve çalışan kalitesi yönünden yeterli hale getirilmesi önerilmektedir (39). Teknik açıdan idarenin gerekli tedbirleri alması, çalışanların yapılan donanımsal düzenlemeler konusunda

bilgilendirilmesi, bunun yanı sıra kullanıcı kaynaklı hataların önüne geçmek için bilgi güvenliği kültürünün oluşturulması bilgi güvenliğini artırmaya katkı sağlamaktadır.

Araştırmamızda Hemşireler, Bilgi Güvenliği Ölçeği alt boyutlarından en yüksek puanı; Erişim ve Yetkilendirme alt boyutu ile Hizmet Sunumu alt boyutundan, en düşük puanı ise Güvenlik politikası alt boyutundan almışlardır. Erişim ve Yetkilendirme alt boyutunda yüksek puan alınması; hemşirelerin, HBYS' de yetki sınırlamaları, kullanıcı hesaplarının tanımlanması, prosedürlerin belirlenmesi ve erişim yetkileri konusunda farkındalığının yüksek olduğunu göstermektedir. Hizmet Sunumu alt boyutunda yüksek puan alınması; hastalara sunulan hizmet kalitesinin bilgi güvenliği süreçleri ve iş akışından etkilenmediği şeklinde yorumlanmaktadır. Güvenlik politikası alt boyutundan düşük puan alınması, bilgi güvenliğine ilişkin eğitimler, politikalar ve çalışanların sorumluluklarına dair yeterlilik ve memnuniyetin düşük olması ile ilişkilendirilebilir. Bilgi güvenliğine ilişkin sorunların nedeni olarak gösterilen eğitim yetersizliği bulgusu ile paralellik göstermektedir. Eğitimler ile bilgi güvenliği konusunda çalışanların sorumlulukları yasal düzenlemeler ve yaptırımlarının ele alınması gerekliliğine vurgu yapılmaktadır.

Araştırmamız sonucu, günlük 4 saatten fazla bilgisayar kullanan hemşirelerin bilgi güvenliği farkındalık düzeylerinin, hiç bilgisayar kullanmayan hemşirelerden yüksek olduğu görülmektedir ($p<0.05$). Ayrıca erişim ve yetkilendirme ile hizmet sunumu alt boyutlarında günlük 3-4 saat ve 4 saatten fazla bilgisayar kullanan hemşirelerin bilgi güvenliği farkındalık düzeyi, hiç bilgisayar kullanmayan hemşirelerden daha yüksektir. Bilgisayar kullanımı ve bilgi güvenliği konusunda bilgi düzeyi yüksek bireylerin, bilgi güvenliği farkındalık düzeylerinin daha yüksek olduğu ifade edilmektedir (127,128). Pattinson'un (2015) Avusturalyalı 500 yetişkin çalışan ile yaptığı çalışmada ise, bilgisayar kullanımı ile bilgi güvenliği davranışları arasında anlamlı ve olumsuz bir ilişki olduğunu göstermiştir. Bilgisayarları iyi kullanan kişilerin, daha az deneyime sahip olanlara göre daha çok riskli bir şekilde bilgisayar kullandığı belirtilmiştir (129). Genel olarak, potansiyel güvenlik riskleri hakkında daha bilgili ve daha bilinçli olan kişilerin aynı zamanda bilgi sistemlerini kullanırken riskli davranışlara daha yatkın oldukları ortaya konmuştur (130). Hemşirelerin günlük bilgisayar kullanım sürelerinin bilgi güvenliği farkındalığı üzerine etkisinin yanı sıra hiç bilgisayar kullanmayan %22.6 oranındaki hemşire sayısının dikkate alınması gerekmektedir. Bilgisayar kullanımı konusunda

hemşirelerin hazır bulunuşluk düzeyi, güvenlik zafiyeti açısından oldukça önemli olduğu düşünülmektedir.

Araştırmamıza katılan hemşirelerin günlük internet kullanım sürelerinin bilgi güvenliği farkındalık düzeyleri üzerine etkisi bulunmamaktadır. Ancak hemşirelerin %99.6'sının günlük olarak internet kullandığı belirlenmiştir. Hiç bilgisayar kullanmayan %22.6 oranındaki hemşire sayısına rağmen günlük internet kullanımındaki bu yüksek oranın mobil cihazlar aracılığı ile erişilen sosyal ağlardan kaynaklandığı şeklinde yorumlanmaktadır.

Araştırmamız sonucunda Bilgi Güvenliği Ölçeği ile örgütsel güvenlik alt boyutunda kadınların bilgi güvenliği farkındalık düzeyleri, erkeklerden anlamlı derecede daha fazla bulunmuştur ($p<0.05$). Literatürde farklı sonuçlara rastlanmakta olup bilgi güvenliği farkındalık düzeylerine bakıldığında erkeklerin farkındalık düzeylerinin kadınlardan yüksek olduğu (4,127) ya da cinsiyet kaynaklı fark bulunamadığına (7,40,42,131) ilişkin çalışmalar mevcuttur. Kadınlarda bilgi güvenliği farkındalık düzeylerinin yüksek bulunduğu şeklinde, araştırmamızla benzer sonuca ulaşan çalışmalar bulunmaktadır (39,132,133). Yapılan çalışmalarda cinsiyete bağlı oluşan bu farklı sonuçların, örneklem gruplarının farklılığı ile ilişkili olabileceği düşünülmektedir. Kadınların bilgi güvenliği farkındalık düzeylerinin yüksek bulunması, internet teknolojisinin getirdiği tehditlerin artması sonucu kadınların toplumsal açıdan artan güvensizlik hissinden kaynaklı olabileceği düşünülmektedir.

Araştırmamız sonucunda bilgi güvenliği ölçeği, erişim ve yetkilendirme ile hizmet sunumu alt boyutlarında ise 41 yaş ve üzeri hemşirelerin bilgi güvenliği farkındalık düzeyleri daha yüksek olduğu belirlenmiştir ($p<0.05$). Güvenlik uygulamaları alt boyutunda ise 18-26 yaş aralığındaki hemşirelerin bilgi güvenliği farkındalık düzeyleri yüksek bulunmuştur ($p<0.05$). Literatüre baktığımızda, bilgi güvenliği farkındalığı ve yaş arasında pozitif doğrusal bir ilişki olduğu, yaş arttıkça bilgi güvenliği farkındalığının arttığı görülmektedir (129,131,132,133).

Sosyo-Demografik veri formu oluşturulurken yaş aralıklarının belirlenmesinde Çaycı ve ark. (2014) çalışmasından faydalanılmıştır. Bu bağlamda Çaycı ve ark. çalışmasında, Z kuşağının (18-26 yaş) sosyal ağlarda kişisel bilgilerin paylaşımı ve hesaplarına kimlerin erişebileceği konusunda X ve Y kuşaklarına göre daha tedbirli

olduğu belirtilmektedir. Güvenlik uygulamaları alt boyutunda 18-26 yaş grubundaki hemşirelerin bilgi güvenliği farkındalık düzeylerinin 27-40 yaş grubundaki hemşirelerden anlamlı derecede daha fazla bulunmuş olması bu sonucu destekler niteliktedir. Çünkü teknolojinin içine doğan Z kuşağı kişisel bilgilerinin gizliliğine önem vermektedir. Ayrıca X ve Y kuşağının kişisel bilgiler konusunda mahremiyete önem vermedikleri belirtmiş olsa da araştırmamızda yer alan X kuşağının bilgi güvenliği farkındalık düzeyi yüksek bulunmuştur (51). Kendi kişisel bilgileri üzerinde söz hakkı kendisine ait olan hemşirelerin, hastalara ait olan sağlık kayıtları söz konusu olduğunda bilgi güvenliğini sağlama konusunda profesyonel bir tutum sergiledikleri görülmektedir. Bu farklılıkta hemşirelerin mesleki deneyiminin ve kurumsal bilgi güvenliği kültürünün etkisi olabileceği düşünülmektedir.

