TÜRKİYE CUMHURİYETİ

MARMARA ÜNİVERSİTESİ

SAĞLIK BİLİMLERİ ENSTİTÜSÜ

BİLGİ GÜVENLİĞİ VE MAHREMİYETİN KORUNMASINA YÖNELİK EĞİTİMİN ETKİLERİNİN DEĞERLENDİRİLMESİ: BİR ÖZEL HASTANE UYGULAMASI

GÖKHAN ÖZASLAN

YÜKSEK LİSANS TEZİ

SAĞLIK YÖNETİMİ ANABİLİM DALI

DANIŞMAN

Prof. Dr. GONCA MUMCU

2019 –İSTANBUL

TEZ ONAYI

Kurum : Marmara Üniversitesi Sağlık Bilimleri Enstitüsü

Programın seviyesi : Yüksek Lisans

Anabilim Dalı : Sağlık Yönetimi Ana Bilim Dalı

Tez Sahibi : Gökhan ÖZASLAN

Tez BaĢlığı : "Bilgi Güvenliği ve Mahremiyetin Korunmasına Yönelik Eğitimin Etkilerinin Değerlendirilmesi: Bir Özel Hastane Uygulaması"

Sınav Yeri :Marmara Üniversitesi Sağlık Bilimleri Fakültesi, BaĢıbüyük YerleĢkesi

Sınav Tarihi : 27.06.2019

Tez tarafımızdan okunmuĢ, kapsam ve kalite yönünden Yüksek Lisans Tezi olarak kabul edilmiĢtir.

Danışman :	**Kurumu**	**İmza**
Prof.Dr.Gonca MUMCU	Marmara Üniversitesi	

Sınav Jüri Üyeleri:

Doç.Dr.Gülfer BEKTAĢ	Acıbadem Üniversitesi
Dr.Nurten ÖZÇELİK	Marmara Üniversitesi

Yukarıdaki jüri kararı Enstitü Yönetim Kurulu'nun 31.07.2019 tarih ve 29 sayılı kararı ile onaylanmıĢtır.

Prof. Dr. Feyza ARICIOĞLU
Sağlık Bilimleri Enstitüsü Müdürü

-Sınav evrakları 3 iĢ günü içinde ıslak imzalı tek kopya halinde Enstitüye teslim edilmelidir.

-Bu form bilgisayar ortamında doldurulacaktır.

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlanmasından yazımına kadar bütün safhalarda etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara kaynak gösterdiğimi ve bu kaynakları da kaynaklar listesine aldığımı, yine bu tezin çalışılması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığı beyan ederim.

Gökhan ÖZASLAN

TEŞEKKÜR

Tezimin konusunun belirlenmesi ve yürütülmesinde yardımlarını esirgemeyen, görüş ve önerileriyle beni sürekli destekleyen değerli danışmanım Sayın Prof. Dr. Gonca MUMCU' ya sonsuz teşekkürlerimi sunarım. Ayrıca her zaman yanımda olan kıymetli aileme, eşim Yasemin ÖZASLAN' a; analizlerinden destek aldığım değerli hocam Yrd. Doç. Dr. Pınar KILIÇ AKSU' ya, bilgi, tecrübe ve dostlukları her zaman beni destekleyen dostlarım Şeyma Birke BULU ve Araştırma Görevlisi Büşra KOPMAZ' a ve istatistik bilgilerini benden esirgemeyen değerli dostum Dyt. İrem ŞEROLAR' a son olarak her anlamda bana varlığını ve desteğini hissettiren Önder YALÇIN' a sonsuz teşekkürlerimi sunarım.

Gökhan ÖZASLAN

İÇİNDEKİLER

TABLOLAR

KISALTMALAR

AHBS: Aile Hekimliği Bilgi Sistemi

ESKS: Elektronik Sağlık Kayıt Sistemi

HBYS: Hastane Bilgi Yönetim Sistemi

SDP : Sağlıkta Dönüşüm programı

KBS : Klinik Bilgi Sistemi

PACS: Picture Archival and Communcation System

TSBS: Türkiye Sağlık Bilgi Sistemi

BGÖ: Bilgi Güvenliği Ölçeği

BİLGİ GÜVENLİĞİ VE MAHREMİYETİN KORUNMASINA YÖNELİK EĞİTİMİN ETKİLERİNİN DEĞERLENDİRİLMESİ: BİR ÖZEL HASTANE UYGULAMASI

Öğrenci: Gökhan ÖZASLAN

Danışman: Prof.Dr.Gonca MUMCU

Anabilim Dalı: Sağlık Yönetimi Anabilim Dalı

ÖZET

Amaç: Çalışmanın amacı, bilgi güvenliği ve mahremiyetine dair düzenlenen eğitim programının özel bir hastanede değerlendirilmesidir.

Gereç ve Yöntem: Bu araştırmada özel bir hastanede hastane bilgi yönetim sistemi (HBYS) kullanan, tıbbi ve idari bölümlerde çalışan 100 personel çalışmaya dahil edilmiştir. Veriler eğitim programından önce ve sonra olmak üzere Bilgi Güvenliği Ölçeği ilgili anket formu ile toplanmıştır. Çalışmada hastanenin kurumsal politikalarına göre ölçeğin üç alt boyut puanı (*Güvenlik Politikaları Alt Boyutu, Erişim ve Yetkilendirme Alt Boyutu ve Güvenlik Uygulamaları Alt Boyutu*) kullanılmıştır.

Bulgular: Hem tıbbi hem de idari personelin eğitim programı sonrasında *Güvenlik Politikaları Alt Boyutu, Erişim ve Yetkilendirme Alt Boyutu ve Güvenlik Uygulamaları Alt Boyutu* puanlarının önemli ölçüde azaldığı görülmüştür ($p < 0.05$). Ancak, bu puanların ön test ve son testte her iki grupta da benzer olduğu tespit edilmiştir ($p > 0.05$). Ayrıca, HBYS eğitiminin ölçek alt grupları puanları üzerinde olumlu bir etkisi olmadığı belirlenmiştir ($p > 0.05$).

Sonuç: Bilgi güvenliği kültürü sağlık yönetimi perspektifinde kritik bir konu olduğundan hastanelerde bilgi güvenliği kültürünü geliştirmek için iyi tasarlanmış eğitim programlarının oluşturulması gerekmektedir.

Anahtar Kelimeler: *Bilgi güvenliği, Mahremiyet, Bilgi Güvenliği Eğitimi, hastane bilgi yönetim sistemi, sağlık yönetimi.*

SUMMARY

THE EVALUATION OF THE TRAINING PROGRAM REGARDING INFORMATION SECURITY AND PRIVACY PROTECTION: THE PRACTICE OF A PRIVATE HOSPITAL

Student: Gökhan ÖZASLAN

Consultant: Prof. Dr. Gonca MUMCU

Department: Department Of Health Management

ABSTRACT

Aim: The aim of the study was to evaluate the effect of the training program regarding information security and privacy protection in a private hospital.

Materials and Methods: In this study,100 staff from medical and administrative departments using hospital information management system (HIMS) were included in this study. Data were collected by a questionnaire regarding Information Security scale before and after training program. According to corporate politics of the hospital, three subgroup scores of the scale (*Security Policy, Acces And Authorisation and Security Applications*) were used in the study.

Results: Scores of subgroups (*Security Policy, Acces And Authorisation and Security Applications*) were significantly decreased by the training program in both medical and administrative staff ($p<0.05$). However, these scores in pre-test and post-test were found to be similar in both groups ($p>0.05$). In addition, there was no positive effect of HIMS training on scores of these subgroups ($p>0.05$).

Conclusion: Sinceinformation security culture is the critical issue in health management' perspective, it is necessary to form well-design training programs for improving information security culture in hospitals.

Key Words: Information Security, Privacy, Information Security Training, hospital information management system, health management

1.GİRİŞ ve AMAÇ

Sağlık hizmetlerinde Hastane Bilgi Yönetim Sistemi (HBYS) yaygın olarak kullanılmaktadır. Hastanelerde farklı birimlerden çok sayıda kullanıcının, HBYS erişiminin olması hizmet sunumuna olumlu katkılar sağlarken, bilgi güvenliği ve mahremiyet açısından sorunların oluşmasına da neden olmaktadır (Kılıç Aksu, 2015). Günümüzde, elektronik kayıt sisteminin kullanımın artması ile beraber bilginin kolayca depolanması veya uzak yakın birçok noktaya kolayca ulaştırılabilmesi, aynı zamanda birçok kullanıcının bu depolanmış hazır bilgiye kolayca ulaşabilmesi de sağlanmıştır. Tabi ki kolay ulaşılan, ağ üzerinden rahatça paylaşılabilen bilgilerin güvenlik riskleri oluşmuş ve günümüzde bilgi güvenliğinin önemi de buna paralel olarak artmıştır (Kılıç Aksu, 2015).

Bilgi, kurum için değerli olan ve bu nedenle korunması gerekli, işlenmiş ve yorumlanmış veridir. Bilgi güvenliği ise; bu bilgilerin yetki sahibi olmayan kişilerin, görmesinden kullanmasından, değiştirmesinden, silinmesinden ve almasından korumak anlamına gelmektedir. Gelişen teknoloji ile beraber depolanması kolaylaşan bilginin güvenlik riskleri de doğmuştur (Calder,2005). Bu durumda bilgi güvenliğine verilen önemin artmasını da öz konusudur. Sağlık kurumları, bu riskleri en aza indirebilmek için kurumsal ve sistemsel önemler alıp kullanıcıları eğitimler ile bilinçlendirmenin önemi ön plana çıkmıştır(Kılıç Aksu ve Ark., 2015).

Bilgi güvenliğinin en temel amacı; mahremiyetin sağlanması, izinsiz ve yetkisiz kişilerin erişiminin engellenip uygun amaç ve zamanda yetkili kişilerin ulaşılabilirliğinin sağlanmasıdır (Korkmaz, 2018).Kişisel verilerin korunması bağlamında ülkemizde net olarak anayasa bir hak olarak Anayasamızın 20. maddesinde “Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir (Küzeci, 2010). Bu araştırmada, HBYS kullanan çalışanlarda bilgi güvenliği ve mahremiyete yönelik eğitimin etkisinin değerlendirilmesi amaçlanmıştır.

2. GENEL BİLGİLER

Günümüzde bilgi ve iletişim teknolojilerinin gelişimi ile bilginin paylaşılması ve uzak noktalardan erişimin sağlanması söz konusudur. Bu yüzden bilgi güvenliği sağlık sektörü dahil birçok kurum ve kuruluşta oldukça önemlidir (Kılıç Aksu ve Ark., 2015). Bilgi güvenliği; gizliliğin, bütünlüğün ve erişilebilirliğin korunmasını ifade eder. Bilgi güvenliğinin sağlanması için atılan ilk adım, bir güvenlik politikasının belirlenmesidir (Whitman, 2012). Her kurumun kendine göre güvenlik politikası bulunmaktadır ve bu politikalar çalışanların sorumlulukları, uygulamaların kontrolü ve sürecin ilerleyişine ilişkin genel kurallardan oluşmaktadır (Kılıç Aksu ve Ark., 2015). Bunların yanı sıra bir güvenlik politikası güvenliğin ihlaline neden olacak durumları önlemeyi ve hassas bilgileri daha detaylı korumayı amaçlamaktadır (Tosun, 2004).

Bilgi güvenliği farklı yaklaşımlardan oluşmaktadır. Bunlar şu şekilde sıralanabilir (Peltier, 2016):

- Hassas bilgileri korumak,
- Bilgiyi bir bütün olarak saklamak,
- Kurumun kültürüne katkıda bulunmak,

Günümüzde bilgi birçok kurumda yoğun şekilde kullanılmaktadır ve bu kurumlar bilgi güvenliğinin sağlanması için gelişen teknolojiden aktif bir şekilde yararlanmaktadırlar. Bilgi, kurumlar için çok kritik bir varlıktır. Kurumların bünyelerinde bulundurduğu bilgiyi değerlendirmeleri, anlamaları ve güvenliği için gerekli önlemleri almaları gerekmektedir (Kılıç Aksu ve Ark., 2015). Hastanelerde bilgi güvenliği politikalarının oluşturulması ve uygulanmasından yöneticiler sorumludur. Ancak HBYS kullanan çalışanlara da önemli sorumluluklar düşmektedir. Sağlık kurumlarında bilgi güvenliği tehditlerinin büyük bölümünün çalışanlardan kaynaklanabildiği de bildirilmektedir (Appari, 2010). Bu açıdan çalışanların bu konuda gerekli eğitimler ile bilinçlendirilmesi büyük önem taşımaktadır (İleri, 2018).

Ülkemizde sağlık hizmetlerinin sunumunda bilginin elektronik ortama aktarıldığı, kurumlar ve sağlık çalışanları arasında paylaşımının giderek arttığı bir süreç yaşanmaktadır. "Türkiye Sağlıkta Dönüşüm Programı" kapsamında sağlık hizmetlerinde ana başlıklardan biri olan Sağlık Bilgi Sistemleri ile birlikte köklü değişimler yaşanmıştır. Elektronik sağlık kayıt

sisteminin bir parçası olan Aile Hekimliği Bilgi Sisteminin oluşturulması, Tele-Tıp projesinin uygulanması, doktor veri bankasının oluşturulması, klinik uygulamalarda uluslararası hastalık sınıflamasının kullanılması, farklı kurumlar arasında verilerin entegrasyonunun sağlanması gibi bileşenlerin uyum içinde çalışabilmesi için bir sağlık bilgi sistemine ihtiyaç duyulmaktadır(https://sbu.saglik.gov.tr Erişim Tarihi: 05 Ağustos 2018).

Hastaneler tıbbi hataları azaltmak, hizmet kalitesini artırmak, maliyet etkinliği sağlamak, zamanında karar verme ve verimliliği artırmak için teknolojiyi kullanmaya ihtiyaç duymaktadır (Masrom, 2015). Sağlık sektöründe yapılan dijital dönüşüm ile bakım ve hizmet kalitesi de yükselmiş ve maliyetlerin düşmesi sağlanmıştır (http://www.resmigazete.gov.tr, Erişim Tarihi:06 Ocak 2019).Bilgi teknolojilerinin sağlık sektöründe kullanımı bu açıdan pozitif etki yaratmıştır (İsmail, 2010). Günümüzde sağlık kuruluşlarında hastaların anamnezi, teşhisi, tedavi planı, tahlil sonuçları ve randevu durumu gibi bilgiler teknoloji kullanarak dijital ortamda kayıt altında tutulmaktadır. Bireylerin sağlık verileri dijital ortama ve sanal arşivlere taşındığı için daha kolay ulaşılmakta ve teşhis ve tedavi süreçlerinin daha hızlı yapılması sağlanmaktadır.

Bilgi ve iletişim teknolojilerindeki gelişmeler, bazı riskleri de beraberinde getirmiştir. Bu bağlamda bilgi güvenliği ve mahremiyetin korunması hem bireysel hem de kurumsal açıdan büyük önem taşımaktadır (Küzeci, 2010).

2.1. Teknoloji Kavramı

Teknoloji insan tarafından ve insanın ihtiyaçlarının karşılanması amacıyla üretilmiştir. İnsanlık var olduğu günden bu yana tecrübelerini üretime çevirmiş, öncelikle basit makine ve aletler üreterek başladığı teknoloji gelişimi, bugün ki seviyesine getirmiştir (Anderson, 2007).

Hayatın her aşamasında, insanın işini kolaylaştıran teknolojinin faydaları göz ardı edilemez. Gelişen teknoloji sağlık anlamındaysa insan sağlığına önemli katkılar sunabilecek imkanları barındırmaktadır. Eskiden ölümcül sonuçlar doğuran hastalıkların teşhisleri artık saniyeler içinde yapılabilmektedir. Zor ve riskli ameliyatlar teknolojinin katkısı ile çok daha kolay bir hale gelmiştir. Sonuç olarak teknoloji teşhisten tedaviye, bilgi yönetim sistemlerine varan sayısız kolaylıklar sağlamaktadır(Sevimli, 2018).

2.2.Sağlık ve Bilgi İletişim Teknolojileri

Günümüzde bilgi iletişim teknolojilerinin sağlık hizmetlerinin sunumuna, sağlık eğitimine ve araştırmalara entegrasyonun kaçınılmazdır. Bu teknolojiler hem klinik hem de idari süreçleri desteklemektedir. Sağlık alanındaki tıbbi uygulamalar ile birlikle teknoloji işbirliğinin sağladığı güçlü bir yapılanmadır. Disiplinler arası iletişimi arttırılarak hizmet sunumunun niteliğini değiştirmiştir(Mumcu, 2011). Sağlık hizmetleri sunumu gerçekleştiren kurumlar ile beraber yazılım ve donanımdaki gelişmeler hem idari hem klinik iş süreçlerine önemli katkılar sağlamıştır. Bu gelişmeler tıbbi kayıtlarda mahremiyet, verinin bütünlüğü gibi konuların ön plana çıkmasına da neden olmuştur. Günümüzde, E-sağlık uygulamaları ve elektronik sağlık kayıt sistemleri uygulamaları, sağlık alanındaki temel uygulamalar arasında yer almaktadır (Işık 2014). Sağlıkta bilgi ve iletişim teknolojileri, verinin uygun bir biçimde işlenmesini sağlamaktadır. Bu açıdan sağlık hizmetleri sunumunda ve stratejik yönetiminde etkin rol oynamaktadır. Günümüzde bilgi iletişim teknolojileri kaliteli, etkin ve verimli hasta bakımı için gerekli desteği sağlamaktadır. Teknolojik iyileştirmeler, internet ağı ve veri tabanı uygulamaları sayesinde, taşınabilir elektronik cihazlar, elektronik sağlık kayıtları ve yeni yazılımlar ile sağlık hizmetlerinin birçok sürecinde önemli değişiklikler olmuştur (Mumcu, 2011).

