T.C.
OKAN ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

SAĞLIKTA KALİTE YÖNETİMİ ANABİLİM DALI
YÜKSEK LİSANS TEZİ

KALİTE YÖNETİM DİREKTÖRLERİNİN BİLGİ GÜVENLİĞİ FARKINDALIĞI: İSTANBUL İLİ ÖRNEĞİ

Çiğdem ÇELİK ÇÖP

Tez Danışmanı
Yrd. Doç. Dr. Onur YARAR

İSTANBUL, 2017

T.C.
OKAN ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

SAĞLIKTA KALİTE YÖNETİMİ ANABİLİM DALI
YÜKSEK LİSANS TEZİ

KALİTE YÖNETİM DİREKTÖRLERİNİN BİLGİ GÜVENLİĞİ FARKINDALIĞI: İSTANBUL İLİ ÖRNEĞİ

Çiğdem ÇELİK ÇÖP

Öğrenci Numarası
142021009

Tez Danışmanı
Yrd. Doç. Dr. Onur YARAR

İSTANBUL, 2017

T.C
OKAN ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜ

YÜKSEK LİSANS
TEZONAYI

ÖĞRENCİNİN
Adı ve Soyadı : Çiğdem Çelik Çöp Öğrenci No : 142021009
Anabilim/Bilim Dalı : Sağlıkta Kalite Yönetimi Anabilim Dalı
Tez Savunma Tarihi : 27.11.2017
Danışman : Yrd. Doç. Dr. Onur Yarar Tez Savunma Saati : 10:00

Tez Konusu : *"Kalite Yönetim Direktörlerinin Bilgi Güvenliği Farkındalığı: İstanbul İli Örneği"*

TEZ SAVUNMA SINAVI, Lisansüstü Öğretim Yönetmeliği'nin **28.Maddesi** uyarınca yapılmış, sorulan sorulara alınan cevaplar sonunda adayın tezinin KABULU 'ne OYBİRLİĞİ / ~~OYÇOKLUĞU~~YLA karar verilmiştir.

JÜRİ ÜYESİ	KANAATİ (KABUL / RED / DÜZELTME)	İMZA
Prof. Dr. Haydar Sur	Kabul	
Yrd. Doç. Dr. Onur Yarar	Kabul	
Yrd. Doç. Dr. Yıldırım B. Gülhan	Kabul	

YEDEK JÜRİ ÜYESİ	KANAATİ (KABUL / RED / DÜZELTME)	İMZA

ÖZET

Araştırma kamu hastanelerinde görev yapan kalite yönetim direktörleri ve kalite birim sorumlularının bilgi güvenliği farkındalıklarını belirlemek amacıyla yapılmıştır. Araştırmanın evrenini İstanbul ilinde faaliyet gösteren kamu hastaneler birliğine bağlı 72 hastanenin kalite yönetim direktörleri ve kalite birim sorumluları oluşturmaktadır. Kamu hastaneler birliğine bağlı 6 genel sekreterliğe araştırma izni başvurusu yapılmış ancak 67 hastane için çalışma onayı alınmıştır. Örneklem seçilmemiş, evrende izin verilen hastanelerin tamamına ulaşılmış olup; toplam 87 kişiden veri toplanmıştır.

Araştırma Kasım 2016-Ağustos 2017 tarihleri arasında 10 aylık bir sürede tamamlanması için etik kurul izni alınmış sonrasında Aralık 2016- Nisan 2017 tarihleri arasında 5 aylık bir sürede veri toplama süreci tamamlanmıştır. Katılımcılara yüz yüze ve elektronik anket uygulaması uygulanmıştır.

Araştırmada veriler kalite direktörlerinin tanımlayıcı özelliklerini belirlemeye yönelik form ve "Bilgi Güvenliği Farkındalık Ölçeği" ile toplanmıştır.

Araştırmada elde edilen veriler SPSS (Statistical Package for the Social Sciences) Windows 22.0 programı kullanılarak analiz edilmiştir. Verilerin değerlendirilmesinde tanımlayıcı istatistiksel yöntemleri olarak frekans, yüzde, ortalama, standart sapma, t-testi, anova testi kullanılmıştır.