Araştırmamız sonucunda eğitim durumuna göre Bilgi Güvenliği Ölçeği alt boyutlarından güvenlik uygulamaları alt boyutunda, sağlık meslek lisesi mezunu olan hemşirelerin bilgi güvenliği farkındalık düzeyleri, eğitim durumu lisansüstü olan hemşirelerden anlamlı derecede daha fazla bulunmuştur. Ancak araştırmaya katılan hemşirelerin Bilgi Güvenliği Ölçeğinden aldıkları toplam puan, eğitim durumlarına göre istatistiksel olarak anlamlı farklılık göstermemektedir. Literatüre baktığımızda eğitim seviyesi yükseldikçe hasta mahremiyeti ve bilgi güvenliği farkındalığının arttığı belirtilen çalışmalar gibi (47,128,134) eğitim durumu ile bilgi güvenliği davranışı arasında ilişki bulunamayan çalışmalar (129) da mevcuttur. Güvenlik uygulamaları alt boyutunda görülen bu farklılığın yetkisiz erişim ve veri ihlali gibi durumlarda denetim mekanizmaları ve yaptırımlar konusunda araştırmamızda sağlık meslek lisesi mezunlarının meslekteki yıllarının fazla olduğu dolayısıyla kuşak farkının getirdiği hiyerarşik yapıya yönelik bakış açılarından kaynaklı olabileceği düşünülmektedir.

Araştırmamızda meslekte çalışma süresi hemşirelerin bilgi güvenliği farkındalık düzeyleri üzerinde istatistiksel olarak farklılık göstermemektedir. 20 ve üzeri yıl olan hemşirelerin erişim ve yetkilendirme alt boyutu ile hizmet sunumu alt boyutlarında bilgi güvenliği farkındalık düzeylerinin, meslekte çalışma süresi 1-5 yıl olan hemşirelerden daha yüksek olduğu bulunmuştur ($p<0.05$). Literatüre baktığımızda Aslan'ın çalışmasında hemşire akademisyenlerin BGFÖ ile meslekteki çalışma süresi arasında farklılık bulunmamıştır (127). Hemşirelerin hasta mahremiyetini korunmanın önemine yönelik algılarının klinik deneyim yılı ile anlamlı

bir fark olmadığı belirtmiştir (47,134). Taner tarafından güvenlik (polis ve jandarma) güçleriyle yapılan çalışmada da BGFÖ ile meslekteki çalışma süresi arasında farklılık bulunmamıştır (128). Lee ve ark. (2021) yaptığı çalışmada meslekte 5 yıldan fazla çalışanların sağlık bilgi güvenliği davranışlarının daha iyi olduğu sonucuna ulaşmıştır. Kariyer uzunluğunun sağlık bilgi güvenliği tehdit değerlendirmesi, sağlık bilgi güvenliği ile başa çıkma değerlendirmesi, sağlık bilgi güvenliği niyetleri ve davranışları üzerinde düzenleyici etkisi olduğunu belirtmişlerdir. Bu sonuç, iş deneyimi ne kadar fazla olursa, sağlık bilgi güvenliği davranışının o kadar fazla görüldüğünü göstermiştir (135). Mesleki deneyim ile bilgi güvenliği farkındalık düzeyi arasında pozitif bir ilişki bulunduğu görülmektedir.

Hemşire ve diğer sağlık çalışanlarının, dijital çağda kişisel sağlık bilgilerini daha iyi koruma ve gizlilik riskleri konusundaki farkındalıkları, çevrimiçi destek arayan ve sosyal ağ sitelerine katılan hasta ve hasta yakınları için önem arz etmektedir (58).

Araştırmamıza katılan hemşirelerin elektronik sağlık kayıtları kullanımında bilgi güvenliği farkındalık düzeylerinin iyi düzeyde (3,73±0,72) olduğu görülmüştür (Bkz. Tablo 4.8). Mahremiyet olgusu ile birlikte anılan bilgi güvenliğinin önemli olduğu konusuna vurgu yapan çalışmalar (16,40,41,125) gibi araştırmamızda da benzer bir sonuca ulaşılmıştır.

Araştırmamız sonucunda elde edilen veriler ışığında bilgi güvenliğini sağlamada hemşirelerin, hastalara ait eriştikleri bilgiler, yetkileri dâhilindeki işlemler, şifrelerin paylaşılması, bilgi paylaşımında onam alınmasına ilişkin verdikleri cevapların her biri kendi içinde önem arz etmektedir. Elektronik sağlık kayıtları üzerindeki yetki denetimlerinin sağlanması ve kullanıcı kaynaklı hataların önüne geçilmesi için düzenli olarak eğitim yapılması gerekliliği öne çıkmaktadır. Bilgi sistemi kullanıcısı hemşirelerin tamamının elektronik sağlık kayıtları konusunda aynı bilgi güvenliği seviyesine ulaşması gerekmektedir. Odağında hastanın yer aldığı sağlık hizmet sunumunda hassas veri olan elektronik sağlık kayıtlarının, hasta mahremiyetinin önemli bir unsuru olduğu unutulmamalıdır. Dijitalleşmenin her geçen gün farklı boyutlara taşındığı görülmekte olup sağlık sektörünün teknolojide yaşanan bu gelişmelere uyumlanması ve gelecek için hazırlıklı olması gerektiği düşünülmektedir. Yetkisiz erişim, siber saldırı, kullanıcı/sunucu kaynaklı hata gibi

durumlarda elektronik sağlık kayıtlarında yer alan verilerin ifşası, tahribatı, kullanılamaması gibi olası veri ihlallerine karşı, bildirim mekanizmaları ve hukuki sorumluklara dair bilgi güvenliği yönetim sistemleri konusunda gerekli eğitim ve denetimlerin yapılması, finansal ve teknik tedbirler alınması gerekmektedir.

6. SONUÇ VE ÖNERİLER

6.1. Sonuçlar

Elektronik sağlık kayıtları kullanımında hemşirelerin bilgi güvenliği farkındalık düzeylerini belirlemek amacıyla yaptığımız araştırma sonucunda elde ettiğimiz sonuçlar;

- Günlük 4 saatten fazla bilgisayar kullanan hemşirelerin bilgi güvenliği ölçeği, erişim ve yetkilendirme ve hizmet sunumu alt boyutlarında farkındalık düzeyleri daha yüksektir ($p<0.05$).
- Kadın hemşirelerin bilgi güvenliği ölçeği ve örgütsel güvenlik alt boyutunda farkındalık düzeyleri daha yüksektir ($p<0.05$).
- Hemşirelerin yaşlarına göre bakıldığında, 18-26 yaş aralığındaki hemşirelerin güvenlik uygulamaları alt boyutunda farkındalık düzeyleri yüksektir. 41 yaş ve üzeri hemşirelerin bilgi güvenliği ölçeği, erişim ve yetkilendirme ile hizmet sunumu alt boyutlarında farkındalık düzeyleri daha yüksektir($p<0.05$).
- Hemşirelerin eğitim durumlarına göre bakıldığında sağlık meslek lisesi mezunlarının güvenlik uygulamaları alt boyutunda farkındalık düzeyleri daha yüksektir($p<0.05$).
- Meslekteki görev süresi 20 yıldan fazla olan hemşirelerin hizmet sunumu ile erişim ve yetkilendirme alt boyutlarında farkındalık düzeyleri daha yüksektir($p<0.05$).
- Hemşirelerin HBYS üzerinden, çoğunlukla hastalara ait kimlik, iletişim, hastalık bilgileri ile tetkik sonuçlarına ulaşabildikleri belirlenmiştir.
- Hemşirelerin, HBYS'de bulunan hastaya ait bilgiler üzerinde genel olarak okuma, yazma ve ekleme yetkilerinin bulunduğu anlaşılmıştır.
- Hastaya ait bilgilerin paylaşımı için çoğunlukla hastadan onam formu alındığı belirtilmiştir.
- Bilgi güvenliğine ilişkin sorunların nedeni olarak ihmal, dikkatsizlik, eğitim yetersizliği, ekranların açık bırakılması ve şifrelerin paylaşılması gösterilmiştir.