2.3. Türkiye Sağlıkta Dönüşüm Programı

Türkiye'de sağlık alanında yapılan yenilikler teknolojinin gelişimi ile hız kazanmıştır. Türkiye, Dünya Sağlık Örgütü (DSÖ) üyesi olan bir ülkedir ve bu örgütün 21.yy hedeflerini benimseyen ülkelerin başında gelir. Sağlıkta Dönüşüm Programı (SDP) ile birlikte ileri seviyede, çağdaş ve kaliteli sağlık hizmetlerini adil ve hakkaniyetli bir şekilde tüm vatandaşlarına hizmet sunabilen, etkin mali koruma sağlayabilecek ve finansal olarak sürdürülebilir ve sağlam temellere dayandırılmış bir sistem inşa etmek amaçlanmıştır(Gülşen, 2017).

Sağlıkta Dönüşüm Programı ile başlayan bu önemli reform süreci, gerekli finansal kaynak oluşturulması, ihtiyaç olan teknolojik ekipmanların tedarik edilmesi, insan kaynakları probleminin çözülüp sağlık personeli ihtiyacının karşılanması, Dünya Sağlık Örgütünün hedefleri doğrultusunda sağlık hizmeti sunumunun gerçekleştirilebileceği uygun fiziki şartlara sahip sağlık kuruluşlarının yapılması ve uygun teknoloji ile hizmet verilmesi amaçlanmıştır(Çiftçi 2016).

SDP ile beraber teknoloji önem kazanmıştır. E-sağlık, E-reçete, E-order, Tele-Tıp, E-arşiv gibi paylaşımın kolay olduğu, çalışanların işini kolaylaştıran sistemler kullanılmaya

başlanmıştır. Hastanın verilerini kolay şekilde ve daha az maliyetle, ayrıca daha uzun süreli saklanabileceği bir yapı olmuştur. Sağlıkta dönüşüm programı ile beraber günümüzdeki halini alan sağlık teknolojileri ile dizayn edilmiş sağlık kuruluşlarında, bilginin kolay ulaşılabilir olmasının yanında önemli riskler de ortaya çıkmaya başlamıştır. Bu teknoloji verileri daha hızlı ulaşılabilir hale getirmiştir. Bu sayede bilginin paylaşımı kilometrelerce uzaktaki kişilerce bile rahatça ve hızlıca ulaşımını sağlanabilir hale gelmiştir. Bilginin izinsiz ve yetkisiz kişiler tarafından kullanılabileceği, kaybedebileceği ya da şeklinin değiştirebileceği gibi riskleri de beraberinde getirmiştir. Böylelikle bilgi güvenliği ve mahremiyet kaçınılmaz olarak en kritik konular olmuştur (Kılıç Aksu ve Ark., 2015).

Bilgi ve iletişim teknolojilerinin kullanımı ile yöneticiler daha etkili, daha nitelikli ve daha hızlı sağlık hizmetini sunabilme fırsatı yakalamışlardır. Tele-Tıp uygulamaları ve robotik cerrahi uygulamaları ile kesintisiz hizmet sunumu söz konusu olmuştur(Baraz, 2015).

2.3.1. E-Sağlık Projesi

E-sağlık; verimli ve kaliteli sağlık hizmeti sunumunda, ulaşılabilirliğin artırılması için bilgi ve iletişim teknolojilerinin en etkili biçimde kullanılmasıdır. Sağlıkta dönüşüm programı ile önem kazanan E-sağlık sisteminin kullanımını, ulusal sağlık bilgi sistemine uyum sağlaması ve geliştirilmesini sağlamak amacıyla Türkiye Sağlık Bilgi Sistemi (TSBS), Sağlık Bakanlığı çatısı altında sivil toplum kuruluşları, üniversiteler ve özel sektörün istişareleri ile temelleri atılmıştır (Kılıç Aksu ve Ark., 2015).

E-sağlık; sağlık hizmetlerinin etkin ve verimli sunulabilmesi, vatandaşın hizmetlere hızlı erişiminin sağlanması, sağlık sektöründe yer alan tüm paydaşlar ile veri paylaşımının sürdürülebilir olması, artan hasta beklentilerinin ve taleplerinin karşılanabilmesi için bilgi ve iletişim teknolojilerinin sağlık sektöründe kullanılması anlamına gelmektedir (Akça 2014). E-sağlık uygulamalarının temelinin atılması da Sağlık Bilgi Sistemi ile olmuştur (Sevimli, 2018).

Türkiye sağlık bilgi sistemi hedefleri;

- Sağlık alanında gelişmeler konusunda ulusal ve uluslararası entegrasyonu gerçekleştirmek amacıyla, ‘‘Veri Sözlüğü ve Standartları’’ nın oluşturulması,
- Sağlık kayıtlarının doğum ile başlayıp yaşam boyu elektronik ortamda saklanmasını sağlanması amacıyla tek bir numara sistemine dayanan ‘‘Kişisel Sağlık Tanımlayıcısı’’ nın oluşturulup hayata geçirilmesi,

- Bağışıklama, tanı ve tedavi prosedürleri, ulusal kanser kayıtları gibi kişisel sağlık verilerini toplamak hedefiyle, birinci, ikinci ve üçüncü basamak sağlık hizmetleri için öncelikli ‘‘Sağlık Veri Modeli ve Minimum Sağlık Veri Setleri’’ nin belirtilmesi,
- Elektronik ortamda depolanan kişisel sağlık kayıtlarının önemli seviyede artması sebebiyle ‘‘Kişisel Verilerin Mahremiyet ve Güvenliği’’nin sağlanmasına yönelik yasal ve teknolojik tedbirlerin alınması,
- Sağlık tehditlerinin zamanında belirlenmesi amacıyla, bulaşıcı hastalıklar ağı gibi ülke düzeyinde uluslararası sistemler ile entegre ‘‘Erken Uyarı Sistemleri’’ oluşturup uygulanabilirliğinin sağlanması,
- Sağlık hizmetlerine erişimde sorun yaşanan bölgelerde iletişim ve bilgi teknolojilerinin mesleki alanda kullanılması için ‘‘Tele-Tıp’’ uygulamalarının yaygınlaştırılması olarak sıralanabilir.

Her bir bireyin kendi sağlık bilgilerine ulaşabildiği, doğum ile başlayan, tüm ömründe, sağlıkla alakalı verilerden oluşmuş, evrensel standartlarla entegre, karar destek sistemleri ile desteklenen, işlevsel bir veri tabanının oluşturulması sağlanmıştır. Türkiye genelini kapsayan bir iletişim ağında paylaşılması, iletilmesi ve Tele-Tıp uygulamalarına ulaşan teknolojilerin mesleki tecrübeyle kullanılabilmesini temel alıp ‘‘Ulusal Sağlık Bilgi Sistemi (USBS)’’nin kurulması önemli bir adımdır (Sağlık Bakanlığı, 2016). Sağlık hizmeti sunumunda, mali ve idari tüm verilerini de kayıt edebilecek bir biçimde oluşturulmuştur. E-sağlık projeleri ile sağlık hizmeti sunan kurumlarda hizmet verimliliğini artırmak amaçlanmaktadır. E-sağlık projelerinin temel hedefleri şu şekilde sıralanabilir (Sevimli, 2018):

- Sağlıkta veri standardizasyonun oluşturulması,
- Elektronik kişisel sağlık kayıtlarının oluşturulması,
- Mali kaynakları tasarrufunun sağlanıp verimliliğinin artırılması,
- Bilimsel çalışmalara destek sunulması,

Bilgi ve iletişim teknolojilerinin etkili kullanımı kullanıcılara önemli kolaylıklar sağlamıştır. Bilgi sistemi kullanıcısının ihtiyaç duyabileceği her türlü bilgiye rahatlıkla erişebilmesi tahlil ve tetkiklerin yeniden yapılmasına gerek kalmadan, maliyet ve zaman açısından önemli tasarrufların sağlandığı görülmüştür (Göktaş , 2017).

2.3.2. Elektronik Kayıt Sistemi (E-Arşiv)

Teknolojinin gelişimi öncesinde elektronik kayıt sistemi kullanılmadan her türlü veri, dosyalar şeklinde arşivlenir, depolarda saklanır, ulaşılması gerektiğinde ise sorunlar yaşanırdı (Odacıoğlu, 2016). Hasta dosyalarının saklanmasında her zaman somut veriler, kağıt grubu gibi fiziki olarak yer kaplayan dosyaların yıpranması önemli sonuçlardandır. E-arşiv ile bu sorunlar ortadan kalkmış olup önemli derecede kolaylıklar sağlanmıştır. Herhangi bir

hastanede, geçmişteki hasta verilerine, saniyeler içerisinde ulaşılabiliyor olmak doğru teşhis, tedavi ve izlem süreçlerine önemli katkılar sağlamaktadır. Bu teknolojiler ile beraber E-arşiv sistemin sayesinde her türlü bilgi daha kolay ulaşılabilir, daha güvenli, daha uzun süre saklanabilir, az maliyetli ve en önemlisi hastanın sağlığın geliştirilmesinde etkin biçimde katkı sağlayabilmektedir (Odacıoğlu, 2016).

Bireylerin ömürleri süresince sağlık durumları ile ilgili bilgilerini kayıt altında olan sistem ‘‘Elektronik Sağlık Kaydı (ESK) sistemi’’dir (Işık, 2014). Sağlık hizmetlerinde elde edilen verilerin temeli, kişiye ait özel verilerden oluşmaktadır. Bunlar; sosyo-demografik veriler, finansal veriler, hasta kimlik verileri ve klinik verilerdir (Tekin, 2016).

Finansal veriler sağlık hizmetinin sunumunun maliyeti ile ilgili tüm veriler için kullanılabilen bir tanımdır. Her türlü hasta ödemesini ya da hastanın aldığı hizmet için genel ya da özel sağlık sigortaları aracılığıyla ödenen ve istenildiğinde ulaşılabilecek biçimde kayıtlı olan veriler bütünüdür. Hastanın kimlik verileri, hastanın sağlık kuruluşuna sağlık hizmeti sunumu için giriş yaptığı anda hastayı tanımlamak ve takip etmek için verilen provizyon numarasıdır. Bu numara aracılığıyla hasta takip edilir, tüm verilerine kolayca ve hızlıca bu numara aracılığıyla ulaşılabilir. Kısacası hem tanımlayıcı hem de takip edilmeyi sağlayan etkin bir araçtır. Klinik veriler ise hastanın tanı ve tedavisini içeren her türlü veridir. Erişim izni olan herkes tarafından ulaşılabilen hastanın tanı ve tedavisi, düzenli takibi, tıbbi ve laboratuvar bulguları, görüntüleme sonuçları, ameliyat raporları ve epikrizleri ifade eder (Sevimli, 2018).Sonuç olarak ESK; dijital ortamda hasta veri havuzunun oluştuğu, verinin depolanıp saklandığı, güvenli şartlarda değişiminin sağlanabildiği ve erişim izni olan başka kullanıcıların kolayca ulaşabileceği bir sistemdir. Anamnez, fizik muayene sonuçları, konsültasyonlar, laboratuvar ve görüntüleme sonuçları, tedavi protokolleri ve ilaç uygulamalarına ait bütün bilgiler bu sistemin parçasıdır. ESK’ da sağlık hizmeti alan tüm hastalar için kullanılmış olan ilaçların listesi, dozları, tedavi süresince kesilen ilaçlar, yeni başlananlar, ek reçete sayılarına ait bilgilere ulaşılabilmek mümkündür (Mumcu, 2011).

Sağlık hizmetlerinde EKS’ a ihtiyaç duyulma ve talep edilme sebepleri ve sağlık hizmetlerinin etkin sunumundaki önemi şöyle sıralanabilir (Mumcu, 2011):

- Hasta güvenliğini, hizmetin kalitesi ve verimliliğini artırma,
- Kağıt kullanımı ile ilgili sorunlar oluşan ve depolama zorluğuna çözüm üretme,
- Gelişen teknolojiden yararlanma ihtiyacı,

- Politika yapıcıların talepleri ve projeleri,
- Mali açıdan tasarruf ve kaynakların etkin kullanımı,

Elektronik sağlık kayıtlarının doğru şekilde saklanması ve korunması için aşağıdaki aşamaların yapılması gerekmektedir;

- Sürdürülebilirliğin sağlanması için kayıtların devamlılığının olması ve uygun görülen sıklıkta bakımlarının yapılması gerekmektedir.
- Yazılımının korunması ve sistemsel önlemlerin alınması önem taşımaktadır.
- Sisteme yönelik teknik şartnameye mutlaka güvenirlik ve bakım garantisi de eklenmelidir.
- Elektronik ortamlarda depolanan sağlık kayıtları her durumda, her yerde ve her dönemde doğumdan ölüme kadar düzenli ve bağlantılı kayıt altında tutulup saklanmalıdır.
- Güvenlik önlemleri tehditlere karşı kararlı ve hızlı koruyucu tepki verebilmelidir (Sevimli, 2018).
- Sistemde kayıtlı olan özel ve değerli verilerin zarar görmesi ya da kaybolmasını engellemek amacıyla uygun şekilde yetkili kişilerce bilinen korunaklı yerlerde yedeğinin olması da gerekmektedir(Işık 2014).

ESK; insanların özellikli ve kullanışlı, değerli bilgilerinden oluşmuştur. Aynı zamanda hekimlerin ve diğer sağlık çalışanlarının iş akışını destekler ve bu kayıtlara ait çıktıları kolaylıkla raporlamaktadır (Işık 2014). Sonuç olarak; ESK sistemi veri bütünlüğü ve güvenliği sağlanarak veriyi işlemeyi sağlayan bir yapılanmadır (Mumcu, 2011).

2.3.3. Tele-Tıp Uygulaması

Sağlıkta Dönüşüm Programının amacı, yüksek kalitede uygun maliyetlerde, insan kaynakları sorunu yaşanmaksızın hizmet sunabilmektir (Korkmaz, 2018),(Kılıç, 2016).

Sağlık hizmeti sunumunun iyileştirilmesini, bir yandan da eğitim ve yönetim açısından bilgi iletişim teknolojilerini etkin biçimde kullanarak uzaktan işlem yapma özelliğini içeren sağlıkla ilgili her türlü etkinlikler, hizmetler ve sistemleridir. Tele-Tıp uygulamalarını ilk

kullanan ülkeler; Kanada, Amerika, İngiltere, Avustralya, Hollanda ve Almanya'dır (Korkmaz, 2018).

Tele-Tıp Uygulaması günümüzde tıbbın tüm alanlarına entegre edilmiştir. İlk olarak tele-radyoloji, tele-patoloji, tele-dermatoloji, tele-konsültasyon, tele-psikiyatri, tele-evde bakım ve tele-cerrahi gibi alanlarda kullanılmaktadır.

Ayrıca tele-evde bakım kapsamında; hastaların kontrolleri sağlanıp ilaç uygulamaları konusunda doğru yönlendirmenin sağlanması da mümkündür. Tele-Tıp uygulaması sayesinde, farklı merkezlerde olan uzmanlar birbirleri ile hızlı şekilde bilgi alış verişinde bulunup hizmetin kalitesini arttırabilmektedir. Bu uygulama sayesinde insan kaynakları kısıtlılığı sorunu azalmıştır. Tedaviye erişim süresi kısalmış, hizmet kalitesi artmış ve maliyetler düşmüştür (Korkmaz, 2018).

Sonuç olarak Tele-Tıp uygulaması ile beraber, uzaktan hasta takibi, tedavi uygulamaları, hasta eğitimi, sağlıklı ve hızlı bilgi alışverişi, uzmanlık istenilen durumlarda uzman görüşü alınabilmesi, maliyetlerinin azaltılması hastaların evde takibi sayesinde hastane doluluk oranlarında azalmalar gibi birçok alanda faydalarının olduğu bildirilmiştir (Kılıç Aksu ve Ark., 2015).