6.2. Öneriler

- Bilgi Güvenliği kültürü oluşturmak için tüm birimler ve çalışanların sorumluluk alması,
- Özellikle, yöneticilerin kurumsal bilgi güvenliği politikalarının yürürlüğe konması, takibi ve denetlenmesi süreçlerinde aktif yer alması,
- Kullanıcı şifre ve parolalarının paylaşılmaması konusunda yasal sorumlulukların bilinmesi ve bu durumunun önlenebilmesi için gerekli denetim mekanizmalarının oluşturulması,
- Sağlık çalışanlarının bilgi güvenliğine yönelik tutumlarının geliştirilmesi ve yaptırımlar konusunda farkındalıklarının devamlılığı için eğitimlerin düzenli olarak tekrarlanması,
- Sağlık hizmetleri teknolojisinin ve hasta bilgilerinin yetkisiz erişime karşı korunması için zaman ayrılması ve finansman yatırılmasının sağlanması,
- Sağlık hizmetlerinde siber güvenlik görevlerinin açıkça tanımlanması, yazılım yükseltme ve veri ihlallerini ele alma konusunda net prosedürlerin oluşturulması, kullanıcıların şüpheli kod açmamaları konusunda eğitilmesi,
- Hemşirelik eğitimcilerinin, öğrencilerin elektronik dokümantasyon kullanımı ve klinik bilgi alma konusunda pratik yapmalarını sağlamak için lisans eğitiminde elektronik tıbbi kayıtları müfredatlarına dâhil etmesi,
- Bu çalışma Sağlık Bakanlığına bağlı hastanelerde yapılmış olup üniversite hastaneleri ve özel hastanelerde çalışan hemşirelerin bilgi güvenliği farkındalığına yönelik kurumsal kültürün etkisinin değerlendirilmesi önerilmektedir.

7. KAYNAKLAR

1. İzgi MC. Mahremiyet kavramı bağlamında kişisel sağlık verileri, *Türkiye Biyoetik Dergisi*, 2014, 1(1):25-37.

2. Pūraitė A, Adamonienė R, Žemeckė A. Sustainable digitalization in public ınstitutions: challenges for human rights, *European Journal of Sustainable Development*, 2020, 9(3):91.

3. Broeders D, Cristiano, F, Weggemans, D. Too close for comfort: cyber terrorism and ınformation security across national policies and ınternational diplomacy, *Studies in Conflict & Terrorism*, 2021:1-28.

4. Yılmaz E, Şahin, YL, Akbulut Y. Öğretmenlerin dijital veri güvenliği farkındalığı, *Sakarya University Journal of Education*, 2016, 6(2):26-45.

5. World Economic Forum 2012. Big data, big impact: New possibilities for ınternational development. https://www.weforum.org/reports/big-data-big-impact-new-possibilities-international-development. 19 Ocak 2022.

6. Ponemon Institute & Accenture. 2019 Cost of Cybercrime Study. https://www.ponemon.org/research/ponemon-library/security/2017-cost-of-cyber-crime-study.html. 19 Ocak 2022.

7. Kılıç Aksu P. Hastane Bilgi Yönetim Sisteminin Bilgi Güvenliği Açısından Değerlendirilmesi, Sağlık Bilimleri Enstitüsü, Doktora Tezi, İstanbul: Marmara Üniversitesi, 2014.

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

9. Shuaib M, Alam S, Alam MS, Nasir MS. Compliance with HIPAA and GDPR in blockchain-based electronic health record, *Materials Today: Proceedings*, 2021.

10. Kişisel Verilerin Korunması Kanunu. T.C. Resmi Gazete, sayı:29677, 07 Nisan 2016.

11. Jalali MS, Bruckes M, Westmattelmann, D, Schewe G. Why employees (still) click on phishing links: investigation in hospitals, *Journal of medical Internet research*, 2020, 22(1).

12. Ay F. Elektronik hasta kayıtları: güvenlik, etik ve yasal sorunlar, *Anadolu Üniversitesi Bilim ve Teknoloji Dergisi,* 2008, 9(2):165-175.

13. Rigby M. Protecting the patient by promoting end-user competence in health informatics systems—moves towards a generic health computer user "driving license", *International journal of medical informatics*, 2004, 73(2):151-156.

14. Safran C, Goldberg H. Electronic patient records and the impact of the Internet, *International Journal of Medical Informatics*, 2000, 60(2):77-83.

15. Tüfekçi N, Yorulmaz R. Cansever İH. Digital hospital, *Journal of Current Researches on Health Sector*, 2017, 7(2):144-156.

16. Uçar A, İLKILIÇ İ. Büyük verinin sağlık hizmetlerinde kullanımında epistemolojik ve etik sorunlar, *Sağlık Bilimlerinde İleri Araştırmalar Dergisi*, 2019, 2(2):80-92.

17. Jalali MS, Landman A, Gordon WJ. Telemedicine, privacy, and information security in the age of COVID-19, *Journal of the American Medical Informatics Association*, 2021, 28(3):671-672.

18. Bani Issa W, Al Akour I, Ibrahim A, Almarzouqi A, Abbas S, Hisham F, Griffiths J. Privacy, confidentiality, security and patient safety concerns about electronic health records, *International Nursing Review*, 2020, 67(2):218-230.

19. Arslan ET, Demir H. Sağlık çalışanlarının hasta mahremiyetine ilişkin tutumu: nitel bir araştırma. *Bolu Abant İzzet Baysal Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 2017, 17(4):191-220.

20. Varol E. (2018). Hemşirelerin mahremiyet hakkındaki tutumları ve bakım uygulamalarının hasta mahremiyetine olan etkileri, Sağlık Bilimleri Enstitüsü, Hemşirelik Anabilim Dalı, Yüksek Lisans Tezi, Balıkesir: Balıkesir Üniversitesi, 2018.

21. Ghazvini A, Shukur Z. Security challenges and success factors of electronic healthcare system, *Procedia Technology*, 2013, 11:212-219.

22. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends, *Technology and Health Care*, 2017, 25(1):1-10.

23. Rockwern B, Johnson D, Sulmasy LS. 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.

24. Sulmasy LS, López AM, Horwitch CA. Ethical implications of the electronic health record: in the service of the patient, *Journal of General İnternal Medicine*, 2017, 32(8):935-939.

25. İleri YY. Örgütlerde bilgi güvenliği yönetimi, kurumsal entegrasyon süreci ve örnek bir uygulama, *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, 2016, 17(4):55-72.

26. Wagner AE, Brooke C. Wasting time: the mission ımpossible with respect to technology-oriented security approaches, *Electronic Journal of Business Research Methods*, 2007, 5(2).

27. Keser H, Güldüren C. Bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme, *Kastamonu Eğitim Dergisi*, 2015, 23(3):1167-1184.

28. Ahmed SM, Rajput A. Threats to patients' privacy in smart healthcare environment, *In Innovation in Health Informatics*, 2020:375-393.

29. Sari PK, Prasetio A, Handayani PW, Hidayanto AN, Syauqina S, Astuti EF, Tallei FP. Information security cultural differences among health care facilities in Indonesia, *Heliyon*, 2021, 7(6).

30. Kamerer JL, McDermott D. Cybersecurity: Nurses on the front line of prevention and education, *Journal of Nursing Regulation*, 2020, 10(4):48-53.

31. T.C. Sağlık Bakanlığı. Sağlık İstatistikleri Yıllığı 2020 Haber Bülteni. https://sbsgm.saglik.gov.tr/Eklenti/41611/0/haber-bulteni-2020pdf.pdf. 08 Ocak 2022.

32. Çakırlar A, Mendi B. Hemşirelerin elektronik sağlık kaydı ve bilişim uygulamaları kapsamındaki bilgi ve tutumlarının değerlendirilmesi, *İstanbul Bilim Üniversitesi Florence Nightingale Tıp Dergisi*, 2016, 2(1):32-39.

33. Eriş H. Hemşirelerin hastanelerde kullandıkları elektronik tıbbi kayıtlar hakkındaki görüşleri: Şanlıurfa örneği, *Sağlık Akademisyenleri Dergisi*, 2016,*3*(3):93-99.

34. Curtis K, Brooks S. Digital health technology: factors affecting implementation in nursing homes, *Nursing Older People*, 2020, 32(2):14-21.

35. Top M, Gider Ö. Nurses' views on electronic medical records (EMR) in Turkey: an analysis according to use, quality and user satisfaction. *Journal of Medical Systems*, 2012, 36(3):1979-1988.

36. Park EH, Kim J, Park YS. The role of information security learning and individual factors in disclosing patients' health information, *Computers & Security*, 2017, 65:64-76.