2.3.4. E-Nabız Kişisel Sağlık Kaydı Sistemi

E-nabız sistemi ile tüm bireylerin sağlık bilgileri, tek veri tabanı üzerinde depolanabilmektedir. E-nabız, güvenlik sisteminin yardımıyla, sağlık verilerinin yalnızca hasta ve hastanın izin verdiği kişilerle paylaşılmasına imkan sağlayan bir sistemdir (Sağlık Bakanlığı, 2016). E-nabız; hastanın, muayenesinin, tetkik sonuçlarının, tedavisinin, ilaç kullanımının ya da görüntüleme sonuçlarının nerede ne zaman yapıldığına bakılmaksızın tek sistem üzerinden tüm verileri aynı anda birbiriyle ilişkili olacak şekilde bir bütün olarak ulaşılmasını sağlayan kullanışlı bir kişisel veri ulaşım sistemidir. Bu teknolojik uygulama sayesinde bireyler kişisel sağlık bilgilerine ulaşma olanağı bulmaktadır. Ancak kamu ve özel sektör kapsamına tam bir veri bütünlüğü yoktur. Bu teknolojik sistem sayesinde bireyler istediği zaman ulaşmak istediği kişisel sağlık verilerine, hızlı ve doğru biçimde, bütünlük içerisinde ulaşabilecek kişisel sağlık durumunu takip etme ihtiyacı olduğunda, ilgili kişilerle paylaşma olanağı bulmaktadır. Her türlü tahlil, radyolojik görüntüleme sonuçları, laboratuvar sonuçları, ilaç kullanımı bilgisi, daha önce alınan tedaviler gibi sonuçları sistemde hastanın erişebileceği şekildedir (Sevimli, 2018).

3. BİLGİ GÜVENLİĞİ VE MAHREMİYET

3.1. Bilgi Kavramı

Bilgi, bir kurum için değerli olan ve bu nedenle korunması gerekli olan her türlü işlenmiş ve yorumlanmış veridir. Başka bir deyişle bilgi, organizasyonların oluşumu için gereken girişim, sermaye, toprak ve insan gücüne ek olarak beşinci olan temel bir varlıktır. Günümüzün değişen şartlarında varlığını sürdürmek isteyen her kurum temel yönetim fonksiyonlarının (planlama, örgütleme, yöneltme, koordinasyon, denetleme) başarı ile yürütülebilmesi için bilgiyi kullanmak zorundadır (Kılıç Aksu ve Ark., 2015).

Toprak, emek ve sermaye üretim faktörlerinin en geleneksel halidir. Bilginin öneminin kavranması küresel ekonominin odak noktası haline getirmiştir. Bilgi; düzenli bir biçimde belirli bir çerçevede başka bir alıcı ile paylaşılan işlenmiş ve yorumlanmış veridir (Koçdar, 2016). Bilgi sistemi ise; bilgilerin toparlanıp depolanıp işlenip yorumlanıp dağıtımı ve erişimi gibi süreçleri barındıran bir yapıdır. Profesyonel kurumların amaçlarına ulaşabilmesi için günlük işlemlerini tamamlayabilmeleri ve uzun vadeli planlar yapması için bu sisteme ihtiyaç duymaktadır (Işık, 2014).

Veri özümlenmemiş ve yorumlanmamış gözlemler, gerçekler anlamına gelirken, bilgi işlenmiş ve yorumlanmış, sistematik veri olarak tanımlanmaktadır (Mumcu, 2011). Veri tek başına düşünüldüğünde yarar sağlama özelliği bulunmamaktadır. Bilgi ise; belirli bir hedef ya da vazife için, biçim ve içeriği uygun olan faydalı, kullanıma hazır ve paylaşılabilir bir özelliktedir(Sevimli, 2018).

Bilgi sistemlerinde bilginin oluşum süreci; girdi, işlem, çıktı, depolama ve dağıtım olmak üzere farklı basamaklardan oluşmaktadır. Girdi aşamasında, ham veriler toplanıp süreç ya da işleme aşamasına aktarılır (Akca,2014). Bunun ardından belirli bir amaç için toparlanan bu ham veriler anlamlı bir biçim haline dönüştürülür (Sevimli, 2018). Çıktı, yani sonuç evresinde ise anlamlı bir bilgi haline ulaşan bu veriler, bu bilgiyi kullanacaklar ile paylaşılır. Çıktılar sistemdeki tüm üyeler tarafından irdelenerek ve doğrulanmak amacıyla geri bildirimlerde bulunur. Ayrıca girdi olarak tekrar sürecin ilk aşamasına döner (Işık, 2014). Bilgiyi var etmek, kullanıcısı ile paylaşmak, korumak ve planlanan iş sürecini tamamlamak olarak tanımlanan bilgi yönetimi; bilginin organizasyon içinde etkin sürede paylaşılmasını sağlar. Bu

aşamalar sayesinde verimsizlik ve zaman kaybı gibi olumsuz sonuçlar önlenmiş olur (Mumcu, 2011).

3.2.Bilgi Güvenliği

Bilgi güvenliliği, verinin yetki sahibi olmayan kişilerin erişimini, değiştirilmesi ya da veriyi silmesinden korumaktır. Bu bilgilerin yetkisiz ve izinsiz kişilerden korunmasıdır (Sevimli, 2018). Bilgi güvenliliği, gelişen teknoloji ile kurumlarda bilgi sisteminin kullanımıyla daha da önemli hale gelmiştir. Bilgi saklama aracı olarak kağıt kullanıldığı dönemler de bilginin korunabilmesi için daha çok fiziksel önlemler ön plandayken gelişen teknolojiyle beraber fiziksel önlemler önemini yitirmeye başlamış yerini ise daha teknolojik koruma yöntemlerine bırakmıştır. Bu teknolojik ilerlemeler ile bilginin CD, DVD, USB ya da internet ortamlarında depolanmasına ve paylaşılmasına kolaylık sağlanırken, gerek bilişim sitemlerinin bağlantı ihtiyaçları sebebiyle gerekse bilinçsiz ve eğitimsiz kullanıcı kaynaklı bilginin güvenlilik ihlalleri önemli bir konu haline gelmiştir (Whitman, 2012).

Bilgi güvenliliğine duyulan ihtiyacın farkındalığı sonrasında ise güvenliğin sağlanması için bilinçli, eğitimli personelin varlığı büyük önem taşımaktadır. Bu bakış açısıyla bilgi güvenliliğinin korunması ancak aşağıdakilerin gerçekleştirilmesi ile mümkün olabilmektedir;

Gizlilik: Veriye sadece yetkili kişi tarafından, yetki çerçevesinde ulaşabilmesidir.

Bütünlük: Verinin bütünlük içinde sağlamaktır.

Erişilebilirlik: İhtiyaç halinde, gerekli olan doğru veriye, yetkili kişinin, yetki sınırlılıkları çerçevesinde en hızlı şekilde ulaşabilmesini garanti etmektir.

Sağlık hizmetlerinde bulunan verinin korunması, sağlık çalışanları ve hastalar için önemli bir konudur. Hastalar, verilerinin korunmasını ve devlet tarafından güvence altına alınmasını isterler (Park, 2017). Ülkemizde sağlık hizmetlerinde bulunan verilerin korunması için 20.10.2016 tarihinde 29863 numaralı Resmi Gazetede yayınlanan ve Sağlık Bakanlığı Mevzuatı Yönetmeliklerinden olan "Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik" ve 29677 numaralı Resmi Gazetede yayınlanan'' Kişisel Verilerin Koruması Kanunu'' kullanılmaktadır (https://www.mevzuat.gov.tr Erişim Tarihi: 24.03.2019). Bu yönetmeliğin ve KVKK' nın amacı ülkemizde bulunan sağlık kurumlarındaki kişisel verilerin korunması, mahremiyetin sağlanması, bu bilgilerin kaydedilmesi, toplanması ve denetimlerinin yapılması ile güvenliğinin sağlanması için gereken usul ve esasların düzenlenmesidir (Dülger, 2016). Bu yönetmelik bireylerin kişisel sağlık verilerinin işlenmesi, aktarılması, korunması ile ilgilidir. Veri alma sürecinde ise hastanın kendisinin

bilgilendirilmesi esastır. Bunun yanı sıra hastanın teşhis, tedavi ve diğer bütün süreçlerde mahremiyetinin korunması ve bilgi güvenliğinin sağlanması açıkça belirtilmektedir. Bilginin gizliliği, kanunun izin verdiği durumlar dışında hiçbir istisnai durum altında ve hiçbir nedenle ihlal edilemez ve bilgiler açıklanamaz (http://www.resmigazete.gov.tr Erişim Tarihi:06 Şubat 2019). Bu bağlamda 28103 sayılı Resmi Gazetede yayınlanan Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesinde, Sağlık Bakanlığının görevleri kapsamında bilginin toplanması, değerlendirilmesi, raporlanması ve paylaşılması süreçlerinde bilgi güvenliğin sağlanması için gerekli tedbirlerin belirlemesini amaçlamıştır (http://www.resmigazete.gov.tr, Erişim Tarihi:06 Ocak 2019)

Bu sürecin yönetiminde insan faktörü en önemli unsurdur. Kurumlardaki tıbbi ve idari birim çalışanları bilgi güvenliği ve mahremiyetin sağlanması konusunda üzerine düşen görevi yerine getirmeli ve süreçler yetkili birimlerce denetlenmelidir (Er, 2007). Ayrıca verilerin sahipleri olan hastalar veri kullanımına itiraz etme hakkına da sahiptirler. Bunun için hastanın onamının alınması ve gerekli denetlemelerin yapılması önemlidir (http://www.ttb.org.tr Erişim Tarihi: 19 Eylül 2018)

Bilgi güvenliğinin sağlanması için alınan tedbirler; bilginin gizlilik, bütünlük ve erişilebilirlik çerçevesinde değerlendirilerek kurum içinden ya da kurum dışından bilinçli veya kazayla oluşabilecek tüm tehlikelerden korunmasını içermektedir (https://bilgiguvenligi.saglik.gov.tr Erişim Tarihi: 01 Ocak 2019).

Sağlık kurumlarında kullanılan bilgi iletişim teknolojileri, bilgiye erişim konusunda çalışanların kimliklerini de denetlemektedir. Bunun için farklı yöntemler kullanılmaktadır. Bunlardan ilki parola ya da kimlik numarası gibi bir denetleme aracının kullanılması, ikincisi sisteme tanımlanan manyetik kart gibi denetleme araçlarının kullanılması ve sonuncusu ise bireylerin biyolojik özelliklerini tanımlayan, parmak izi, göz taraması gibi unsurlarla kimlik saptama amacıyla kullanılan biometrik yöntemlerdir (Akgül, 2015).

Kurumsal açıdan bakıldığında bu konuda kurumsal politikaların oluşturulması ve çalışanlara eğitimlerin verilmesi kritik önem taşır. Kullanıcı eğitimlerinde sistemi verimli kullanırken, olası riskler, bu risklere yönelik müdahaleler ve korunma yöntemleri konusunda da bilgiler aktarmak gerekmektedir (Dodge, 2007), (Wang, 2013). Kılıç Aksu ve Arkadaşları çalışanların bilgi güvenliği politikaları hakkında farkındalığının oluşu ve çalışanlara uygun ve yeterli bilgi güvenliği eğitiminin verilmesi konusunda benzer görüşlere sahip olup, bilgi güvenliği eğitimin önemini açıkça vurgulamışlardır (Kılıç Aksu ve Ark., 2015). 2018 yılında

Sağlık Bakanlığı tarafından yayımlanan Bilgi Güvenliliği Farkındalık Bildirgesinde de bilgi güvenliliğinin önemi ve nelere dikkat edilmesi gerektiği açıkça belirtilmiş olup bilgi güvenliği eğitiminin gerekliliği vurgulamıştır (https://bilgiguvenligi.saglik.gov.tr Erişim Tarihi: 01 Ocak 2019).

3.2.1. Bilgi Güvenliğini Etkileyen Faktörler

Bilgi güvenliğinin gerçekleştirilmesinden, bilginin kullanıcısı, yönetici ya da sahibi olan kişiler sorumlu olurlar. Bilgi güvenliğinin ihlali için tehdit oluşturan durumlar ise; kurumun zarar görmesine neden olabilecek tüm sebeplerdir. Tehditler; kurum içi, kurum dışı, doğal kaynaklı tehdit ve insan kaynaklı tehdit olarak düşünülmektedir (Kılıç Aksu ve Ark., 2015).

İnsan Faktörü

Bilgi güvenliğinin temelinde, bilginin kullanıcısı ve sahibi olan insan vardır. İnsanlar veriyi bilgiye dönüştürür, bilgiyi depolar, güvenliği için gerekli önlemi alırlar ve korurlar. Teknoloji ne kadar gelişirse gelişsin, bilginin kullanıcısı olan insan aracılığıyla ancak tam bir bilgi güvenliği sağlanabilir. Bilgi güvenliğinde önemli yere sahip olan insan aynı zaman da bilgi için büyük de bir tehdit olduğu düşünülmektedir (Kılıç Aksu ve Ark., 2015).Bilgi güvenliği tehditleri içerisinde tehditlerden biri de iç tehdittir. Kurum içerisinde çalışan tüm personellerin gerek bilinçli gerekse bilinçsiz ihmalleri kaynaklı oluşabilecek her türlü risk durumudur. Tehdit çeşitleri arasında önemli bir orana sahiptir. Verinin tamamı ile yetkileri ölçüsünde, kurum çalışanlarına emanet edilir. Çalışanların bilinçsizliği, bilgi güvenliği bağlamında farkındalık eksikliği gibi etkenler önemli bir risk ve tehdit sebebidir(Sevimli, 2018).

Güvenlik olaylarını 6 ana başlık altında açıklanabilir;

Çalışan Olumsuz Tarafları: Çalışanın veriyi amacı ve yetkisi dışında, uygunsuz kişi ve kişilerce paylaşıp karışığında menfaat elde etmek istemesidir.

Taklit: Bir kişinin başka bir kişi ya da kurumun verisini kendisinin gibi tanıtmasıdır.

Kayıp: Verinin ihmal nedeniyle kaybı ya da sanal ortamlarda depolanan verinin silinmesidir.

Sızma/Nüfuz Etme: Sisteme yetkisiz ve izinsiz kişilerin, kurum dışından giriş sağlamasıdır.

Hırsızlık: Depolama araçlarında saklanan ya da sanal ortamlarda depolu verilerin kasıtlı bir biçimde çalınmasıdır.

Yetkisiz Açıklama(ifşa): Kişinin onayı ve bilgisi olmadan kişisel verilerinin yetkisiz kişilere sunumu ve paylaşımıdır (Kılıç Aksu, 2015).

3.2.2. Bilgi Güvenliğinin Sağlanması

Bilginin güvenliğinin sağlanması ancak gerekli önlemlerin alınması ile sağlanabilir. Başta fiziki önlemler olmak üzere yetkilendirme sürecinin doğru yönetimi, karmaşık şifre kullanımı ile sağlanır. Veriler için gerekli fiziki ortam hazırlandıktan sonra yetkili kişilerin haricinde bu veriye erişmeleri engellemek amacıyla kullanıcı adı ve karmaşık şifrelerle erişim mümkün kılınmalıdır. Teknolojik önlemler ile bilgi güvenliği sağlanabilir. Ancak bilgi güvenliğinin tam anlamıyla sağlanması için bilginin kullanıcısı olan insan faktörü devreye girmektedir. Kullanıcının eğitimi ve farkındalığın seviyesi çok önemlidir. Bilgi güvenliğinin sağlanmasının en önemli halkası insandır. Anti-virüs sistemleri, güvenlik duvarları, yedekleme, erişim denetimi, kullanıcı eğitimleri ve farkındalık gibi güvenlik zincirinin tüm halkasının tamamlanması ile mümkündür (Kılıç Aksu ve Ark., 2015).

3.3. Mahremiyet

Mahremiyet kavramı; hasta için bir haktır. Onam vermeden kimse ile verinin paylaşılmamasıdır. Mahremiyet tek başına ele alındığında değerli ve özel bir kavramdır. Bilgi yönetimi perspektifinde mahremiyet kavramı kişinin maddi değerlerine, kendisiyle ilgili özel bilgilere manevi değerlerine başka kişilerin ulaşmasına sınır koyduğu zamanlarda bu kavram devreye girmektedir. Mahremiyet kavramının yakından ilişkili olduğu diğer kavramlar sır ve gizlilik kavramlarıdır (Burhanettin ve ark. 2018). Her geçen gün artan teknoloji ve yeni bilgilerin varlığı bilgiye her anlamda ve her yerde ulaşmanın kolaylığı, verilerin kolay elde edilmesi, toplanması ve işlenmesini kolaylaştırdığı için kişilerin mahremiyetleri tehlikeye girmektedir (Sevimli, 2018).

3.4. Bilgi Yönetimi

Bilgi yönetimi, organizasyon verilerini yararlı bilgi haline getirilerek bunları doğru zamanlarda, doğru kimselerin, istenilen her yerden ulaşılabilmesini sağlayıp, organizasyonun iş süreçlerinde verimliliğini artırmaya çalışmak, tekrarlanan işlemlerin tamamının teknolojik araçlarla yapılmasını sağlamak amacıyla yapılan bir dizi teknolojik işlemlerdir (Kılıç Aksu, 2015).

Bilgi yönetiminin temel amaçları ise şöyle sıralanabilir;

- Organizasyon için yeni bilgiler üretmek, sunmak ve korumak
- Örgütsel karar verme sürecinde bilginin kullanılması
- Öğrenen organizasyon olmak
- Kurum için değerli bilgiler edinmek ve kurumun rekabet gücünü artırmak
- Bilgiyi korumak, doğru sunmak ve denetlemek

Bilgi yönetimi, öğrenmeyi, bilgi paylaşımını ve bilgi teknolojilerini kullanmayı motive eden, kurumsal bir kültüre ihtiyaç duymaktadır. Bu bağlamda, öğrenen örgüt ile bilgi yönetimi arasında önemli bir bağ olduğu düşünülmektedir (Kılıç Aksu ve Ark., 2015).

3.5. Kullanıcı Kavramı ve Eğitimi

Kullanıcı kavramı, bilgi güvenliğinin en önemli faktörü olarak yerini korumaktadır. Kurumlar değerli verilerini korumak için gerek sistemsel, gerek teknolojik gerekse yönetimsel bir sürü önlem almaktadırlar. Yalnız alınan önlemler çok güçlü önlemler de olsa asıl bilgiyi koruyacak olan kişi, kullanıcı yani insandır. Dolayısıyla kullanıcıya verilen farkındalık eğitimleri, sorumluluk yükler. Bilgileri koruması gerekliliğini kullanıcıya hatırlatır ve denemeye yardımcı olur (Ekiz, 2017).

4.HASTANE BİLGİ YÖNETİM SİSTEMLERİ ve BİLGİ GÜVENLİĞİ

4.1. Hastane Bilgi Yönetim Sistemleri (HBYS)

Hastaneler topluma sağlık hizmeti sunma misyonunda olan karmaşık bir iletişim ağına sahip kurumlardır. Nitelikli iş gücü ile sağlık hizmeti sunan hastaneler, tüm paydaları ile de yakın ilişki içerisindedir. Günümüzde pahalı yatırımlar olan hastaneler arasındaki rekabet artmış gerek hasta gerekse kurumun değerli verilenin korunma ihtiyacını da beraberinde getirmiştir. Bu süreçleri yönetmede, Hastane Bilgi Yönetim Sisteminin (HBYS) kullanımını zorunlu hale gelmiştir (İsmail, 2010).

HBYS aracılığıyla hastaneler, tüm hizmet alan hastaların tüm sağlık verilerini bu sistem üzerinde kayıt edip istenilen zamanda yetkisi olan kişilerce paylaşımını sağlayıp hastaların tedavilerinde hizmet alımı süreçlerine katkı sağlamıştır (Sevimli, 2018).

HBYS, sağlık kurumlarının çeşitli seviyelerinde karar alıcılara yardım sağlamak için veri toplama ve veriyi paylaşma fonksiyonlarını üstlenmiş, farklı kaynaklardan elde edilen verileri bütün olarak irdeleyip sunabilen teknolojik bir sistemdir. HBYS öncelikle, herhangi bir hastanedeki tüm tıbbi ve idari işlemlerin ve verilerin bütünleşmesini sağlamıştır. Kullanıcılar tarafından ana bir veri tabanına girilip kaydedilmesi ve korunması gerekli olan tüm çıktıların bu veri tabanından tekrar anlamlı bir şekilde geri alınmasını sağlayan, hastanelere zaman, işgücü, maddi kazanç ve en önemlisi doğru ve güvenilir istatistiki veri sağlayan bir yazılımlar bütünü olarak da tanımlanmaktadır (Kılıç Aksu ve Ark., 2015).

HBYS, özel ya da Kamu olmak üzere tüm sağlık kurum ve kuruluşlarında kullanılmaktadır. Hastanın tüm verilerinin kaydedildiği ve ihtiyaç duyulduğunda yetkili kişilerce rahatlıkla ulaşılıp kullanılabilen, hem hastanın hem de kullanıcın hatta en önemlisi kurumların süreçlerini kolaylaştıran, hızlı ve maliyet avantajı sağlayan bir sistemlerdir. Hastanın farklı kaynaklardan elde ettiği veriler dahil tüm bilgilerini içerir. Görüntüleme sistemi sonuçları, laboratuvar sonuçları, kişisel bilgiler, hastalık öyküsü, anamnezler gibi verilerin entegre olduğu bir sistemdir(Mumcu, 2014).

HBYS' nin hayata geçirilmesi ile elde edilen kazanımlar kısaca şu şekilde sıralanmaktadır:

- En iyi hasta bakımını sağlamak,
- Her türlü iş süreçlerinde zamandan tasarruf elde etmek ve verimliliği arttırmak,

- Sağlık sunucuları arasındaki bilgi paylaşımını hızlandırarak ve en iyi tedaviyi oluşturmak,
- Depolama alanı tasarrufu sağlamak,
- Kağıtsız hastane yapılanması ile eski verilere kolaylıkla ulaşımı sağlamaktır (Mumcu G).

4.1.1. Hastane Bilgi Yönetim Sistemlerini Oluşturan Temel Bileşenler

HBYS' nin kullanılması tanı ve tedaviyi desteklemeye yönelik sistemler ile yönetim fonksiyonlarını desteklemeye yönelik sistemler olmak üzere iki ana başlık altında incelenebilir. Hasta kayıttan klinik bilgilere, laboratuvar ve görüntüleme sistemleri sonuçlarından anamnezlere kadar hastanın tüm tedavisi sürecinin ilaç kullanımlarının orderların kayıt altına alındığı ve takip edilebildiği modüllerin bütünüdür. Klinik süreçlerin denetlenmesinin yanında yönetimsel süreçlerin de denetlenmesi söz konusudur. Satın alma süreçleri kayıt sistemi, envanter ve lojistik takip sistemleri, yönetimsel raporlama ve süreç takip sistemleri, personel ve mali kayıt sistemleri gibi modüller yer almaktadır(Kılıç Aksu, 2015).

HBYS, yönetime bilgi sağlamak, takip ve denetimi kolaylaştırmak amaçlı oluşturulan modülleri kapsar. Hastanın kaydından günlük işlere ve raporlamalara kadar her türlü yönetime yararlı işin yapılmasını sağlar. Hastanın hastaneye adım atışından itibaren tüm süreçlerinin nitelikli biçimde kayıt altına alınmasını sağlayan bu sistemde bulunan modüller aşağıdaki gibi sıralanabilir (Kılıç Aksu ve Ark., 2015);

- Hasta kabul modülü,
- Randevu işlemleri modülü,
- Poliklinik modülü,
- Hasta yatış, yatan hasta takip ve hasta çıkış işlemleri modülü,
- Girişimsel işlemler – ameliyathane modülü,
- Fatura – vezne modülü,
- Hekim modülü,
- Elektronik order verme ve elektronik reçeteleme,
- Karar destek modülü en sık kullanılanlardır.

4.1.1.1. Hastane Bilgi Yönetim Sistemlerinde Bilgi Güvenliği

Günümüz teknolojisinin katkılarıyla artık, sağlık hizmeti sunumunu gerçekleştiren kurum ve kuruluşların bu sunumu kaliteli, zamanında ve doğu şekilllerde gerçekleştirmek için HBYS kullanımı kaçınılmaz olur. Sürecin kusursuz ilerlemesi ve takibi için HBYS kullanımı büyük bir öneme sahiptir. Hastaların, çalışanların ve kurumun özel bilgilerini rahatlıkla depolayıp paylaşılmasına imkan sunan bu sistemin kullanım süreci kadar güvenlik ihtiyacı da doğmaktadır (Mumcu, 2014). Yıllar boyunca sistemde, sıralı biçimde kayıt edilen bu gizli bilgilerin güvenliği için başta yönetsel ve sistemsel önlemler olmak üzere kullanıcının eğitim ve farkındalığının oluşması büyük önem taşır (Kılıç Aksu ve Ark., 2015).

Sağlık hizmetleri sunumunda hastanede etkin kullanılan bu sistem ile hastanın verilerinin doğru kaydedilmesi, doğru saklanmasını ve doğru tedaviye ışık tutmasını sağlamak esastır. Bir çok veriyi bir arada bulundurup birçok farklı kullanıcı tarafından aynı zamanda kullanılan bu sistem verilerin paylaşılmasını kolaylaştırıp sağlık hizmeti sunumunu nitelikli hale getirmiştir. Öte yandan da bu paylaşılması kolaylaşan ve ortak kullanıcılı bu sistem bilginin ciddi güvenlik risklerini de beraberinde getirmiştir (Sevimli, 2018). Bu noktada bilgi güvenliği eğitimi kritik önem taşımaktadır.

5.GEREÇ VE YÖNTEM

Araştırma evreni olarak İstanbul ilindeki açılışı 0-3 süre ile hizmet veren özel hastaneler seçilmiştir. Evreni temsil edebilecek nitelikte olduğu için İstanbul'da 28 Haziran 2017'de açılan özel bir hastane seçilmiştir. Belirlenen hastanenin yönetiminden çalışmanın yapılabilmesi için gerekli izin alınmıştır (Ek-1).

Bu araştırmada HBYS kullanan çalışanlarda bilgi güvenliği ve mahremiyet eğitimi etkilerinin değerlendirilmesi amaçlanmıştır. Araştırma kapsamında bilgi güvenliği eğitimi öncesi ve sonrası ön test ve son test yapılarak veriler toplanmıştır. Ön test yapıldıktan sonra bir hafta sonra ön teste katılan çalışanlara iş süreçlerini aksatmayacak bir biçimde belirli aralıklarla hastane seminer salonunda eğitimler verilmiştir. Bu eğitim süreci üç iş gününde tamamlanıp bir hafta sonrasında ise son test yapılmış ve veri toplama işlemi tamamlanmıştır.

Bu hastanenin toplam 403 çalışanı bulunmaktadır. HBYS kullanan sayısı ise 313'tür. Kurumsal politika gereği tüm çalışanların bu eğitimi alması planlanmıştır. Ön teste katılan sayısı 256 kişi katılmıştır. Ancak hastanedeki iş sürecinin aksamaması açısından araştırma kapsamında çalışmaya katılmayı kabul eden hem ön teste hem eğitime hem de son teste katılan 100 kişi araştırmaya dahil edilmiştir. Araştırmaya katılım gönüllülük esasına dayanmaktadır. Bunun için katılımcılara araştırmanın amacı ve önemi hem yazılı hem de sözlü bilgilendirme yapılıp ve katılımcıdan imzalı onam formu alınmıştır.

Araştırmada veri toplama aracı olarak anket yöntemi kullanılmıştır. Bu araştırmada, araştırmanın amacına uygun olarak Kılıç Aksu (2015)' nun çalışmasında yer alan Bilgi Güvenliği Ölçeği kullanılmıştır. Ölçeğin; *Güvenlik politikası*, *Örgütsel güvenlik*, *Güvenlik uygulamaları*, *Erişim ve Yetkilendirme* ile *Hizmet sunumu* alt boyutları bulunmaktadır (Kılıç Aksu ve Ark., 2015).

Bu araştırmada, araştırmanın amacına uygun olarak ve kurumun izin verdiği ölçüde, Kılıç Aksu' nun çalışmasında yer alan Bilgi Güvenliği Ölçeği' nin, *Güvenlik politikası*, *Güvenlik uygulamaları*, *Erişim ve Yetkilendirme* olmak üzere 3 alt boyutu kullanılmıştır.

Araştırmanın Hipotezleri

Hipotez 1: Bilgi güvenliği eğitimi öncesi ve sonrasındaki bilgi güvenliği ölçek alt grup puanlarında yöneticiler arasında fark yoktur.

Hipotez 2: Bilgi güvenliği eğitimi öncesi ve sonrasındaki bilgi güvenliği ölçek alt grup puanlarında tıbbi birim çalışanları ve idari birim çalışanları arasında fark yoktur.

Veri Analizi

Araştırmada verileri SPSS 22 programı ile çözümlenmiştir. Araştırmanın hipotezleri doğrultusunda veri analizleri gerçekleştirilmiştir. Yapılan bu araştırmada öncelikle bilgi güvenliği eğitiminin etkililiğinin test edilmesi amaçlanmıştır. Bu amaç doğrultusunda katılımcıların Bilgi Güvenliği Ölçeği alt boyut puanları ve ön test ve son test puanları çalışılan pozisyona göre karşılaştırılmıştır. Bununla birlikte daha önce HBYS için eğitim alıp almama, cinsiyet, yaş, öğrenim durumu ve kurumda çalışma sürelerine göre katılımcıların Bilgi Güvenliği Ölçeği' nden aldıkları puanların istatistiksel açıdan anlamlı fark gösterip göstermediğinin de belirlenmesi amaçlanmıştır. Normal dağılım gösteren verilerin bağımsız değişkenlerin kategori sayısı iki olduğunda Eşleşmemiş T testi, tek bir örneklemden farklı ölçümler alındığında Eşleşmiş T testi, bağımsız değişkenlerin kategori sayısı ikiden fazla olduğunda tek yönlü varyans analizi (ANOVA) ile veriler değerlendirilmiştir.

Bilgi Güvenliği Eğitimi

Gelişen teknoloji ile beraber bilgiye ulaşmak, kullanmak, saklamak ve başka alıcılara ulaştırmak da kolaylaşmıştır. Bu durum birçok önemli riski beraberinde getirip bu bağlamda kullanıcılara büyük bir sorumluluk da yüklemektedir (Ganbat, 2013). Bilgi güvenliği ve mahremiyete yönelik eğitimin içeriğinde aşağıda belirtilen konulara ek olarak çalışanların ön test sonrasında ihtiyaç duydukları konularda eklenecektir (İleri, 2018).

- KVKK,
- Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması HakkındaYönetmelik
- Sağlık Bakanlığı Bilgi Güvenliği Yönergesi
- Sağlık Bakanlığı Hasta Hakları yönetmeliği
- Bilgi güvenliğine yönelik koruma yolları (Erdinç, 2017):
    - ✓ Biometrik verilere ilişkin projeler, eğitimler
    - ✓ Ses tanıma
    - ✓ Göz tarama, iris tarama
    - ✓ Yüz tanıma
    - ✓ Avuç içi tarama

- ✓ Parmak izi

Kullanıcılara bu temellerde oluşturulan bilgi güvenliği eğitimi belirlenen verilmiş olup eğitimin kullanıcıların bilgi güvenliğine verdiği önemin artması hedeflenmiştir.

6. BULGULAR

Araştırma grubunun çoğunun erkek katılımcılardan (%76) oluştuğu görülmektedir. Tıbbi birim çalışanlarının %80,3'ü (n=53), idari birimde çalışanların ise %67.7' sini (n=23) erkek çalışanlardan oluşmaktadır (Tablo 1).

Katılımcıların yaş dağılımları incelendiğinde %64'nün 20-30 yaş arasında, %21'nin 31-40 yaş arasında olduğu görülmektedir. Katılımcıların en son mezun oldukları okul incelediğinde %59'nun üniversite, %40'nın lise olduğu görülmektedir. Katılımcılardan sadece bir kişi ortaokul mezunudur. Araştırmanın yapıldığı kurumda çalışma süresi incelendiğinde ise %51'i 0-1 sene, %37'si 1-2 sene ve %12'si ise iki yıldan fazla görev yaptıklarını belirtmişlerdir (Tablo 1).Araştırmaya katılanlardan yönetici olanların sayısı 4 olduğu için ilk hipotez test edilemedi.

Tablo 1. Katılımcıların Demografik Özellikleri

		Tıbbi		İdari		Toplam	
		n	%	n	%	n	%
Cinsiyet	Kadın	13	19,70	11	32,30	24	24,00
	Erkek	53	80,30	23	67,70	76	76,00
Yaş	20-30	43	65,20	21	61,80	64	64,00
	31-40	11	16,70	10	29,40	21	21,00
	41-50	5	7,60	1	2,90	6	6,00
	51 ve üzeri	7	10,60	2	5,90	9	9,00
Öğrenim Durumu (En son mezun olunan okul)	Ortaokul			1	2,90	1	1,00
	Lise	25	37,90	15	44,10	40	40,00
	Üniversite	41	67,10	18	52,90	59	59,00
Kurumda çalışma süresi	0-1 yıl	39	59,10	12	35,30	51	51,00
	1-2 yıl	20	30,30	17	50,00	37	37,00
	>2 yıl	7	10,60	5	14,70	12	12,00

Bilgi Güvenliği Ölçeği alt boyutları ön test çalışılan pozisyona göre karşılaştırıldığında; tıbbi ve idari birim çalışanları arasında anlamlı fark tespit edilmedi ($p>0.05$)(Tablo 2).

Tablo 2. Bilgi Güvenliği Ölçeği Alt Boyutları Ön test Puanlarının, Çalışılan Pozisyona Göre Karşılaştırılması

	Gruplar	n	Ortalama	Std. Sapma	p
Ön Test - Güvenlik Politikaları Alt Boyutları	**Tıbbi**	66	20,34	7,52	0.923
	İdari	34	20,5	7,02	
Ön Test - Erişim ve Yetkilendirme Alt Boyutları	**Tıbbi**	66	13,39	4,59	0.236
	İdari	34	12,29	3,88	
Ön Test - Güvenlik Uygulamaları Alt Boyutu	**Tıbbi**	66	8,90	3,15	0.412
	İdari	34	8,35	3,23	

Bilgi güvenliği ölçeği alt boyutlarında, tıbbi birimde görev yapan katılımcılar için ön test–son test puanları kıyaslamalarına baktığımızda, bilgi güvenliği eğitimi öncesi ve sonrası anlamlı farklılıklar tespit edildi (p<0,005). Tüm alt boyutlarda azalmanın olduğu görüldü(Tablo 3).