37. Kim L. Cybercrime, ransomware, and the role of the informatics nurse, *Nursing2020*, 2020, 50(3):63-65.

38. Özaslan G. Bilgi Güvenliği ve Mahremiyeti Korunmasına Yönelik Eğitimin Etkilerinin Değerlendirilmesi: Bir Özel Hastane Uygulaması, Sağlık Bilimleri Enstitüsü, Sağlık Yönetimi Anabilim Dalı, Yüksek Lisans Tezi, İstanbul: Marmara Üniversitesi Sağlık Bilimleri Enstitüsü, 2019.

39. Filik T. Tıbbi Sekreterlerde Bilgi Güvenliği Farkındalık Düzeyinin Elektronik Sağlık Kayıtlarının Güvenlik ve Mahremiyet Uygulamalarına Etkisin Değerlendirilmesi, Lisansüstü Eğitim Enstitüsü, Sağlık Yönetimi Anabilim Dalı, Yüksek Lisans Tezi, Kayseri: Kayseri Üniversitesi, 2020.

40. Başdinkçi N. Sağlık Kurumlarında Bilgi Güvenliği Risk Değerlendirilmesi ve Kullanıcıların Bilgi Güvenliği Farkındalık Düzeyinin Ölçülmesi, Fen Bilimleri Enstitüsü, Endüstri Mühendisliği Anabilim Dalı, Yüksek Lisans Tezi, Adana: Çukurova Üniversitesi,2017.

41. Baran S, Şener E. Hastanelerde Bilgi Güvenliği Yönetimi: Nitel Bir Araştırma, *Süleyman Demirel Üniversitesi Vizyoner Dergisi*, 2019, 10 (23):108-125.

42. Kurt SG. Bilgi Güvenliğinin Bilgi İşlem Çalışanları Tarafından Değerlendirilmesi–Sağlık Sektöründe Bir Çalışma, Sağlık Bilimleri

Enstitüsü, Sağlık Yönetimi Ana Bilim Dalı, İstanbul: Marmara Üniversitesi, 2019.

43. Alpbaz MM. Türkiye'de iç ve dış politika tartışmalarına kaynaklık eden Bir belge olarak İnsan Hakları Evrensel Bildirgesi ve Anayasa Mahkemesi kararları: Avrupa İnsan Hakları Sözleşmesi ile karşılaştırmalı bir inceleme, *İnsan Hakları Yıllığı*, 2019, 37:54-88.

44. Büke KK. İnsan Hakları Bağlamında Kişisel Verilerin Korunması Önerisi, *Journal of Health and Sport Sciences*, 2020,3(1):19-23.

45. Hasta Hakları Yönetmeliği, T.C. Resmi Gazete, sayı:23420, 01 Ağustos 1998.

46. Zihaghi M, Saber S, Nouhi E. Respect for privacy by nurses from the perspective of the elderly hospitalized in internal and surgical wards, *Medical-Surgical Nursing Journal*, 2017, 5(3).

47. Kim K, Han Y, Kim J. Nurses' and patients' perceptions of privacy protection behaviours and information provision, *Nursing Ethics*, 2017, 24(5):1-14.

48. Price WN, Cohen IG. Privacy in the age of medical big data, *Nature Medicine*, 2019,25(1):37-43.

49. Aslanyürek M. İnternet ve sosyal medya kullanıcılarının internet güvenliği ve çevrimiçi gizlilik ile ilgili kanaatleri ve farkındalıkları, *Maltepe Üniversitesi İletişim Fakültesi Dergisi*, 2016,*3*(1):80-106.

50. Solmaztürk AB, Gürer A. Kariyer uyum yeteneklerinin x, y ve z kuşakları bakımından incelenmesi: Bir alan araştırması, *Turkish Studies-Social*, 2020, 15(3):1471-1487.

51. Çaycı B, Karagülle AE. X kuşağından Z kuşağına değişen mahremiyet algısı, *International Trends and Issues in Communication & Media Conference Proceedings Book*, 2014:190-196.

52. Uçak M. Kişisel verilerin hukuka uygun işlenmesinde çocuğun rızası, *Kişisel Verileri Koruma Dergisi*, 2021, 3(1):41-60.

53. Özkan İ. Siber saldırıların ekonomik boyutu, Sosyal Bilimler Enstitüsü, İktisat Anabilim Dalı, Yüksek Lisans Tezi, Bilecik: Bilecik Şeyh Edebali Üniversitesi, 2019.

54. Az A, Akbıyık Az ZA. COVID-19 bağlamında temaslı takibi: etik sorunlar ve değerlendirmesi, *Klimik Dergisi*, 2021, 34(1):18-24.

55. Altuncu SN, Altuncu MT. Mahremiyet, verileştirme ve dijital COVID-19 takip uygulamaları, *TRT Akademi*, 2021, *6*(11):72-87.

56. Sharon T. Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers, *Ethics and Information Technology*, 2021, 23(1):45-57.

57. Karaarslan E, Ergin AM, Turğut N, Kılıç Ö. Elektronik sağlık kayıtlarının gizlilik ve mahremiyeti, *XX. Türkiye'de İnternet Konferansı Bildiri Kitabı*, 2015:215-220.

58. Charbonneau DH. Privacy practices of health social networking sites: implications for privacy and data security in online cancer communities, *CIN: Computers, Informatics, Nursing*, 2016, 34(8):355-359.

59. Nguyen D. Mediatisation and datafication in the global COVID-19 pandemic: on the urgency of data literacy, *Media International Australia*, 2021, 178(1):210-214.

60. Telekomünikasyon Sektöründe Kişisel Bilgilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik. T.C. Resmi Gazete, sayı:25365, 06 Şubat 2004.

61. Politou E, Michota A, Alepis E, Pocs M, Patsakis C. Backups and the right to be forgotten in the GDPR: An uneasy relationship, *Computer Law & Security Review*, 2018, 34(6):1247-1257.

62. Sayar İB. The administrative fines regime of the General Data Protection Regulation and its ımpact, *Kişisel Verileri Koruma Dergisi*, 2021, 3(1):1-16.

63. Türk Ceza Kanunu. T.C. Resmi Gazete, sayı:25611, 26 Eylül 2004.

64. Wang J, Zhang Z, Xu K, Yin Y, Guo PA research on security and privacy issues for patient related data in medical organization system, *International Journal of Security and Its Applications*, 2013, 7(4):287-298.

65. Shuaib M, Alam S, Daud SM, Ahmad S. Blockchain-based ınitiatives in social security sector, 2nd International Conference on ICT for Digital, Smart and Sustainable Development, Yeni Delhi, Hindistan, *ICIDSSD Proceedings Book*, 2020:294-300.

66. Shuaib M, Daud SM, Alam S, Khan WZ. Blockchain-based framework for secure and reliable land registry system, *Telkomnika*, 2020, 18(5):2560-2571.

67. Shuaib M, Alam S, Daud SM. Improving the authenticity of real estate land transaction data using blockchain-based security scheme, *Second International Conference on Advances in Cyber Security*, Penang, Malezya, *Advances in Cyber Security Proceedings Book,* 2020:3-10.

68. Small SS, Hohl CM, Balka E. Patient perspectives on health data privacy and implications for adverse drug event documentation and communication: Qualitative study, *Journal of Medical Internet Research*, 2021, 23(1).

69. Mondschein CF, Monda C. The EU's General Data Protection Regulation (GDPR) in a research context, *Fundamentals of Clinical Data Science*, 2019:55-71.

70. Goddard M. The EU General Data Protection Regulation (GDPR): European regulation that has a global impact, *International Journal of Market Research*, 2017, 59(6):703-705.

71. Taylor MJ, Prictor M. Insight or intrusion? Correlating routinely collected employee data with health risk, *Social Sciences*, 2019, 8(10):291.

72. Tankard C. What the GDPR means for businesses, *Network Security*, 2016, 2016(6):5-8.

73. Voigt P, Von dem Bussche A. *The EU General Data Protection Regulation (GDPR), A Practical Guide*, 1st Ed., Springer International Publishing, 2017:9-30.

74. Rubinstein I. Big data: the end of privacy or a new beginning?, *International Data Privacy Law*, 2013, 3(2):(74-87).

75. Tikkinen-Piri C, Rohunen A, Markkula J. EU General Data Protection Regulation: Changes and implications for personal data collecting companies, *Computer Law & Security Review*, 2018, 34(1):134-153.