Tablo 3. Bilgi Güvenliği Ölçeği Ön Test-Son Test Puanlarının Tıbbi Birimde Görev Yapan Katılımcıların Karşılaştırılması

		n	Ortalama	Std. Sapma	p
Güvenlik Politikaları Alt Boyutları	**Ön Test**	66	20,34	7,52	**0.000***
	Son Test		14,56	3,19	
Erişim ve Yetkilendirme Alt Boyutları	**Ön Test**	66	13,39	4,59	**0.000***
	Son Test		10,71	1,87	
Güvenlik Uygulamaları Alt Boyutu	**Ön Test**	66	8,9	3,15	**0.000***
	Son Test		6,22	1,58	

Bilgi güvenliği ölçeği alt boyutlarında, idari birimde görev yapan katılımcılar için ön test ve son test puanları kıyaslamalarına baktığımızda; *Güvenli Politikaları Alt Boyutunda* ve *Güvenlik Uygulamaları Alt Boyutu*, bilgi güvenliği eğitimi öncesi ve sonrası anlamlı farklılıklar tespit edildi (p=0.000;p=0.001). *Erişim ve Yetkilendirme Alt Boyutunda* ise anlamlılığa erişmedi (p=0.07),(Tablo 4).

Tablo 4. Bilgi Güvenliği Ölçeği Ön Test-Son Test Puanlarının İdari Birimde Görev Yapan Katılımcılarda Karşılaştırılması

		n	Ortalama	Std. Sapma	p
Güvenlik Politikaları Alt Boyutları	**Ön Test**	66	20,05	7,02	**0.000***
	Son Test		14,88	2,69	
Erişim ve Yetkilendirme Alt Boyutları	**Ön Test**	66	12,29	3,88	0,07
	Son Test		10,94	1,89	
Güvenlik Uygulamaları Alt Boyutu	**Ön Test**	66	8,35	3,23	**0.001***
	Son Test		6,11	1,64	

*p<0.05

Bilgi Güvenliği Ölçeği alt boyutları son test çalışılan pozisyona göre karşılaştırıldığında; tıbbi ve idari birim çalışanları arasında anlamlı fark tespit edilmedi (p>0.05)(Tablo 5).

Tablo 5. Bilgi Güvenliği Ölçeği Son Test Puanlarının Çalışılan Pozisyona Göre Karşılaştırılması

	Gruplar	n	Ortalama	Std. Sapma	p
Son Test - Güvenlik Politikaları Alt Boyutları	**Tıbbi**	66	14,56	3,19	0.617
	İdari	34	14,88	2,69	
Son Test - Erişim ve Yetkilendirme Alt Boyutları	**Tıbbi**	66	10,71	1,87	0.566
	İdari	34	10,94	1,89	
Son Test - Güvenlik Uygulamaları Alt Boyutu	**Tıbbi**	66	6,22	1,58	0.747
	İdari	34	6,11	1,64	

Tıbbi birim çalışanlarına bakıldığında; Bilgi Güvenliği Ölçeği alt boyut puanlarına göre ön test ve son test puanlarının; *Güvenlik Politikaları Alt Boyutları* incelendiğinde; kadınlarda *Güvenlik Politikaları Alt Boyutları* (ön test puanı: 22,07±7,97 ve son test puanı: (14,07 ±2,36) ve *Güvenlik Uygulamaları Alt Boyutu* puanlarının(9,53 ± 3,09 ve 8,75±3,18 sırasıyla.) son testte, ön teste göre daha düşük olduğu belirlendi (p:0.003; p=0.000). *Erişim ve Yetkilendirme Alt Boyutunda* ise anlamlı farklılık tespit edilmedi (p=0.106) (Tablo 6). Erkeklerde ise, son testte tüm puanlarda anlamlı şekilde düşmenin olduğu görüldü/tespit edildi (p<0.05) (Tablo 6).

Tablo 6. Tıbbi Birim Çalışanlarını Bilgi Güvenliği Ölçeği Alt Boyut Puanlarının Eğitim Öncesi Ve Sonrası Cinsiyete Göre Değerlendirilmesi

		n	Ortalama	Standart Sapma	p
Kadın	**Ön Test Güvenlik Politikaları Alt Boyutu**	13	22,07	7,97	**0.001***
	Son Test Güvenlik Politikaları Alt Boyutu	13	14,07	2,36	
	Ön Test Erişim ve Yetkilendirme Alt Boyutu	13	13	3,76	0,106
	Son Test Erişim ve Yetkilendirme Alt Boyutu	13	10,69	1,93	
	Ön Test Güvenlik Uygulamaları Alt Boyutu	13	9,53	3,09	**0.003***
	Son Test Güvenlik Uygulamaları Alt Boyutu	13	5,76	1,09	
Erkek	**Ön Test Güvenlik Politikaları Alt Boyutu**	53	19,92	7,43	**0.000***
	Son Test Güvenlik Politikaları Alt Boyutu	53	14,67	3,37	
	Ön Test Erişim ve Yetkilendirme Alt Boyutu	53	13,49	4,8	**0.000***
	Son Test Erişim ve Yetkilendirme Alt Boyutu	53	10,71	1,88	
	Ön Test Güvenlik Uygulamaları Alt Boyutu	52	8,75	3,18	**0.000***
	Son Test Güvenlik Uygulamaları Alt Boyutu	52	6,3	1,67	

İdari birim çalışanlarına bakıldığında; kadınlarda eğitim sonrası *Güvenlik Uygulamaları* alt boyutu puanında(5,36±0,92) eğitim öncesine (8,18±3,12) göre azalmanın olduğu belirlendi (p=0.020). İdari birim çalışanlarda erkeklerde ise eğitim sonrası hem *Güvenlik Uygulamaları Alt Boyutu* puanında (6,47±1.80) eğitim öncesine (8,43±3,35) göre azalmanın olduğu belirlendi hem de *Güvenlik Politikaları Alt Boyutları* puanında (15,39±2,58) eğitim öncesine (21,78±7,06) göre azalmanın olduğu belirlendi (p=0.011;p=0.001, sırasıyla). *Erişim ve Yetkilendirme Alt Boyutunda* hem kadınlarda hem de erkelerden anlamlı farklılık tespit edilmedi (p=0.677; p=0.079), (Tablo 7).

Tablo 7. İdari Birim Çalışanlarını Bilgi Güvenliği ölçeği Alt Boyut Puanlarının Eğitim Öncesi Ve Sonrası Cinsiyete Göre Değerlendirilmesi

		n	Ortalama	Standart Sapma	p
Kadın	**Ön Test Güvenlik Politikaları Alt Boyutu**	11	17,81	6,43	0,066
	Son Test Güvenlik Politikaları Alt Boyutu	11	13,81	2,71	
	Ön Test Erişim ve Yetkilendirme Alt Boyutu	11	10,63	2,83	0,677
	Son Test Erişim ve Yetkilendirme Alt Boyutu	11	10,36	2,06	
	Ön Test Güvenlik Uygulamaları Alt Boyutu	11	8,18	3,12	**.020***
	Son Test Güvenlik Uygulamaları Alt Boyutu	11	5,36	0,92	
Erkek	**Ön Test Güvenlik Politikaları Alt Boyutu**	23	21,78	7,06	**0.001***
	Son Test Güvenlik Politikaları Alt Boyutu	23	15,39	2,58	
	Ön Test Erişim ve Yetkilendirme Alt Boyutu	23	13,08	4,11	0,079
	Son Test Erişim ve Yetkilendirme Alt Boyutu	23	11,21	1,78	
	Ön Test Güvenlik Uygulamaları Alt Boyutu	23	8,43	3,35	**0.011***
	Son Test Güvenlik Uygulamaları Alt Boyutu	23	6,47	1,8	

Tablo 8'de tıbbi birim çalışanlarının eğitim düzeylerine göre bilgi güvenliği ve mahremiyet eğitiminin etkinliği değerlendirilmiştir. Hem lise hem de üniversite düzeyinde eğitim alan çalışanlarda, bilgi güvenliği ölçek alt boyut puanlarının anlamlı şekilde azaldığı belirlenmiştir ($p<0.05$).

Tablo 8. Araştırmaya Katılan Tıbbi Birim Çalışanlarının Bilgi Güvenliği Ölçeği Alt Boyut Puanlarının Eğitim Düzeylerine Göre Değerlendirilmesi

		n	Ortalama	Standart Sapma	p
Lise	**Ön Test Güvenlik Politikaları Alt Boyutu**	25	18,8	5,31	**0.000***
	Son Test Güvenlik Politikaları Alt Boyutu	25	14,4	3,25	
	Ön Test Erişim ve Yetkilendirme Alt Boyutu	25	12,76	3,73	**0.001***
	Son Test Erişim ve Yetkilendirme Alt Boyutu	25	10	1,47	
	Ön Test Güvenlik Uygulamaları Alt Boyutu	25	8,52	3	**0.000***
	Son Test Güvenlik Uygulamaları Alt Boyutu	25	5,96	1,69	
Üniversite	**Ön Test Güvenlik Politikaları Alt Boyutu**	41	21,29	8,53	**0.000***
	Son Test Güvenlik Politikaları Alt Boyutu	41	14,65	3,19	
	Ön Test Erişim ve Yetkilendirme Alt Boyutu	41	13,78	5,05	**0.000***
	Son Test Erişim ve Yetkilendirme Alt Boyutu	41	11,14	1,98	
	Ön Test Güvenlik Uygulamaları Alt Boyutu	41	9,15	3,26	**0.000***
	Son Test Güvenlik Uygulamaları Alt Boyutu	41	6,35	1,51	

Tablo 9'daidari birim çalışanlarının eğitim düzeylerine göre bilgi güvenliği ve mahremiyet eğitiminin etkinliği değerlendirilmiştir. Hem lise hem de üniversite düzeyinde eğitim alan çalışanlarda, bilgi güvenliği ölçek alt boyut puanlarının anlamlı şekilde azaldığı belirlenmiştir ($p<0.05$).Ancak *Erişim ve Yetkilendirme Alt Boyutunda* anlamlı fark tespit edilmedi ($p=0,864$)

Tablo 9. Araştırmaya Katılan İdari Birim Çalışanlarının Bilgi Güvenliği Ölçeği Alt Boyut Puanlarının Eğitim Düzeylerine Göre Değerlendirilmesi

		n	Ortalama	Standart Sapma	p
Lise	**Ön Test Güvenlik Politikaları Alt Boyutu**	15	20,68	6,06	**0.014***
	Son Test Güvenlik Politikaları Alt Boyutu	15	15,68	2,19	
	Ön Test Erişim ve Yetkilendirme Alt Boyutu	15	11,68	4,3	0,864
	Son Test Erişim ve Yetkilendirme Alt Boyutu	15	11,5	1,72	
	Ön Test Güvenlik Uygulamaları Alt Boyutu	15	9,25	4,04	**0.028***
	Son Test Güvenlik Uygulamaları Alt Boyutu	15	6,56	1,58	
Üniversite	**Ön Test Güvenlik Politikaları Alt Boyutu**	18	20,33	8,05	**0.005***
	Son Test Güvenlik Politikaları Alt Boyutu	18	14,16	2,99	
	Ön Test Erişim ve Yetkilendirme Alt Boyutu	18	12,83	3,65	**0.011***
	Son Test Erişim ve Yetkilendirme Alt Boyutu	18	10,44	1,97	
	Ön Test Güvenlik Uygulamaları Alt Boyutu	18	7,55	2,3	**0.010***
	Son Test Güvenlik Uygulamaları Alt Boyutu	18	5,72	1,63	

Tablo 10'daBilgi Güvenliği Ölçeği ön test puanlarının Hastane Bilgi Yönetim Sistemi kullanmak için eğitim alıp almama durumlarına göre bilgi güvenliği ve mahremiyet eğitiminin etkinliği değerlendirilmiştir. Eğitim alan ve almayan arasında fark tespit edilmedi ($p>0.05$). Ayrıca Hem lise hem de üniversite düzeyinde eğitim alan çalışanlarda, bilgi güvenliği ölçek alt boyut puanlarında anlamlı fark görülmemiştir ($p>0.05$).

Tablo 10. Bilgi Güvenliği Ölçeği Ön Test Puanlarının Hastane Bilgi Yönetim Sistemi Kullanmak İçin Eğitim Alıp Almama Durumlarına Göre Değerlendirilmesi

	Gruplar	n	Ortalama	Standart sapma	p
Ön Test - Güvenlik Politikaları Alt Boyutları	**Evet**	67	19.46	7.41	0.068
	Hayır	33	22.30	6.87	
Ön Test - Erişim ve Yetkilendirme Alt Boyutları	**Evet**	67	12.67	4.61	0.259
	Hayır	33	13.72	3.81	
Ön Test - Güvenlik Uygulamaları Alt Boyutu	**Evet**	67	8.55	3.24	0.458
	Hayır	33	9.06	3.04	

Tablo 11'deBilgi Güvenliği Ölçeği son test puanlarının Hastane Bilgi Yönetim Sistemi kullanmak için eğitim alıp almama durumlarına göre bilgi güvenliği ve mahremiyet eğitiminin etkinliği değerlendirilmiştir. Hem lise hem de üniversite düzeyinde eğitim alan çalışanlarda, bilgi güvenliği ölçek alt boyut puanlarında anlamlı fark görülmemiştir ($p>0.05$).

Tablo 12'deBilgi Güvenliği Ölçeği ön test puanlarının yaşa göre bilgi güvenliği ve mahremiyet eğitiminin etkinliği değerlendirilmiştir. Her yaş gurubundaki çalışanlarda, bilgi güvenliği ölçeği alt boyut puanlarında anlamlı fark görülmemiştir ($p>0.05$).Benzer şekilde son test puanlarında da fark tespit edilmedi ($p>0.05$)(Tablo 13).

Tablo 11. Bilgi Güvenliği Ölçeği Son Test Alt Grup Puanlarının Hastane Bilgi Yönetim Sistemi Kullanmak İçin Eğitim Alıp Almama Durumlarına Göre Değerlendirilmesi

	Gruplar	n	Ortalama	Standart sapma	p
Son Test - Güvenlik Politikaları Alt Boyutları	**Evet**	67	14.32	2.95	0.108
	Hayır	33	15.36	3.09	
Son Test - Erişim ve Yetkilendirme Alt Boyutları	**Evet**	67	10.73	1.96	0.643
	Hayır	33	10.90	1.70	
Son Test - Güvenlik Uygulamaları Alt Boyutu	**Evet**	67	6.17	1.63	0.923
	Hayır	33	6.21	1.55	

Tablo 12. Bilgi Güvenliği Ölçeği Tüm Boyutlarda Ön Test Puanlarının Yaşa Göre Ortalama, Standart Sapma Değerleri

	Gruplar	n	Ortalama	Standart sapma	p
Ön Test - Güvenlik Politikaları Alt Boyutları	20-30	64	20.78	7.84	0.305
	31-40	21	17.90	5.56	
	41-50	6	21.66	3.26	
	>51	9	22.66	8.45	
Ön Test - Erişim ve Yetkilendirme Alt Boyutları	20-30	64	13.26	4.69	0.285
	31-40	21	11.52	3.70	
	41-50	6	14.83	2.56	
	>51	9	13.55	4.00	
Ön Test - Güvenlik Uygulamaları Alt Boyutu	20-30	64	8.56	3.09	0.076
	31-40	21	7.85	2.66	
	41-50	6	10.00	1.89	
	>51	9	10.88	4.56	

Tablo 13. Bilgi Güvenliği Ölçeği Tüm Boyutlarda Son Test Puanlarının Yaşa Göre Ortalama, Standart Sapma Değerleri

	Gruplar	n	Ortalama	Standart sapma	p
Son Test - Güvenlik Politikaları Alt Boyutları	20-30	64	14.79	3.09	0.773
	31-40	21	14.76	3.44	
	41-50	6	14.50	2.07	
	>51	9	13.66	2.00	
Son Test - Erişim ve Yetkilendirme Alt Boyutları	20-30	64	10.71	1.93	0.353
	31-40	21	11.14	1.90	
	41-50	6	11.50	1.51	
	>51	9	10.00	1.50	
Son Test - Güvenlik Uygulamaları Alt Boyutu	20-30	64	6.14	1.75	0.723
	31-40	21	6.09	1.44	
	41-50	6	6.16	1.47	
	>51	9	6.77	0.66	

7. TARTIŞMA ve SONUÇ

Sağlık bilgi sistemleri, sağlık verilerini bilgiye dönüştürür, bilginin yönetilmesini sağlar ve paylaşım süreçlerinde etkin rol alır (Mumcu, 2013). Hasta kayıtlarının elektronik ortama kaydedilmeye başlamasıyla bilgi sistemlerinin önemi artmıştır (Sevimli, 2018). Elektronik kayıt sisteminin kullanımı, bilginin ulaşılabilirliğini ve paylaşımını kolaylaştırması ile beraber bilgi güvenliği ve hasta mahremiyeti bağlamında riskler oluşmaktadır (Kılıç Aksu ve Ark., 2015).