76. Veri Sorumluları Sicili Hakkında Yönetmelik, T.C. Resmi Gazete, sayı:30286, 30 Aralık 2017.

77. T.C Sağlık Bakanlığı VERBİS Bildirimi, https://kisiselveri.saglik.gov.tr/TR,84757/verbis-bildirimi.html 23 Ocak 2022.

78. Marşap A, Akalp G, Yeniman E. Sağlık işletmelerinde insan kaynağının kurumsal bilgi güvenliği kültürü gelişimi, *Bilişim Teknolojileri Dergisi,* 2010, 3(1):31-40.

79. Zheng Q. Information system security evaluation algorithm based on PSO-BP Neural Network, *Computational Intelligence and Neuroscience*, 2021.

80. Aras M. İşletmelerde Bilgi Koruma Stratejileri, *ODÜ Sosyal Bilimler Araştırmaları Dergisi (ODÜSOBİAD)*, 2018, *8*(3):613-621.

81. Sağlık Hizmeti Kalitesinin Geliştirilmesi ve Değerlendirilmesine Dair Yönetmelik. T.C. Resmî Gazete, sayı:28730, 06 Ağustos 2013.

82. T.C. Sağlık Bakanlığı. 2017 Yılı Sağlıkta Kalite Değerlendirmeleri Süreç Raporu. https://kalite.saglik.gov.tr/Eklenti/34962/0/2017-yili-skd-sonuc-raporuu-son-duzeltilmispdf.pdf. 08 Ocak 2022.

83. Jalali MS, Kaiser JP. Cybersecurity in hospitals: a systematic, organizational perspective, *Journal of medical Internet research*, 2018, 20(5).

84. Türk Standardları Enstitüsü. TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi. https://www.tse.org.tr/IcerikDetay?ID=2311&ParentID=6890. 09 Ocak 2022.

85. Box D, Pottas D. Improving information security behaviour in the healthcare context, *Procedia Technology*, 2013, 9:1093-1103.

86. Alhogail A, Mirza A. Information security culture: A definition and a literature review, *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, Hammamet, Tunus, *Institute of Electrical and Electronics Engineers (IEEE) Proceedings Book*, 2014, 1-7.

87. Coventry L, Branley D. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward, *Maturitas*, 2018, 113:48-52.

88. Box D, Pottas D. A model for information security compliant behaviour in the healthcare context, *Procedia Technology*, 2014, 16:1462-1470.

89. Alnatheer MA. A conceptual model to understand information security culture, *International Journal of Social Science and Humanity*, 2014, 4(2):104.

90. Zarei J, Sadoughi F. Information security risk management for computerized health information systems in hospitals: a case study of Iran, *Risk Management and Healthcare Policy*, 2016, 9:75.

91. Fenz S, Ekelhart A, Neubauer T. Information security risk management: In which security solutions is it worth investing?, *Communications of The Association for Information Systems*, 2011, 28(1): 22.

92. Shahri AB, Ismail Z, Mohanna S. The impact of the security competency on "self-efficacy in information security" for effective health information security in Iran, *Journal of Medical Systems*, 2016, 40(11):1-9.

93. T.C. Sağlık Bakanlığı. Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu. https://bilgiguvenligi.saglik.gov.tr/files/Bilgi%20Güvenliği%20Politikaları%20Kılavuzu%20(Sürüm%202.1).pdf . 08 Ocak 2022.

94. T.C Sağlık Bakanlığı. Bilgi Güvenliği Yönetim Sistemi. https://bilgiguvenligi.saglik.gov.tr/home/hizmetlerimiz 23 Ocak 2022.

95. T.C. Sağlık Bakanlığı. Bilgi Güvenliği Disiplin Prosedürü. https://bilgiguvenligi.saglik.gov.tr/files/BGYS_Dokuman_Ornekleri/BG.PR...%20B%C4%B0LG%C4%B0%20G%C3%9CVENL%C4%B0%C4%9E%

C4%B0%20D%C4%B0S%C4%B0PL%C4%B0N%20PROSED%C3%9CR%C3%9C.pdf . 15 Ocak 2022.

96. Rau HH, Wu YS, Chu CM, Wang FC, Hsu MH, Chang CW, Wen HC. Importance-performance analysis of personal health records in Taiwan: A web-based survey, *Journal of Medical Internet Research*, 2017, *19*(4):131.

97. Alam S, Siddiqui ST, Ahmad A, Ahmad R, Shuaib M. Internet of Things (IoT) enabling technologies, requirements, and security challenges, 2nd International Conference on Data and Information Sciences (ICDIS 2019), Agra, Hindistan, *Advances in Data And İnformation Sciences Proceedings Book*, 2020, 94:119-126.

98. Shuaib M, Samad A, Alam S, Siddiqui ST. Why adopting cloud is still a challenge?—A review on issues and challenges for cloud migration in organizations, *Ambient Communications and Computer Systems*, 2019:387-399.

99. Isık O, Yılmaz A, Barıscı N, Akbolat M, Odacıoglu Y, Akca N, Esatoglu AE. Sağlık Bilgi Sistemlerinin Gelişimi. İçinde: Yılmaz A.(editör). *Sağlık Kurumlarında Bilgi Sistemleri,* 1. Baskı. Eskişehir, T.C. Anadolu Üniversitesi Açıkögretim Fakültesi Yayını No: 1819, 2013:2-23.

100. Lærum H, Karlsen TH, Faxvaag A. Use of and attitudes to a hospital information system by medical secretaries, nurses and physicians deprived of the paper-based medical record: a case report, *BMC medical informatics and decision making*, 2004, 4(1):18.

101. Çetin İ. Hemşirelik öğrencileri için yeni bir ders: hemşirelikte bilgiye ulaşım, *Fırat Sağlık Hizmetleri Dergisi*, 2008,3(7):107-124.

102. Van Bemmel JH, Musen MA. A Handbook of Medical Informatics . Heidelberg: Springer-Verlag, 1997.

103. Lee TT, Yeh CH, Ho LH. Application of a computerized nursing care plan system in one hospital: experiences of ICU nurses in Taiwan, Journal of Advanced Nursing, 2002, 39(1):61-67.

104. Roemer LK, Richardson SJ, Sward K, Tilley C. Redundancy in a computer-generated order list: meeting the needs of nurses at various levels of practice expertise, *CIN: Computers, Informatics, Nursing*, 2005, 23(2):73-82.

105. Lee TT. Evaluation of computerized nursing care plan: instrument development, *Journal of Professional Nursing*, 2004, 20(4):230-238.

106. Aronsky D, Haug PJ. Assessing the quality of clinical data in a computer-based record for calculating the pneumonia severity index, *Journal of the American Medical Informatics Association*, 2000, 7(1):55-65.

107. Mahalli AE. Adoption and barriers to adoption of electronic health records by nurses in three governmental hospitals in Eastern Province, *Perspectives in health information management*, 2015, 12(Fall).

108. Ay F. Uluslararası elektronik hasta kayıt sistemleri, hemşirelik uygulamaları ve bilgisayar ilişkisi, *Gülhane Tıp Dergisi;* 2009, 51: 131-136.

109. Sethi N, Lane G, Newton S, Egan P, Ghosh S. Disaster easily averted?–Data confidentiality and the hospital desktop computer, *International Journal of Medical İnformatics*, 2014, 83(5):385-391.

110. Banerjee U, Rao P, Tamakuwala P, Koru G. Achieving information security in healthcare information systems: an essential challenge for the future of nursing informatics, *SINI: 28th Summer Institute in Nursing Informatics*, 2018. https://archive.hshsl.umaryland.edu/handle/10713/8979. 15 Ocak 2022.

111. T.C Sağlık Bakanlığı. Bilgi Güvenliği Politikaları Yönergesi. https://dosyamerkez.saglik.gov.tr/Eklenti/15584,bilgi-guvenligi-politikalari-yonergesi20180502pdf.pdf?0 23 Ocak 2022.

112. Eikey EV, Murphy AR, Reddy MC, Xu H. Designing for privacy management in hospitals: understanding the gap between user activities and IT staff's understandings, *International Journal of Medical İnformatics,* 2015, 84(12):1065-1075.

113. Fernando JI, Dawson LL. The health information system security threat lifecycle: An informatics theory, *International Journal of Medical İnformatics*, 2009, *78*(12):815-826.

114. Öztürk E, Öztaş D. Transkültürel hemşirelik. *Batman Üniversitesi Yaşam Bilimleri Dergisi*, 2012, 1(1):293-300.

115. Kahouei M, Mohammadi HB, Majdabadi HA, Solhi M, Parsania Z, Roghani PS, Firozeh M. Nurses' perceptions of usefulness of nursing information system: module of electronic medical record for patient care in two university hospitals of Iran, *Materia Socio-Medica*, 2014, 26(1):30.

116. Kowitlawakul Y, Chan SWC, Wang L, Wang W. Exploring faculty perceptions towards electronic health records for nursing education, *International Nursing Review*, 2014, 61(4):499-506.

117. Masrom M, Rahimly A. Overview of data security issues in hospital information systems, *Pacific Asia Journal of the Association for Information Systems*, 2015, 7(4):5.

118. Agaku IT, Adisa AO, Ayo-Yusuf OA, Connolly GN. Concern about security and privacy, and perceived control over collection and use of health information are related to with holding of health information from healthcare

providers, *Journal of the American Medical Informatics Association*, 2014, 21(2):374-378.

119. Glenn T, Monteith S. Privacy in the digital world: medical and health data outside of HIPAA protections, *Current Psychiatry Reports*, 2014, 16(11):494.

120. Handayani PW, Saladdin IR, Pinem AA, Azzahro F, Hidayanto AN, Ayuningtyas D. Health referral system user acceptance model in Indonesia, *Heliyon*, 2018, 4(12).

121. Eriş H, Havlioğlu S, Doni N. Kalite sistemi ve bilgi güvenliği sistemlerinin hasta güvenliği üzerine etkisi: bir üniversite hastanesi uygulaması, *Sağlık Akademisyenleri Dergisi*, 2017, 4(3):207-215.

122. Upfold CT, Sewry DA. An investıgation of information security in small and medium enterprises (SME'S), *Small*, 2005, 46(603):8244.

123. White JA, Levin J, Rispel LC. Migrants' perceptions of health system responsiveness and satisfaction with health workers in a South African province, *Global Health Action*, 2020, 13(1).

124. Karimi Z, Peikari HR. The impact of nurses' perceived information security training and information security policy awareness on their perceived severity and certainty of information security breach penalties (Case: the Educational Specialized Hospitals of Isfahan City), *Journal of Nursing Education*, 2018, 7(2):17-24.

125. Thapa C, Camtepe S. Precision health data: Requirements, challenges and existing techniques for data security and privacy, *Computers in Biology and Medicine*, 2021,129, 104130.

126. Kaye J, Whitley EA, Lund D, Morrison M, Teare H, Melham K. Dynamic consent: a patient interface for twenty-first century research networks, *European Journal of Human Genetics*, 2015, 23(2):41-146.

127. Aslan, Z. Hemşire Akademisyenlerin Bilgi Güvenliği Farkındalık Düzeylerinin Ve Etkileyen Faktörlerin Belirlenmesi, Sağlık Bilimleri Enstitüsü, Hemşirelikte Öğretim Anabilim Dalı, Yüksek Lisans Tezi, İzmir: Ege Üniversitesi, 2019.

128. Taner E, Kılıç İ. Güvenlik güçlerinin bilgi güvenliği farkındalığını belirlemeye yönelik bir araştırma, *Güvenlik Bilimleri Dergisi*, 2019, *8*(2):253-269.

129. Pattinson M, Butavicius M, Parsons K, McCormac A, Calic D. Factors that influence information security behavior: An Australian web-based study, *In International Conference on Human Aspects of Information Security, Privacy, and Trust*, 2015:231-241.

130. Velki T, Romstein K. User risky behavior and security awareness through lifespan, *International Journal of Electrical and Computer Engineering Systems*, 2018, 9(2):53-60.

131. Wiley A, McCormac A, Calic D. More than the individual: examining the relationship between culture and ınformation security awareness, *Computers & Security*, 2020, 88.

132. McCormac A, Zwaans T, Parsons K, Calic D, Butavicius M, Pattinson M. Individual differences and information security awareness, *Computers in Human Behavior*, 2017, 69:151-156.

133. McCormac A, Calic D, Parsons K, Butavicius M, Pattinson M, Lillie M. The effect of resilience and job stress on information security awareness, *Information & Computer Security*, 2018, 26(3).

134. Aktan GG, Eşer İ, Kocaçal E. Hemşirelerin hasta mahremiyetini koruma ve sürdürme durumları ile etkileyen faktörler, *Koç Üniversitesi Hemşirelikte Eğitim ve Araştırma Dergisi,* 2019, 16(4):301-305.

135. Lee E, Seomun G. Structural model of the healthcare ınformation security behavior of nurses applying protection motivation theory, *International Journal of Environmental Research and Public Health*, 2021, 18(4):2084.

EK-2. Sosyo-Demografik Veri Formu

Sayın Katılımcı,

Bu form Yıldırım Beyazıt Üniversitesi Sağlık Bilimleri Enstitüsü Hemşirelik Esasları Anabilim Dalında "Elektronik Sağlık Kayıtlarının Kullanımında Hemşirelerin Bilgi Güvenliği Farkındalık Düzeylerinin Belirlenmesi" konulu yüksek lisans tezi için hazırlanmıştır. Araştırma bilimsel bir nitelik taşıdığından verdiğiniz tüm bilgiler gizli tutulacaktır. Çalışmaya katılım tamamen isteğe bağlıdır. Çalışma ile ilgili sorularınız varsa aşağıda iletişim bilgileri yer alan araştırmacıya sorabilirsiniz.

1. Çalıştığınız Kurum
   1) Sağlık Bilimleri Üniversitesi Etlik Zübeyde Hanım Kadın Hastalıkları Eğitim ve Araştırma Hastanesi
   2) Sağlık Bilimleri Üniversitesi Dr. Abdurrahman Yurtaslan Ankara Onkoloji Eğitim ve Araştırma Hastanesi
2. Çalıştığınız birim
   1) Kadın Doğum Klinikleri
   2) Psikiyatri Klinikler
   3) Onkoloji Klinikleri
   4) Diğer…
3. Cinsiyetiniz
   1) Kadın
   2) Erkek
4. Medeni durumunuz
   1) Evli
   2) Bekâr
5. Yaşınız
   1) 18-26
   2) 27-40
   3) 41 ve üzeri
6. Eğitim durumunuz
   1) Sağlık Meslek Lisesi
   2) Ön lisans
   3) Lisans
   4) Lisansüstü
7. Meslekteki görev süreniz
   1) 1 yıldan az
   2) 1-5 yıl
   3) 6-10 yıl
   4) 11-20 yıl
   5) 20 yıl üzeri
8. Akıllı telefon, tablet, laptop vb. en az birine sahip misiniz)?

1) Evet 2) Hayır

9. Günlük bilgisayar kullanım süreniz
   1) Hiç kullanmıyorum
   2) 1-2 saat
   3) 3-4 saat
   4) 4 saatten fazla
10. Günlük internet kullanım süreniz
   5) Hiç kullanmıyorum
   6) 1-2 saat
   7) 3-4 saat
   8) 4 saatten fazla

Araştırmacının Adı Soyadı: Emel TAÇAR

İletişim Bilgileri: 05529263295

EK-3. Bilgi Güvenliği Ölçeği

Bilgi Güvenliği İle İlgili Genel Sorular

1. Hastanedeki hangi tür bilgilere kolaylıkla ulaşabiliyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)

   1) Hastaya ait bilgiler 2)Çalışanlara ait bilgiler 3)Hastaneye ait mali bilgiler 4)Yönetimsel raporlar
   5)Süreçsel raporlar 6)Kurum prosedürleri 7)Sigorta şirketi bilgileri 8)Sosyal güvence bilgileri
   9)Diğer……..

2. Hastanedeki günlük çalışma düzeninizde hangi tür bilgileri kullanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)

   1) Hastaya ait bilgiler 2)Çalışanlara ait bilgiler 3) Hastaneye ait mali bilgiler 4)Yönetimsel raporlar
   5)Süreçsel raporlar 6)Kurum prosedürleri 7)Sigorta şirketi bilgileri 8)Sosyal güvence bilgileri
   9)Diğer……..