Sağlık hizmetinin sunumunda bilgi güvenliği ve mahremiyet dikkat edilmesi gereken bir konudur. Günümüz teknolojisinde Türkiye'de sağlık hizmeti sunumunda tüm hasta bilgilerinin elektronik ortamlarda depolanıp kolayca farklı kullanıcılarla paylaşılabildiği bir dönemdeyiz. Sağlıkta Dönüşüm Programı ile beraber, E-sağlık uygulamaları hız kazanarak evrakla sağlık hizmeti yerini daha çok dijital hizmet sunumu ve takibine bırakmıştır. Hastaneler ve birçok paydaşın dijital ortamdaki bu hasta bilgilerini yetki ve izin çerçevesinde kullanıp birbiri arasında paylaşımını sağlamaktadırlar. Hastanın kişisel bilgileri, ödeme bilgileri, iletişim bilgileri, bulaşıcı hastalık durumları, sosyal güvencesi laboratuvar sonuçları, tıbbi görüntüleme sistemleri sonuçları, ilaç kullanımları gibi hasta bilgileri, elektronik kayıt sisteminde depolanıp en sık paylaşılan bilgilerdir (Sevimli, 2018).

Bilginin mahremiyeti, güvenliği ve her an kullanıma hazır bir biçimde güncel olması günümüz ticari rekabet ortamında ciddi avantaj sağlarken şüphesiz hizmet kalitesini de artırmaktadır. Bu sebeple değerli olan bu bilgilerin güvenliği ciddi önem taşımaktadır. Bilgi güvenliğinin sağlanmasının ise artık sadece teknik önlemler ile mümkün olmadığı net olarak bilinmektedir. Bu süreçte kullanıcı faktörünün etkisi gün geçtikçe artmaktadır (Kılıç Aksu ve Ark., 2015).

Bu araştırmada, sağlık hizmetlerinin sunumunda yaygın olarak kullanılan hastane bilgi yönetim sisteminde, bilgi güvenliği ve mahremiyetin korunmasına yönelik eğitimin etkilerinin HBYS kullanan çalışanlar üzerinde etkisi değerlendirilmiştir.

Gelişen teknoloji ile beraber bilgiye ulaşmak, kullanmak, saklamak ve başka alıcılara ulaştırmak da kolaylaşmıştır. Bu durum birçok önemli riski beraberinde getirip bu bağlamda kullanıcılara ve yöneticilere büyük bir sorumluluk da yüklemektedir (Ganbat, 2013),(İleri, 2018), (Erdinç, 2017).

Araştırma kapsamında bilgi güvenliği ve mahremiyete yönelik eğitimin içeriğinde yer alan konular; KVKK, Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik, Sağlık Bakanlığı Bilgi Güvenliği Yönergesi, Sağlık Bakanlığı Hasta Hakları yönetmeliği, Bilgi güvenliğine yönelik koruma yolları olarak sıralanabilir. Yapılan araştırmada bilgi güvenliği eğitimi sonrasında tıbbi ve idari çalışanlarında *Bilgi Güvenliği Ölçeği*' nin, *Güvenlik politikaları, Erişim ve Yetkilendirme* ve *Güvenlik Uygulamaları Alt Boyutlarına* ait puanlarda anlamlı şekilde azalmanın olduğu görüldü. Bu durum eğitimin süreçteki etkisini göstermektedir. Kılıç Aksu ve arkadaşlarının araştırmasında kullanıcı kaynaklı sorunları önlemek için bilgi güvenliği eğitimin önemi vurgulanmıştır (Aksu 2015).

Günümüz teknolojisinin sağlık iletişimi ve elektronik kayıt bağlamında kullanımının yaygınlaşması bilgi güvenliğinin önemini ve bu konuda alınması gereken önlemleri konusunu da ön sıralara getirmiştir. Bilgi güvenliği konusunda yönetimsel önlemlerden teknolojik yapısal önlemlere, güvenlik yazılımlarına birçok önlemler alınabilmektedir (İleri, 2018).

Bilgi güvenliği kapsamında kritik öneme sahip olan kullanıcının ise bilgi güvenliği eğitimi alması ve bu bağlamda farkındalığının oluşturulması da gereklidir (Gebrasilase, 2011). Kullanıcının birçok veriye hızlıca ulaştığı ve paylaşabildiği günümüzde (Burhanettin ve ark., 2018), bilgi güvenliği eğitimleri ile kullanıcının farkındalığının arttırılmasının önemli olduğu unutulmamalıdır (Kılıç Aksu 2015). Bu açıdan eğitimin içeriği güncel olmalı ve kullanıcıların ihtiyaçlarını karşılayacak nitelikte olmalıdır.

Tıbbi ve idari birim çalışanları ön test ve son test puanları karşılaştırması sonucuna bakıldığında guruplar arasında anlamlı fark görülmemiştir. Hem tıbbi hem de idari birim çalışanları konuya gereken özeni benzer şekilde gösterdiği düşünülmektedir. Günümüzde kurumlar için tartışılmaz derecede önemli bir unsur olan bilgi güvenliği, en çok ihlal ve ihmal edilen bir olgudur. Bu ihmaller ciddi riskler oluşturduğu görülmüştür. Yasal sonuçlar başta olmak üzere mali kayıplar, hasta ve personel memnuniyetsizliği gibi kurumu ciddi zararlara uğratabilecek sonuçların olması söz konusudur. Bilgi güvenliliği ve mahremiyetin sağlanmasının amacı; bilginin yetkili kullanıcılar tarafından en hızlı biçimde kullanılmasını mümkün kılarken her türlü risklere karşı da korunmasını sağlamaktır. Kurumlarda bilgi güvenliği ve mahremiyetin sağlanması; bilinçli ve farkındalığı yüksek personelin varlığı, periyodik eğitim programları ve sürecin denetlenmesinin yanı sıra kurumsal politikalar ile sağlanabildiği unutulmamalıdır (Burhanettin ve ark., 2018). Bu açıdan tüm çalışanlar için önemli bir konudur.

Araştırmada HBYS eğitimi alan ve almayanlarda ön test ve son test alt boyut puanlarında anlamlı farklılık tespit edilmedi. Organizasyonlarda HBYS kullanımı ile maliyet avantajı oluşturmak, zaman tasarrufu sağlayıp zamanı etkin kullanma ihtiyacı, kaliteli hizmet üretebilmek ve sağlığın korunması ve geliştirilmesi gibi birçok amacın gerçekleştirilmesini sağlamıştır. Özellikle hastaya hizmet sunumunun doğru zamanda, doğru tedavinin uygulanmasını da imkan tanımıştır (Mumcu, 2014). Bu açıdan HBYS kullanıcı eğitimi büyük önem taşımaktadır.

Araştırmamızda HBYS eğitiminin, bilgi güvenliği ve mahremiyet sağlaması açısından yeterli olmadığı ve bilgi güvenliği ve mahremiyet eğitiminin HBYS eğitiminden farklı olması gerektiği düşünülmektedir. Bilgi güvenliği kurum kültürü oluşturulması, çalışanların farkındalığının arttırılması ancak belli aralıklarla yapılan bilgi güvenliği ve mahremiyet eğitimi ile mümkün olduğu düşünülmektedir. Tehditlerin hedefi;

- Yazılımlar
- Donanım araçları,
- Veriler,
- Depolama alanları olabilmektedir.

Gizliliğin kişisel boyutunu irdelediğimizde, bir kişinin ya da grubun kendilerine ait bilgileri hangi alıcıya hangi durumlarda ve nasıl iletileceğini, direk kişinin ya da grubun onayı ve izni ile olabileceği anlamına gelmektedir.

Bilgi güvenliği ihlalleri;

- İzinsiz ve yetkisiz erişim,
- Veriye zarar verme,
- Verinin bütünlüğünün bozulması ya da değiştirilmesi ile oluşur (Kılıç Aksu, 2015).

Bu açıdan HBYS eğitimi içeriğine veya ayrı olarak bilgi güvenliği ve mahremiyeti içeren bir eğitim programının kullanımının büyük önem taşıdığı unutulmamalıdır.

Tıbbi birim çalışanlarda bilgi güvenliği ölçeğinin tüm alt boyutlarda erkeklerin puanlarında olumlu şekilde azalmanın olduğu görülmüştür. Benzer şekilde kadınlarda da Güvenlik Politikaları ve Güvenlik Uygulamaları Alt Boyut puanlarında azalmaların olduğu görüldü. Kadınlarda Erişim ve Yetkilendirme Alt Boyutunda ise anlamlı bir değişikliğin olmadığı

görüldü. İdari birim çalışanlarında ise kadınlarda sadece Güvenlik Uygulamaları Alt Boyutunda erkeklerde ise tüm alt boyutunda azalmaların olduğu görüldü. Bilgi güvenliği ve mahremiyet tıbbi birim çalışanları için hastaya ait bilginin korunması açısından önemli olduğu, idari birim çalışanlarının ise kurumsal bilgilerin korunması açısından kullanıcıların sorumluluklarının olduğu unutulmamalıdır(Sevimli ve ark, 2018). Bu durumu kadınların bu konuda farkındalığının olması ile ilişkilendirebiliriz.

Tıbbi birim çalışanlarında farklı eğitim düzeylerine göre ön test son test puanlarında anlamlı şekilde azalmanın olduğu görüldü. Benzer durum idari birim çalışanlarında da gözlendi. Ancak idari birim çalışanlarının *Erişim ve Yetkilendirme Alt Boyutunda* lise düzeyinde azalmanın olmadığı tespit edildi. Bu grubun iş süreçleri arasında erişim yetkileri az olan çalışanlar olması ile ilişkili olabileceği düşünülmektedir.

Yaşa gruplarına göre Bilgi Güvenliği Ölçeği ön test ve son test alt grup puanlarında anlamlı farklılığın olmadığı belirlendi. Bu faktörün süreçte etkisi olmadığı görüldü. Gençler teknoloji kullanımına daha yatkın iken daha yaşlı grubun sistemi uzun süre kullanılmasın ile bağlantılı olarak bu sonucun çıktığı düşünülebilir.

Araştırma sonuçlarına göre, bilgi güvenliği ve mahremiyetin sağlanmasında eğitimin büyük önem taşıdığı görülmüştür. Sağlık yönetimi açısından bu konuda farkındalığın oluşması, bilgi güvenliği zafiyetine bağlı olarak oluşabilecek mali kayıpların önlenmesi yada hukuksal süreçler oluşmasının engellenmesi açısından öncelikli bir alan olarak görülmesi gerekmektedir. Kurumsal bilgi güvenliği politikasının oluşturulması ve çalışanlara düzenli olarak bu konuda eğitimlerin verilmesi ve denetlenmesi ile yöneticilerin proaktif yaklaşımı kritik önem taşımaktadır.

Sonuç

- Sağlık kurumlarında, bilgi güvenliğinin sağlanması için teknik koruma yöntemlerinin yeterli olmayacağı ve asıl faktörün kullanıcı olduğu görülmektedir. Bu sebeple donanımsal önemlerin yanında kullanıcı faktörünün kurumlar tarafından önemi yönünden farkındalığı arttırmak gereklidir.

- Sağlık yöneticileri kurumun özel bilgilerinin korunması için bilgi güvenliği politikaları oluşturulmalıdır. Süreçler, kullanıcı görev ve sorumlulukları açık ve net olarak açıklanmalı ve uygulamaya yönelik denetlemeler yapılmalıdır.

- Bilgi güvenliğinin sağlanmasında, riskler ve tehditlerin tamamı doğru biçimde tanımlanmalı ve bu bağlamda önlemler oluşturulmalıdır. İhtiyaç durumunda eylem planı ve yedekleme sitemleri hazır bulundurulmalıdır.

- Yalnızca teknik alt yapı oluşturmakla bilgi güvenliğinin sağlanamayacağı gerçeği artık kabul edilmelidir. Kullanıcı olan insan faktörüne verilen önemin artırılıp güçlü ve uygulanabilir kullanıcı eğitimleri hazırlanmalı ve belirli aralıklarla eğitim verilmeli, sonuçları ve uygulanabilirliği denetlenmelidir. Bilgi güvenliği bilinci her HBYS kullanıcısına benimsetilmeli ve farkındalık yaratılmalıdır.

- HBYS eğitiminin, bilgi güvenliği ve mahremiyet açısından yeterli olmadığı ve bilgi güvenliği ve mahremiyet eğitiminin HBYS kullanımı ile birlikte verilmesi gerektiği düşünülmektedir.

8. KAYNAKLAR

1. Akbolat M. Hastane Bilgi Sistemleri. İçinde: Sağlık Kurumlarında Bilgi Sistemleri, Ed: Ali Yılmaz, Anadolu Üniversitesi Yayınları, 2. Baskı, Eylül, Eskişehir, 2014, s.108-135.
2. Akca N. E-sağlık. İçinde: Sağlık Kurumlarında Bilgi Sistemleri, Ed: Ali Yılmaz, Anadolu Üniversitesi Yayınları, 2. Baskı, Eylül, Eskişehir, 2014, s.158-189.
3. Akgül , A. Kişisel Verilerin Korunması Bağlamında Biometrik Yöntemlerin Kullanımı Ve Danıştay Yaklaşımı, 2015.
4. Aldosarı B. An Evaluation Of EHR System Audit Functions In A Saudi Arabian Hospital. Journal Of Health Informatics In Devoloping Countries, 6(2), 2012 p.496-508.
5. Anderson J. G. Social, Ethical And Legal Barriers To E-Health. International Journal Of Medical Informatics, Vol:76, 2007 .p.480-483.
6. Appari A, Johnson M. E. Information Security And Privacy In Healthcare: Current State Of Research. Int. J. Internet And Enterprise Management, 6(4), 2010, p.279- 314.
7. Baraz B. A. Bilgi Güvenliği ve Yönetimi. İçinde: Büro Teknolojileri, Ed: Ekrem Özkul, Anadolu Üniversitesi Yayınları, 4. Baskı, Nisan, Eskişehir, 2015, s.138-163.
8. Baraz B. A. Bilgi İşleme Sistemleri Ve Mobil İletişim. İçinde: Büro Teknolojileri, Ed: Ekrem Özkul, Anadolu Üniversitesi Yayınları, 4. Baskı, Nisan, Eskişehir, 2015, s.112-136.
9. Burhanettin U., Mehmet Y., Sağlıkta Kalite Standartları Ve Bilişsel Mahremiyet, Selçuk Üniversitesi Sosyal Ve Teknik Araştırmalar Dergisi Sayı: 16, 2018, ss. 24-33.
10. Büyüköztürk, Ş., Kılıç Çakmak, E., Akgün, Ö. E., Karadeniz, Ş. Ve Demirel, F. Bilimsel Araştırma Yöntemleri. Ankara: Pegem Akademi, 2010
11. Büyüköztürk. Ş. Sosyal Bilimler İçin Veri Analizi El Kitabı (10.Baskı). Ankara: Pegem Akademi, 2009
12. Büyüköztürk. Ş., Çokluk. Ö. Ve Köklü. N. Sosyal bilimler için istatistik(8. Baskı). Ankara: Pegem Akademi, 2011
13. Calder A, A Business Guide To Information Security: How To Protect Your Company's It Assets, Reduce Risks And Understand The Law, KoganPage Publishers, 2005 p: 8.
14. Çiftçi F. Bostan. Sağlıkta Dönüşüm Programı Uygulamalarının Hastane Hizmetleri Üzerindeki Değişim Etkisi: Sağlık Çalışanlarının Görüşleri. SDÜ Sağlık Bilimleri Enstitüsü Dergisi Cilt 7, Sayı 2, 2016 (https://dergipark.org.tr Erişim Tarihi: 11.01.2019)
15. Çokluk, Ö, Şekercioğlu, G. Ve Büyüköztürk, Ş. Sosyal bilimler için çok değişkenli SPSS ve lisrel uygulamaları. Ankara: Pegem A Yayıncılık, 2012
16. Dodge, R. C., Carver, C., Ferguson, A. J. (PhishingFor User Security Awareness. Computers & Security, 26(1), 2007 p: 73-80.
17. Dülger M. V. Kişisel Verilerin Korunması Kanunu Ve Türk Ceza Kanunu Bağlamında Kişisel Verilerin Ceza Normlarıyla Korunması. İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi, 3(2), 2016, s.101-167.
18. Ekiz P. Sağlıkla ilgili Bilgilere Erişimde İnternetin Rolü, Marmara Üniversitesi Sağlık Bilimleri Enstitüsü, Yüksek Lisans Tezi, İstanbul,2017 (Danışman: Prof. Dr. Gonca Mumcu).
19. Erdinç. G.H, Bilgi Güvenliği, Kişisel Verilerin Korunması Ve Biometrik Verilerin İşlenmesine İlişkin Öneriler, Yüksek Lisans Tezi, İtü, 2017.
20. Ganbat O. (Bilgi Güvenliği Yönetim Sistemi ISO/IEC 27001 Ve Bilgi Güvenliği Risk Yönetimi ISO/IEC 27005 Standartlarının Uygulanması. Ege Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, İzmir, 2013 (Danışman: Prof. Dr. Ata Önal).
21. Gebrasilase T, Lessa F. L. Information Security Culture In Public Hospitals: The Case Of Hawassa Referral Hospital. The African Journal Of Information Systems, 3(3), 2011, p.71-86.