3. Hastanedeki hangi tür bilgiler koruma altındadır? (Birden fazla seçenek işaretleyebilirsiniz)

   1) Hastaya ait bilgiler 2)Çalışanlara ait bilgiler 3) Hastaneye ait mali bilgiler 4)Yönetimsel raporlar
   5)Süreçsel raporlar 6)Kurum prosedürleri 7)Sigorta şirketi bilgileri 8)Sosyal güvence bilgileri
   9)Diğer…….

4. Hastane bilgi yönetimi sistemi üzerinden hasta verilerine erişiminiz kim/kimler tarafından denetleniyor?

5. Bilgi güvenliğinin sağlanması için sisteme girişte kimlik belirleme yöntemi olarak aşağıdakilerden hangisini /hangilerini kullanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)

   1) Kullanıcı adı 2)Şifre 3)Akıllı kart 4)Parmak izi 5)Diğer

6. Aşağıdaki şifre yapılarından herhangi birini kullanıyor musunuz? (Birden fazla seçenek işaretleyebilirsiniz)
   1) 1234…..
   2) 8765…..
   3) Kullanıcı adı ve şifrenin aynı olması
   4) Şifrede kişisel isim kullanımı
   5) Şifrede bölüm adı kullanımı
   6) Şifrede hastane adı kullanımı
   7) Sayı ve harfin bir arada kullanımı
   8) Diğer

7. Hastaya ait olan bilgilerin paylaşımı için hastalardan onam formu alıyor musunuz?

   1) Evet 2)Hayır

8. Hastane bilgi yönetimi sisteminde hastaya ait bilgiler için aşağıdaki işlemlerden hangisini/hangilerini yapabiliyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)

   1) Okuma 2)Yazma 3)Silme 4)Gönderme 5)Değiştirme 6)Kopyalama 7)Ekleme

   8) Diğer…….

9. Hastaya ait hangi bilgilere erişebiliyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)

   1) Kimlik bilgileri 2)İletişim bilgileri 3)Hastalık bilgileri 4)Tıbbi raporlar 5)Tetkik sonuçları

   6) Önceden aldığı tıbbi hizmetlere ait bilgiler 7)Ödeme bilgileri 8) Sigorta bilgileri 9)Diğer……..

10. Sizce hastane bilgi yönetim sistemi kullanılırken bilgi güvenliğini artırmak için aşağıdaki önlemlerden hangileri alınmalıdır? (Birden fazla seçenek işaretleyebilirsiniz)

1) Anti-virüs programlarının kullanımı
2) Yazılım ve donanımın ihtiyaca göre güncellenmesi
3) Şifre kullanımı
4) Bilgisayarda kişisel USB kullanımının engellenmesi
5) Bilgisayarı çalışanlar dışında kimsenin kullanmasına izin verilmemesi
6) Çalışanın birimden ayrılırken mutlaka bilgisayarını kapatması
7) Şifrenin kesinlikle paylaşılmaması
8) Şifrenin uygun kalitede seçiminin sağlanması
9) Diğer.....

11. Sizce bilgi güvenliği ile ilgili sorunların nedeni nedir?

12. Sizce kurumdaki bilgi güvenliği konusunda farkındalığı artırmak için yapılabilecek uygulamaları öncelik sırasına göre numaralandırınız.

1) Eğitici posterlerin hazırlanması (.....)
2) SMS ile hatırlatıcı mesaj gönderilmesi (.....)
3) Hastane bilgi yönetim sistemi üzerinden hatırlatıcı e-posta gönderilmesi (.....)
4) E-konferans düzenlenmesi (.....)
5) Diğer..... (.....)

13. Bilgi güvenliği ile ilgili yaşanan kazaların ve nedenlerinin sistem kullanıcılarına duyurulmasını ister misiniz?

1) Evet 2)Hayır

14. Bilgilendirmenin aşağıdaki yöntemlerden hangilerini kullanarak yapılmasını istersiniz? Öncelik sırasına göre numaralandırınız.

1) SMS ile gönderilmesini isterim (.....)
2) E-posta ile gönderilmesini isterim (.....)
3) E-konferans ile bildirilmesini isterm (.....)
4) Haber verilmesini istemem (.....)

15. Hastanedeki bilgi güvenliği için kaç puan verirsiniz?

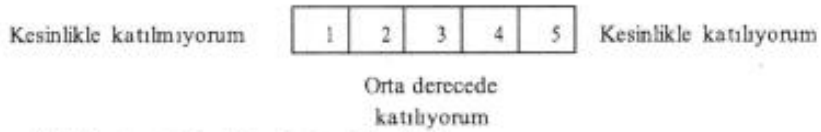
(Çok kötü) 0 ——————————————————————— 100 (Çok iyi)

16. Hastanede bilgi güvenliğinin sağlanması için görevler ve sorumluluklar net olarak belirlenmiştir (örneğin, yedeklerin alınmasından, kullanıcıların sisteme kaydedilmesinden sorumlu olan çalışanlar bulunmaktadır).

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum

Orta derecede katılıyorum

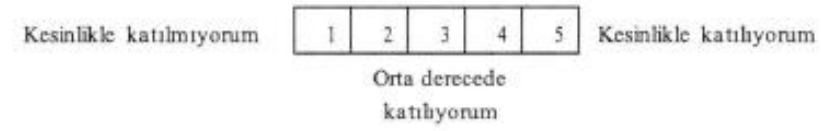
17. Hastanede, bilgi güvenliğine ilişkin yazılı politikalar vardır.



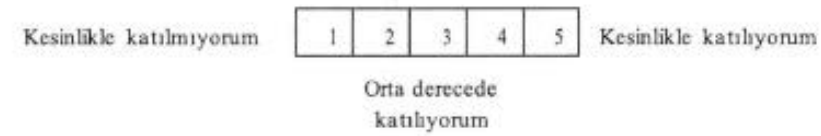
18. Çalışanlar bilgi güvenliği politikalardan haberdardır.



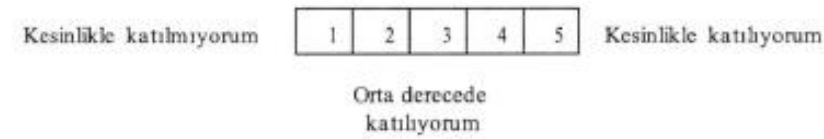
19. Tüm personele yeterli ve uygun bilgi güvenliği eğitimi verilmektedir.



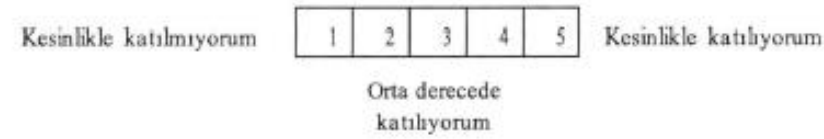
20. Çalışanlar bilgi sisteminde izin verilen ve onaylanmayan uygulamalar konusunda yeterince bilgilidir (örneğin; elektronik posta kullanımı ve internete bağlanma).



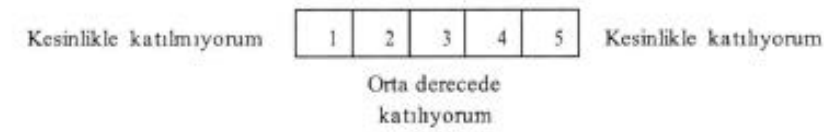
21. Bilgi güvenliğinin sağlanması için çalışanlar gerekli özeni gösterir.



22. Hastanedeki yöneticiler bilgi güvenliğine gereken özeni gösterir.



23. Yöneticiler bilgi güvenliliğinin uygulaması konusunda sorumluluk sahibidirler.



24. Hastane içinde bilgi güvenliği konusunda bir uzman bulunmaktadır.



25. Bilgi güvenliği uzmanı bulunmadığında dışarıdan danışmanlık hizmeti alınmaktadır.

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum

Orta derecede katılıyorum

26. Çalışanlar, güvenlik ihlali olaylarının derhal yönetime bildirilmesi gerektiğinden haberdardır.

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum

Orta derecede katılıyorum

27. Çalışanlar kendi çalışma alanlarından uzaklaştığında, bilgisayarlarını daima güvenli şekilde bırakmaları konusunda eğitilmiştir (örneğin; bilgisayar başından ayrıldığında bilgisayarların şifrelenmesi ya da oturumun kapatılması).