22. George, D., and Mallery, M. SPSS For Windows Step By Step: A Simple Guide And Reference, 17.0 Update (10a ed.) Boston: Pearson, 2010, Tabachnick, B.G. And Fidell, L.S. Using Multivariate Statistics (5th Edition), 2005 Boston [etc.]: Allyn And Bacon.
23. Göktaş B, Önder Ö, Duran M, Şakar S, Yılmaz M, Güler S, Çınar İ, Çamlıdağ T, Şenkal Y, Özdemir G, Türkiye'de Sağlık Bilgi Sistemleri Üzerinde bir Araştırma. Ankara Sağlık Bilimleri Dergisi 2017, 125-138.
24. Gülşen M.A, Yıldıran M. Sağlıkta Dönüşüm Programı Sonrasında Uygulanan Sağlık Regülasyonlarının Üniversite Hastanelerinin Mali Yapısına Etkisi, 2017.
25. Günay D. Teknoloji Nedir? Felsefi Bir Yaklaşım Yüksek Öğretim Ve Bilim Dergisi, 2017, s.194
26. Ismail, A., Jamil, A. T., Rahman, A. F .A., Bakar, J. M. A., Saad, N. M., Saadi, H. Theimplementation Of Hospital Information System (HIS) In Tertiary Hospitals In Malaysia: A Qualitative Study. Malaysian Journal of Public Health Medicine, 10(2), 2010.s, 16-24
27. Işık O. Sağlık Bilgi Sistemlerinin Gelişimi. İçinde: Sağlık Kurumlarında Bilgi Sistemleri, Ed: Ali Yılmaz, Anadolu Üniversitesi Yayınları, 2. Baskı, Eylül, Eskişehir, 2014 s.2-23.
28. İleri, Y. Y. Kurumsal Bilgi Kaynaklarına Erişimde Güvenlik: Hekimlerin Şifre Yönetimine Yönelik Bir Araştırma. Usaysad Dergisi, 2018.
29. Kılıç Aksu P., Çatar Ö., Şişman Kitapçı N., Köksal L., Mumcu G., Hastane Bilgi Yönetim Sisteminde Bilgi Güvenliğinin Sağlık Çalışanları Tarafından Değerlendirilmesi, Kişisel Sağlık Verileri Ulusal Kongresi, İstanbul, 2015.
30. Kılıç Aksu P., Kitapçı Şişman N., Çatar R. Ö., Köksal L., Mumcu G. An Evaluation Of Information Security From The Users' Perspective In Turkey. Journal Of Health Informatics In Devoloping Countries, 9(2), (2015) p.55-67.
31. Kılıç T. E-Sağlık Ve Tele-Tıp. Az Kitap Yayınevi. 1. Baskı, İstanbul, 2016
32. Kişisel Verileri Koruma Kurumu, Kişisel Verilerin Korunması Kanunu, 2016 (https://www.mevzuat.gov.tr Erişim Tarihi: 24.03.2019)
33. Korkmaz S, Hoşman İ, Sağlık Sektöründe Tele-Tıp Uygulamaları: Tele-Tıp Uygulama Boyutlarını İçeren Bir Araştırma. Usaysad Dergi, 2018, 4(3):251 -263, Araştırma makalesi, (http://saysad.org. Erişim Tarihi: 05.01.2019)
34. Küzeci E. Türkiye'de Kişisel Verilerin Korunması. İçinde: Bilişim Hukuku, Ed: Gökhan Güneysu, Anadolu Üniversitesi Yayınları, 1. Baskı, Aralık, Eskişehir, 2015, s.50-69.
35. Küzeci, E. Kişisel Verilerin Korunması. Ankra: Turhan Kitabevi, 2010
36. Masrom, M., & Rahimly, A. Overview Of Data Security Issues In Hospital Information Systems. Pacific Asia Journal Of The Association For Information Systems, 7(4), 2015.
37. Mumcu G. Elektronik Sağlık Kayıt Sistemi İçinde: Sağlık Hizmetlerinde Bilişim Teknolojisinin Uygulama Alanları, Ed: Deniz Şelimen, Gonca Mumcu, Bedray Yayıncılık, Ankara, 2011 s. 61-70.
38. Mumcu G., Köksal L., Şişman N., Çatar R. Ö. The Effectiveness and Outcomes Of Computerized Provider Order Entry In Emergency Care Department Of Private Hospitals. Journal Of Marmara University Institute Of Health Sciences, 3(2), 2013, p.83-90.
39. Mumcu G., Köksal L., Şişman N., Çatar R. Ö., Tarım M., The Effect Of Pharmacy Information Management System On Safety Medication Use: A Study From Private Hospitals In İstanbul. Marmara Pharmaceutical Journal, 18, 2014 p.1-4.
40. Odacıoğlu Y. Hasta Dosyaları Ve Elektronik Hasta Dosyaları. İçinde: Tıbbi Belgeleme, Ed: Nedim Ünal, Anadolu Üniversitesi Yayınları, 1. Baskı, Mayıs, Eskişehir, 2016, s.32-59.
41. Park, E.h., Kim,.J, Park, Y.S.,. The role of Information Security Learning And Individual Factors In Disclosing Patients Health Information. Computers & Security, 65, 2017.s,64-76.
42. Peltier, TR. Information Security Policies, Procedures, AndStandards: Guidelines For Fective Information Security Management. Crc Pres., 2016

43. Sağlık Bakanlığı Bilgi Güvenliliği Yönergesi, 2018. (https://bilgiguvenligi.saglik.gov.tr Erişim Tarihi: 01.09.2018)
44. Sağlık Bakanlığı, Bilgi Güvenliliği Farkındalık Bildirgesi, 2018. (https://bilgiguvenligi.saglik.gov.tr Erişim Tarihi: 04.10.2018)
45. Sağlık Bakanlığı. Kişisel Sağlık Sistemi Platformu ‘‘E-Nabız’’ Tanıtım Dokümanı. T.C. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü Yayını, Ankara, 2016.
46. Sevimli, E. Sağlık Yönetiminin Gelecekteki Paydaşlarından Bilgisayar Mühendisliği Öğrencilerinin Sağlık Bilgi Sistemlerini Bilgi Güvenliği Ve Hasta Mahremiyeti Açısından Değerlendirilmesi, Yüksek Lisans Tezi, Marmara Üniversitesi, İstanbul, (2018).
47. Tavşancıl, E. Tutumların Ölçülmesi Ve SPSS ile Veri Analizi. Nobel Yayıncılık: Ankara, 2005.
48. Tekin Ş. P. Sağlık Hizmetlerinde Bilgi ve Belge Yönetimi. İçinde: Tıbbi Belgeleme, Ed: Nedim Ünal, Anadolu Üniversitesi Yayınları, 1. Baskı, Mayıs, Eskişehir, 2016, s.2-30.
49. Tenğilimoğlu, D., Çelik, Y., Ülgü, M. Comparison Of Computing Capability And Information Systemabilities Of State Hospital Sowned By Ministry of Laborand Social Security And Ministry Of Health. Journal Of Medical Systems, 30(4), 2006 s, 269-275.
50. Tosun, Y. Güvenlik Politikaları, Ağ Güvenliği Projesi, 2004 (web.itu.edu.tr Erişim Tarihi: 28.01.2017)
51. Wang, Y., Liu, K., Zheng, L. Implementation And Application Of Electronic Medical Records In The Outpatient And Imergency Departments Of Hospitals. Chinese Medical Record English Edition, 1(10) , 2013. 446-450.
52. Whitman, M.E., Mattord, H.J.) Principles Of Information Security. 4th ed. Cengage Learning, 2012 s,35-73.
53. 2 Kasım 2011 Tarihinde 28103 Sayılı Resmi Gazete Yayınlanan ‘’Bilgi Güvenliği Politikaları Yönergesi’’ (http://www.resmigazete.gov.tr Erişim Tarihi:06.01.2019)

9.EKLER

Ek 1: Kurum İzni

MEHMET TOPRAK HASTANESİ

Sayın Özel Mehmet Toprak Hastanesi Yönetimi'ne;

Marmara Üniversitesi Sağlık Yönetimi programında yapmakta olduğumuz yüksek lisans çalışması için tek elden veri toplanması gerekmektedir. Bu amaçla İstanbul ilin'de faaliyet göstermekte olan özel hastanelerden seçilen örneklemde yer alan hastanenizin de araştırmada yer alması planlanmaktadır.

Elde edilen veriler bilimsel amaçlı kullanılacak ve üçüncü şahıslar ile araştırma etiği açısında paylaşılmayacaktır.

Akademik çalışmamıza katkınız ve desteğiniz için şimdiden teşekkür eder, çalışmalarınızda başarılar dileriz.

Prof. Dr. Gonca MUMCU
Tez Danışmanı

Gökhan ÖZASLAN
Araştırmacı

İletişim Bilgileri: ozaslangokan@hotmail.com
541 950 5642

Özel Mehmet Toprak Hastanesi
Cevizli Mh. Bağdat Cd. No : 547 Maltepe / İSTANBUL
T: +90 216 225 49 49 / F: +90 216 225 49 50
info@mehmettoprakhospital.com.tr

2

www.mehmettoprakhospital.com.tr

Ek 2: Kongre Başvurusu:

(?modul=bildirilerilistele)

(?modul=yeni_bildiri_gonder) (?modul=yeni_poster_gonder) (?modul=yeni_sergi_gonder)

Bildiri Detayları

Bildiri Numarası :

UTSAK2019-13

Başlık

BİLGİ GÜVENLİĞİ VE MAHREMİYETİN KORUNMASINA YÖNELİK EĞİTİMİN ETKİLERİNİN DEĞERLENDİRİLMESİ: BİR ÖZEL HASTANE UYGULAMASI - Evaluation of the Effects of Education for Information Security and Protection of Privacy: A Private Hospital Practice,

Kategori

Sağlık ve Spor Bilimleri (Poster)

Başvuru Durumu

Yeni Başvuru

Not

Ödeme:

Ödeme Yapılmamıştır / No Payments

Yazarlar

Araştırmacı Gökhan Özaslan, Prof.Dr. Gonca Mumcu,

Özet

ÖZET Günümüzde bilgi ve iletişim teknolojilerinin gelişimi ile bilginin paylaşılması ve uzak noktalardan erişimin sağlanması söz konusudur. Bu yüzden bilgi güvenliği sağlık sektörü dahil birçok kurum ve kuruluşta oldukça önemli bir yer kazanmıştır. Ülkemizde sağlık hizmetlerinin sunumunda bilginin elektronik ortama aktarıldığı, kurumlar ve sağlık çalışanları arasında paylaşımının giderek arttığı ve kolaylaştığı bir dönem yaşıyoruz. Hastaneler tıbbi hataları azaltmak, hizmet kalitesini artırmak, maliyet etkinliği sağlamak, zamanında karar verme ve verimliliği artırmak için teknolojiyi kullanıma ihtiyaç duymaktadır. Sağlık sektöründe yapılan dijital dönüşüm ile bakım ve hizmet kalitesi yükselmiş ve maliyetlerin düşmesi sağlanmıştır. Sağlanan bu avantajlar kurumlara ve çalışanlara ciddi kolaylıklar sunmasının yanında bilginin korunmasının da öneminin artması anlamına gelmektedir. Bilgi güvenliliğinin öneminin artması ile de kurumlar güvenlik önemlerini artırmaktadırlar. Kurumlarda bilginin güvenliğinden yöneticiler sorumludur. Yalnız, gelişen teknolojiyle erişilebilirliği kolaylaşan bilginin korunmasında biometrik önlemler ve HBYS kullanıcılarının da rolü büyüktür. Kurumların çok sık kullanıldığı bu bilginin güvenliliğinin öneminin farkındalığının oluşması şarttır. Bilgi güvenliği; bilgileri yetki sahibi olmayan kişilerin görmesinden, kullanmasından, almasından ya da değiştirmesinden korumaktır. Bu bilgilerin yetkisiz ve izinsiz kişilerden gizli tutulması ise mahremiyettir. Bilgi güveliği, gelişen teknolojiyle kurumlarda bilişim sistemini kullanımıyla daha da önemli hale gelmiştir. Bilgi saklama aracı olarak kağıt kullanıldığı dönemlerde bilginin korunabilmesi için daha çok fiziksel önlemler önemini yitirmeye başlamış yerini ise teknolojik şifreleme sistemlerine bırakmıştır. Bu teknolojik ilerleme ile bilginin cd, dvd, usb ya da internet ortamında depolanmasına ve paylaşılmasına kolaylık sağlarken, gerek bilişim sistemlerinin bağlantı ihtiyaçları sebebiyle gerekse bilinçsiz ve eğitimsiz kullanıcı kaynaklı

(?modul=bildirilerilistele)

bilginin güvenliği de daha riskli hale gelmiştir. Bu araştırmanın amacı; bilgi güvenli ve mahremiyetin korunmasına yönelik eğitimin değerlendirilmesidir. Özel bir hastane uygulamasında farklı zamanlarda anket yapılıp eğitimler verilerek, eğitimin bilgi güvenliğine etkisinin değerlendirilmesi ve bilgi güvenliği ve mahremiyet kültürünün oluşturulmasıdır. Bu özel hastane uygulamasının kuruma, bilgi güvenliği ve mahremiyet bağlamında katkılarının olacağı düşünülmektedir.

(?modul=yeni_bildiri_gonder) (?modul=yeni_poster_gonder) (?modul=yeni_sergi_gonder)

The development of information and communication Technologies makes the sharing of information easier and allows accessing from a remote setting. Therefore, information security has gained significant importance in many institutions and organizations including the health sector. In our country, we are in an era where information is transferred to the electronic environment in the delivery of health services so that sharing of information among institutions and health workers is increasing and getting easier. Hospitals need technology to reduce medical errors, improve service quality, ensure cost-effectiveness, timely decision-making and increase efficiency. With the digital transformation made in the health sector, the quality of care and service increased and the costs were reduced. These advantages provide significant benefits to institutions and employees, as well as increasing the importance of information protection. With the increasing importance of information security, institutions increase their security importance. Managers are responsible for the security of information in institutions. Information security means to protect the information from the sight, use, receipt or alteration of unauthorized persons. The confidentiality of this information from unauthorized persons is confidential. Information security has become even more important with the use of information system in corporations with the developing technology. In the periods when the paper was used as an information storage tool, more physical measures started to lose their importance in order to protect the information and left to technological encryption systems. The purpose of this research is to evaluate the education of the security of information and protection of privacy. In a private hospital setting, a questionnaire is conducted at different times and pieces of training are given, evaluating the effect of education on information security and creating a culture of information security and privacy.

Dosya Panel

Dosya ID	Seri	Dosya İsmi	Yükleme Tarihi

Dosya Yükleme

Ek 3: Anket

BİLGİ GÜVENLİLİĞİ VE MAHREMİYETİN KORUNMASINA YÖNELİK EĞİTİMİN ETKİLERİNİN DEĞERLENDİRİLMESİ: BİR ÖZEL HASTANE UYGULAMASI

Hastanemizde **"Bilgi Güvenliği ve Mahremiyetin Korunmasına Yönelik Eğitimin Etkilerinin Değerlendirilmesi: Bir Özel Hastane Uygulaması"** konusu ile ilgili olarak yürüttüğümüz çalışmada size bazı sorular sorulacaktır. Bu anket tamamen bilimsel çalışma amaçlı olup sizin ya da kurumun adı kullanılmayacaktır. Gerekli desteği sağlayabilmeniz hususunu arz ve rica ederiz.

Gökhan ÖZASLAN	**Prof.Dr. Gonca Mumcu**
Yüksek Lisans Programı Öğrencisi Marmara Üniv. Sağlık Bilimleri Enstitüsü	Tez Danışmanı Marmara Üniv. Sağlık Bilimleri Fakültesi

I-Kişisel Bilgiler

1. Çalışma pozisyonunuz aşağıdakilerden hangisidir?

A) ***Tıbbi Birimler*** 1**)**Uzman hekim 2**)**Pratisyen hekim 3**)**Eczacı 4**)**Hemşire 5**)**Ebe 6**)**Acil tıp teknisyeni 7**)**Laboratuvar teknisyeni8)Radyoloji teknisyeni 9**)**Anestezi teknisyeni 10**)**Biyolog 11**)** Fizyoterapist 12)Sağlık memuru 13)Diyetisyen 14)Diğer…….....

B) ***İdari Birimler*** 1)Hasta Hizmetleri 2)Destek Hizmetler 3)Muhasebe/Faturalama 4)Teknik Hizmetler 5)Satın alma 6) İnsan Kaynakları 7)Kalite 8)Pazarlama 9) Biyomedikal 10)Arşiv 11) Hasta ilişkileri 12) Üst Yönetim 13)Diğer…….....

2. En son mezun olduğunuz okul?

3. Yaşınız:

4. Cinsiyetiniz: 1)Erkek 2)Kadın

5. Kurumda çalışma süreniz: ….....yıl ……..... ay

6. Hastane bilgi yönetimi sistemi kullanımı deneyim süreniz: …..... yıl …….....ay

7. Hastane bilgi yönetimi sistemini kullanmak için eğitim aldınız mı? 1)Evet 2)Hayır

8. Hastane bilgi yönetimi sistemini kullanmak için aldığınız eğitim ne kadar sürdü? …….....saat

9. Aldığınız eğitimi nasıl değerlendirirsiniz? 1)Yetersiz 2)Kararsızım 3)Yeterli

10. Genel olarak bilgisayar kullanım becerinizi nasıl değerlendirirsiniz?

(Çok yetersiz) 0 _____ 100 (Çok yeterli)

11. Genel olarak hastane bilgi yönetimi sistemi kullanım becerinizi nasıl değerlendirirsiniz?

(Çok yetersiz)0 _____ 100 (Çok yeterli)

II-Bilgi Güvenliği İle İlgili Genel Sorular

12. 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)SGK bilgileri 9)Diğer…….

13. 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) SGK bilgileri 9)Diğer……..

14. Hastanedeki hangi tür bilgiler koruma altına alınmıştır? (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) SGK bilgileri 9)Diğer……

15. Hastane bilgi yönetimi sistemi üzerinden hasta verilerine erişiminiz kim/kimler tarafından denetlenmektedir?

1) İlgili Olduğum Birim Sorumlusu 2)Bilgi işlem Sorumlusu 3)Hastane Müdürü 4)Başhekim 5)Diğer

16. Bilgi güvenliğinin sağlanması için 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

17. Aşağıdaki şifre yapılarından hangileri kullanılabilir? (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) Hiçbiri

18. Hastaya ait olan bilgilerin paylaşımı için hastalardan onam formu alınması gerekli mi?

1)Evet 2)Hayır

19. 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…….

20. 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……..

21. 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……..

22. Sizce bilgi güvenliği ile ilgili sorunların nedeni nedir?

……
……
……

23. 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…….. (…...)

6) Denetleme (…...)

24. Hastanedeki bilgi güvenliği için kaç puan verirsiniz?

(Çok kötü) 0 _____ 100 (Çok iyi)

	Lütfen aşağıdaki ifadeler için size uygun olan seçenekleri işaretleyiniz.	**KesinlikleKatılıyorum**	**Katılıyorum**	**Kararsızım**	**Katılmıyorum**	**KesinlikleKatılmıyorum**
25.	Hastanede bilgi güvenliğinin sağlanması için görevler ve sorumluluklar net olarak belirlenmiştir (örneğin, yedeklerin alınmasından, kullanıcıların sisteme kaydedilmesinden sorumlu olan çalışanlar bulunmaktadır).					
26.	Hastanede, bilgi güvenliğine ilişkin yazılı politikalar vardır.					
27.	Çalışanlar bilgi güvenliği politikalardan haberdardır.					
28.	Tüm personele yeterli ve uygun bilgi güvenliği eğitimi verilmektedir.					
29.	Çalışanlar bilgi sisteminde izin verilen ve onaylanmayan uygulamalar konusunda yeterince bilgilidir (örneğin; elektronik posta kullanımı ve internete bağlanma).					
30.	Bilgi güvenliğinin sağlanması için çalışanlar gerekli özeni gösterir					

31.	Hastanedeki yöneticiler bilgi güvenliğine gereken özeni gösterir					
32.	Yöneticiler bilgi güvenliliğinin uygulaması konusunda sorumluluk sahibidirler.					
33.	Çalışanlar, güvenlik ihlali olaylarının derhal yönetime bildirilmesi gerektiğinden haberdardır.					
34.	Çalışanlar kendi çalışma alanlarından uzaklaştığında, bilgisayarlarını daima güvenli şekilde bırakmaları konusunda eğitilmiştir (örneğin; bilgisayar başından ayrıldığında bilgisayarların şifrelenmesi ya da oturumun kapatılması).					
35.	Güvenlik politikalarımızı ve süreçlerimizi ihlal eden çalışanlarımıza yönelik disiplin uygulamaları bulunmaktadır					
36.	Bir güvenlik ihlalinin meydana gelmesi durumunda, yapılacaklar ve yardım için kimin aranacağı bilinmektedir.					
37.	Anti-virüs sistemimiz günceldir ve bir virüs saldırısı durumunda, sistemlerimizi mümkün olan en iyi şekilde korumaktadır.					
38.	Kullanıcıların sistemlerimizde oturum açmalarına yetki verecek uygun mekanizmalar bulunmaktadır.					
39.	Çalışanlar, kendi kullanıcı hesaplarıyla yetkilendirilip tanımlamaları yapılmadan, sistemlerimizde oturum açamaz / sistemlerimize erişim sağlayamazlar.					
40.	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).					
41.	Hastanede, kullanıcıların hangi verilere erişebileceğini belirleyen bir yetkilendirme prosedürü vardır.					
42.	Bilgi işlem uygulamaları sadece yetkilendirilmiş iş amaçları doğrultusunda kullanılır.					
43.	Bilgi güvenliği gün içinde yaptığımız işleri düşününce öncelikli bir konu değildir.					

II-BÖLÜM-TEKNİK BİRİM ÇALIŞANLARI

Hastane Bilgi Yönetim Sistemi ve Bilgisayar Teknoloji Alt Yapısı İle İlgili Bilgiler

I-Genel Değerlendirme

44. Hastanenizde kaç adet bilgisayar (pc-ipad-leptop) bulunmaktadır?
…….

45. İnternet aşağıdaki iş amaçlarından hangileri için kullanılır? (Geçerli olan tüm şıkları işaretleyiniz)

1)Hastalar ile ilgili bilgilerin toplanması 2)Diğer hastaneler ile ilgili bilgilerin toplanması

3)Bir hastane varlığının oluşturulması (örneğin web sitesi) 4)Hastalar ile rutin iletişim

5)Tedarikçiler ile rutin iletişim 6)Hastalara hizmet/destek sağlanması
7)Diğer……

46. Hastanede şifre kırılma olayları sıklığı nedir?..... kez/ay ……kez/yıl

47. Şifre kırılma olayları için alınan önlemler nelerdir?

48. Hastalar ile ilgili acil durumlarda çalışanların verilere erişiminde yetkilendirme değiştiriliyor mu? 1)Evet 2)Hayır

49. Yetkilendirme değişimi kimin/kimlerin isteği ile yapılıyor?

50. Bilgi işlem çalışanları üst yönetime danışmadan acil durumlarda yetki değişimi yapabiliyor mu? 1)Evet 2)Hayır

51. Bilgi güvenliği ile ilgili olarak bilgi sistemleri bölümünün günlük olarak yaşadığı sorunlar nelerdir?

52. Kurumunuzdaki bilgi güvenliği için 0 (Çok kötü) -100 (Çok iyi) arasında kaç puan verirsiniz?

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

II-Teknik Açıdan Bilgi Güvenliğini Değerlendirme

	Lütfen aşağıdaki ifadeleri için size uygun olan seçenekleri işaretleyiniz.	**Kesinlikle Katılıyorum**	**Katılıyorum**	**Kararsızım**	**Katılmıyorum**	**Kesinlikle Katılmıyorum**
53.	Kurum dışından bilgi sistemlerimize erişim için bir üst yöneticinin onayı gereklidir.					
54.	Bilginin işlenmesi için kullanılan tüm varlıkları (yazılım, donanım, personel ve hizmetler dahil) tanımlayabilir ve yerlerini belirtebiliriz.					
55.	Bilgi varlıklarımıza yerel ve uzaktan erişim kontrol edilir.					
56.	Hastanede bilgi teknolojileri ile ilgili taşınabilir ve stok malzemeler vardır.					
57.	Hastane bilgi sistemine müdahaleyi önlemek amacıyla fiziksel ve çevresel güvenlik süreçlerine sahibiz.					
58.	Hastaneye ait taşınabilir bilgisayarlarla seyahat eden çalışanlar, hırsızlık ve veri gizliliğin ihlal edildiği durumlarda olası yükümlülüklerden haberdardır.					
59.	Sunucularımız iklimlendirmesi ve güç kaynakları olan, yangına dayanıklı güvenli yerlerde tutulmaktadır.					
60.	Sistemlerimiz, üreticiden alınan kullanıma hazır ürünler şeklinde veya özel sistemler şeklinde satın alınır.					
61.	Sistemlerimiz, sistem kullanımı ve veri girişine ait değişikliklerinin denetlenmesine ihtiyaç duyar.					
62.	Yangın / sel gibi bir felaket durumunda, kimlerin hangi sorumluluğu üstleneceğini ve hastanenin faaliyetini sürdürmesini sağlamak için nelerin yapılması gerektiğini belirten, bir iş devamlılığı planına sahibiz.					
63.	Hastanede iş devamlılığı sürecinin yönetilmesinde sorumlu					

	olarak belirlenmiş bir çalışan vardır.					
64.	Güvenlik önlemlerimiz geçtiğimiz yıl içerisinde gözden geçirilmiştir.					
65.	Uluslararası bilgi güvenliği standartlarının bulunduğundan haberdarız.					
66.	Bilgi güvenliği hastanelerin kaygı duyması gereken önemli bir konudur.					

67. Hastanede son 12 ay içerisinde aşağıdaki hangi güvenlik ihlalleri ile karşılaşıldı? (lütfen geçerli olan tüm şıkları işaretleyiniz.)

1) Bilgi güvenliği ihlali yok
2) Dikkatsizlik sonucu oluşan ihlaller
3) Ekipman arızası
4) Yedekleme yapılmaması
5) Veri hırsızlığı
6) Çevresel faktörler
7) Telif hakkı ihlali
8) Diğer.....

Ek 4: Turnitin Raporu

gökhan özaslan

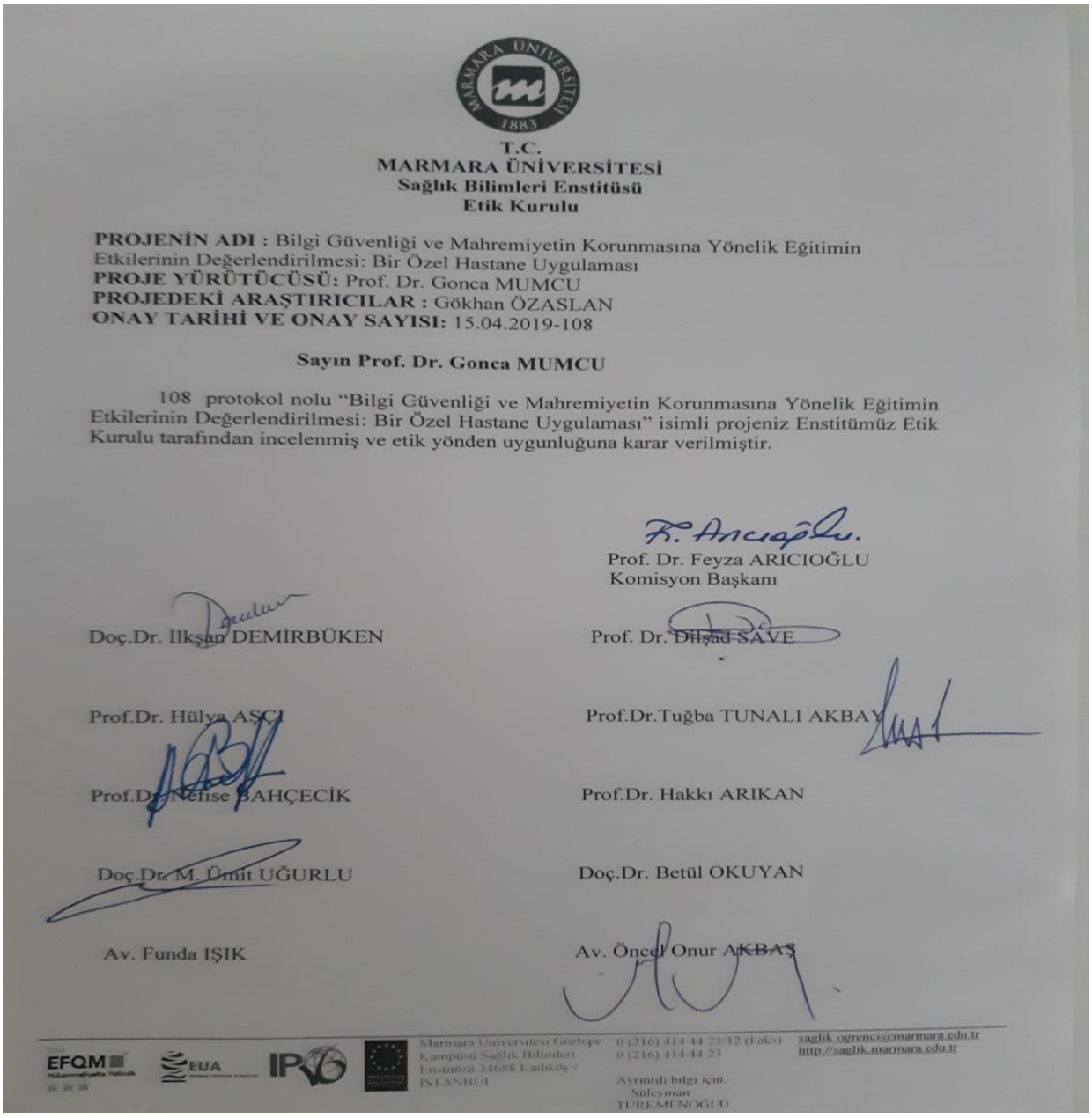
ORIJINALLIK RAPORU

%17	%5	%3	%16
BENZERLIK ENDEKSI	İNTERNET KAYNAKLARI	YAYINLAR	ÖĞRENCI ÖDEVLERI

BIRINCIL KAYNAKLAR

1	Submitted to Bahcesehir University Öğrenci Ödevi	%10
2	eprints.sdu.edu.tr İnternet Kaynağı	%1
3	Submitted to Beykent Universitesi Öğrenci Ödevi	%1
4	Submitted to Suleyman Demirel University Öğrenci Ödevi	%1
5	sbu.saglik.gov.tr İnternet Kaynağı	%1
6	Submitted to Istanbul Aydin University Öğrenci Ödevi	<%1
7	docplayer.biz.tr İnternet Kaynağı	<%1
8	Submitted to Karabük Üniversitesi Öğrenci Ödevi	<%1
9	ARSLAN, Nihan and AKIN, Ahmet. "Çözüm	<%1

Ek 5: Etik Kurul Onayı



T.C.
MARMARA ÜNİVERSİTESİ
Sağlık Bilimleri Enstitüsü
Etik Kurulu

PROJENİN ADI : Bilgi Güvenliği ve Mahremiyetin Korunmasına Yönelik Eğitimin Etkilerinin Değerlendirilmesi: Bir Özel Hastane Uygulaması
PROJE YÜRÜTÜCÜSÜ: Prof. Dr. Gonca MUMCU
PROJEDEKİ ARAŞTIRICILAR : Gökhan ÖZASLAN
ONAY TARİHİ VE ONAY SAYISI: 15.04.2019-108

Sayın Prof. Dr. Gonca MUMCU

108 protokol nolu "Bilgi Güvenliği ve Mahremiyetin Korunmasına Yönelik Eğitimin Etkilerinin Değerlendirilmesi: Bir Özel Hastane Uygulaması" isimli projeniz Enstitümüz Etik Kurulu tarafından incelenmiş ve etik yönden uygunluğuna karar verilmiştir.

Prof. Dr. Feyza ARICIOĞLU
Komisyon Başkanı

Doç.Dr. İlkşan DEMİRBÜKEN

Prof. Dr. Dilşad SAVE

Prof.Dr. Hülya AŞCI

Prof.Dr.Tuğba TUNALI AKBAY

Prof.Dr. Nelise BAHÇECİK

Prof.Dr. Hakkı ARIKAN

Doç.Dr. M. Ümit UĞURLU

Doç.Dr. Betül OKUYAN

Av. Funda IŞIK

Av. Öncel Onur AKBAŞ

EFQM EUA IPv6

Marmara Üniversitesi Göztepe Kampüsü Sağlık Bilimleri Enstitüsü 34688 Kadıköy / İSTANBUL
0 (216) 414 44 23/12 (Faks)
0 (216) 414 44 23
Ayrıntılı bilgi için: Süleyman TÜRKMENOĞLU
saglik.ogrenci@marmara.edu.tr
http://saglik.marmara.edu.tr

10. ÖZGEÇMİŞ

Adı	Gökhan	**Soyadı**	ÖZASLAN
Doğum Yeri	Nizip-Gaziantep	**Doğum Tarihi**	01.02.1990
Uyruğu	T.C.	**Tel**	0541 9505642
E-mail	ozaslangokan@hotmail.com		

Eğitim Düzeyi

	Mezun Olduğu Kurumun Adı	**Mezuniyet Yılı**
Yüksek Lisans	Marmara Üniversitesi Sağlık Bilimleri Enstitüsü	Halen
Lisans	Marmara Üniversitesi Sağlık Bilimleri Fakültesi	2012
Lise	Gaziantep Lisesi Yabancı Dil Ağırlıklı Lisesi	2007

İş Deneyimi

Görevi	**Kurum**	**Süre (Yıl - Yıl)**
Gece Müdürü	İnayet Topçuoğlu Hastanesi	2013-2014
Satın Alma Koordinatorü	NCR International Hospital Grubu	2014-2016
Satın Alma ve İdari İşler Müdürü	Özel Mehmet Toprak Hastanesi	2016-Halen

Yabancı Dilleri	**Okuduğunu Anlama***	**Konuşma***	**Yazma***
İngilizce	İyi	İyi	İyi

Bilgisayar Bilgisi

Program	**Kullanma becerisi**
Office	İyi

***Çok iyi, iyi, orta, zayıf olarak değerlendiriniz.