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum

Orta derecede katılıyorum

28. Güvenlik politikalarımızı ve süreçlerimizi ihlal eden çalışanlarımıza yönelik disiplin uygulamaları vardır.

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum

Orta derecede katılıyorum

29. Sistem arızası, çökmesi ya da hırsızlık gibi durumlarda, veri yedeklerimiz işimizde kesintiye yol açmayacak şekilde bilgilerimizi geri kazanmamızı sağlar.

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum

Orta derecede katılıyorum

30. Sistemlerimiz herhangi bir sorun oluşması beklenmeden, önceden oluşturulmuş bir plan doğrultusunda güncellenmektedir.

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum

Orta derecede katılıyorum

31. Bir güvenlik ihlalinin meydana gelmesi durumunda, yapılacaklar ve yardım için kimin aranacağı bilinmektedir.

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum

Orta derecede katılıyorum

32. Anti-virüs sistemimiz günceldir ve bir virüs saldırısı durumunda, sistemlerimizi mümkün olan en iyi şekilde korumaktadır.

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum

Orta derecede katılıyorum

33. Halka açık ağlara bağlı olmasına rağmen, sistemlerimiz İnternet Hizmeti Sağlayıcısının güvenliği ve/veya kendi güvenlik sistemlerimiz tarafından yeterince korunmaktadır.

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum

Orta derecede katılıyorum

34. Kullanıcıların sistemlerimizde oturum açmalarına yetki verecek uygun mekanizmalar bulunmaktadır.

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum

Orta derecede katılıyorum

35. Çalışanlar, kendi kullanıcı hesaplarıyla yetkilendirilip tanımlamaları yapılmadan, sistemlerimizde oturum açamaz / sistemlerimize erişim sağlayamazlar.

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum

Orta derecede katılıyorum

36. Şifre değiştirme sıklığını belirleyen ve şifre karmaşıklığını engelleyen bir şifre yönetim sistemi bulunmaktadır (örneğin, şifre iki haftada bir değiştirilmelidir ve en az ..... sayısı kadar karakter uzunluğunda olmalıdır).

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum

Orta derecede katılıyorum

37. Hastanede, kullanıcıların hangi verilere erişebileceğini belirleyen bir yetkilendirme prosedürü vardır.

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum

Orta derecede katılıyorum

38. Bilgi işlem uygulamaları sadece yetkilendirilmiş iş amaçları doğrultusunda kullanılır.

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum

Orta derecede katılıyorum

39. Hastanedeki iş yükünün fazla olması, bilgi güvenliğine gereken önemin verilmesini engellemez.

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum

Orta derecede katılıyorum

40. Bilgi güvenliği süreçleri, hizmet kalitesini olumsuz yönde etkilemez.

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum

Orta derecede katılıyorum

41. Bilgi güvenliği gün içinde yaptığımız işleri düşününce öncelikli bir konudur.

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum

Orta derecede katılıyorum

42. Bilgisayar kullanımı ile iş akışında olan değişimler bilgi güvenliğine gereken önemi vermeyi engellemez.

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum

Orta derecede katılıyorum

EK-7. Bilgilendirilmiş Onam Formu

BİLGİLENDİRİLMİŞ ONAM FORMU

LÜTFEN BU DÖKÜMANI DİKKATLİCE OKUMAK İÇİN ZAMAN AYIRINIZ

Değerli katılımcı,

Sizi Ankara Yıldırım Beyazıt Üniversitesi Sağlık Bilimleri Enstitüsü Yüksek Lisans Öğrencisi Emel TAÇAR tarafından yürütülen "Elektronik Sağlık Kayıtları Kullanımında Hemşirelerin Bilgi Güvenliği Farkındalık Düzeylerinin Belirlenmesi" başlıklı araştırmaya davet ediyorum. Bu araştırmaya katılıp katılmama kararını vermeden önce, araştırmanın neden ve nasıl yapılacağını bilmeniz gerekmektedir. Bu nedenle bu formun okunup anlaşılması büyük önem taşımaktadır. Eğer anlayamadığınız ve sizin için açık olmayan şeyler varsa, ya da daha fazla bilgi isterseniz bize sorunuz.

Bu çalışmaya katılmak tamamen gönüllülük esasına dayanmaktadır. Çalışmaya katılmama veya katıldıktan sonra herhangi bir anda çalışmadan çıkma hakkında sahipsiniz. Araştırmaya katılım için, online sistemde sunulan bilgilendirilmiş onam formunu okuyup araştırmaya katılmayı onayladığınıza dair ilgili kutucuğun işaretlemeniz gerekmektedir. Bu işaretleme katılımcıların onam imzaları yerine geçer. Katılımcılar onam formunun sonundaki "araştırmaya katılmayı kabul ettiklerine dair" ilgili kutucuğu işaretlemedikleri takdirde onay vermemiş sayılırlar ve bu durumda araştırmaya devam edilmez.

Size yöneltilen formlardaki soruları yanıtlarken kimsenin baskısı veya telkini altında olmayın. Bu formlardan elde edilecek bilgiler tamamen araştırma amacı ile kullanılacaktır. Eğer araştırmanın amacı ile ilgili verilen bu bilgiler dışında şimdi veya sonra daha fazla bilgiye ihtiyaç duyarsanız emel.tge@gmail.com e-posta adresi üzerinden araştırmacıya ulaşabilirsiniz.

1. Araştırmayla İlgili Bilgiler:

a. Araştırmanın Amacı: Elektronik Sağlık Kayıtları Kullanımında Hemşirelerin Bilgi Güvenliği Farkındalık Düzeylerinin Belirlenmesi

b. Araştırmanın İçeriği: Sağlıkta bilgi sistemleri ve sağlıkta kalite standartları incelendiğinde, hastalara ait bilgi ve belgelerin güvenliği gibi konuların önemli bir yere sahip olduğu anlaşılmaktadır. Hastanelerde bilgi güvenliğini sağlamak ve hasta memnuniyetini artırmak için bilgi güvenliği kültürünün oluşturulması gerekmektedir. Bu çalışmayla, başta kadın doğum, psikiyatri ve onkoloji kliniklerinde çalışan hemşireler

olmak üzere, hemşirelerin hastalara ait kişisel sağlık verilerinin ve elektronik sağlık kayıtlarının korunmasında bilgi güvenliğine yönelik farkındalık düzeylerinin belirlenmesi amaçlanmıştır.

c. Araştırmanın Nedeni: Tez çalışması

d. Araştırmanın Öngörülen Süresi: 1 ay

e. Araştırmaya Katılması Beklenen Katılımcı/Gönüllü Sayısı: 261

f. Araştırmanın Yapılacağı Yer(ler): SBÜ Etlik Zübeyde Hanım Kadın Hastalıkları Eğitim ve Araştırma Hastanesi, SBÜ Dr. Abdurrahman Yurtaslan Ankara Onkoloji Eğitim ve Araştırma Hastanesi

2. Çalışmaya Katılım Onayı:

Yukarıda yer alan ve araştırmadan önce katılımcıya/gönüllüye verilmesi gereken bilgileri okudum ve katılmam istenen çalışmanın kapsamını ve amacını, gönüllü olarak üzerime düşen sorumlulukları tamamen anladım. **Çalışma hakkında yazılı ve sözlü açıklama aşağıda adı belirtilen araştırmacı tarafından yapıldı, soru sorma ve tartışma imkanı buldum ve tatmin edici yanıtlar aldım. Bana, çalışmanın muhtemel riskleri ve faydaları sözlü olarak da anlatıldı.** Bu çalışmayı istediğim zaman ve herhangi bir neden belirtmek zorunda kalmadan bırakabileceğimi ve bıraktığım takdirde herhangi bir olumsuzluk ile karşılaşmayacağımı anladım.

Bu koşullarda söz konusu araştırmaya kendi isteğimle, hiçbir baskı ve zorlama olmaksızın katılmayı kabul ediyorum.

Katılımcının (Kendi el yazısı ile)

Adı

Soyadı:.....

İmzası:

(Varsa) Velayet veya Vesayet Altında Bulunanlar İçin;

Veli veya Vasisinin (kendi el yazısı ile)

Adı-

Soyadı:.....

İmzası:

Not: *Bu form, iki nüsha halinde düzenlenir. Bu nüshalardan biri imza karşılığında gönüllü kişiye verilir, diğeri araştırmacı tarafından saklanır.*