Araştırma sonucunda kalite yönetim direktörlerin "kişisel verilerin korunması" düzeyinin yüksek; "saldırı ve tehditlere yönelik farkındalık" düzeyinin orta; "bilgi güvenliği farkındalığı genel" düzeyinin orta seviyede olduğu belirlenmiştir. Araştırmada ayrıca bilgi güvenliği farkındalığına yönelik cinsiyet ve meslek grubuna göre farklılıklar bulunduğu sonucuna ulaşılmıştır.

Anahtar Kelimeler: Bilgi Güvenliği, Kalite yönetim direktörleri, Kalite, Hastane.

ABSTRACT

INFORMATION SECURITY AWARENESS OF QUALITY MANAGEMENT DIRECTORS: ISTANBUL PROVINCE EXAMPLE

The research was conducted in order to determine the awareness of quality Management Directors and quality unit principals who serve in public hospitals. The world of 72 is the quality Management Directors and quality unit principals of the hospital, which is connected to the public hospitals union operating in the province of Istanbul. 6 General Secretaries of public hospitals have been applied for research permits, but 67 hospitals have been approved for work. The sample is not selected, all the hospitals allowed in the universe have been reached; data collected from a total of 87 people.

The data collection process has been completed between December 2016-April 2017 in a 5-month period after the research was obtained from November 2016 to August 2017 for completion of a 10-month period. Participants were applied face-to-face and electronic survey application.

The data in the research was collected with the form and "Information security awareness Scale" to determine the descriptive characteristics of the quality directors.

The data obtained in the study was analyzed using the SPSS (Statistical Package for the Social Sciences) Windows 22.0 program. As descriptive statistical methods for evaluating data, frequency, percentage, average, standard deviation, T-Test, ANOVA test were used.

As a result of the research, the level of "protection of personal data" is high the level of "awareness of attacks and threats" is moderate; It has been determined that the level of "information security awareness" is at the middle level. The survey also found that there were differences according to gender and occupation group in terms of information security awareness.

Keywords: İnformation Security, Quality management directors, Quality, Hospital.

ÖNSÖZ

Bu araştırma, yaklaşık bir yıllık yoğun ve titiz bir çalışmanın ürünü olarak ortaya çıkmıştır. Araştırmanın her aşamasında gerçek bilgi ve verilere ulaşmak için uygun bilimsel yöntemler kullanılmış olup, özenle çalışma yürütülmüştür. Araştırma sonucunda elde edilen bulgulardan çıkan sonuçlar bilgi güvenliğine yönelik algı, tutum ve davranışları ortaya koymaktadır. Tespit edilen özellikler ve kullanılan ölçek ışığında, ortaya çıkan verilere bağlı olarak geliştirilen önerilerle bilgi güvenliğine yönelik çıkarımlar sağlanacağı umulmaktadır. Araştırmanın kuramsal çerçeveyi içeren bölümlerinde bilgi güvenliği her yönüyle ve oldukça kapsamlı bir biçimde ele alınmaya çalışılmıştır.

Öncelikle yüksek lisans öğrenim yaşamımda bana her konuda destek olup; bilgi ve tecrübelerini paylaşarak katkıda bulunan değerli hocam Yrd. Doç. Dr.Onur YARAR'a saygılarımı sunarım.

Araştırma kapsamında yer alan verilerin toplanmasında katkı sağlayan katılımcılara samimi ve gerçek bilgi verdikleri için;

Çalışmam boyunca desteğini ve sabrını hiçbir zaman esirgemeyen eşim Ahmet ve kızım Aslı Zeynep'e, çalışmam ile ilgili döküman temininde yardımını esirgemeyen arkadaşım Tevfik KESEMEN'e, çalışmamda yol gösterip, deneyimlerinden faydalandığım arkadaşlarım Ebru TANIŞIK, Hatice YILDIZ'a ve desteğinden dolayı arkadaşım Aysel ARSLAN'a da teşekkür ederim.

BEYAN

Bu çalışmanın, kendi tez çalışmam olduğunu, tezde kullanılan bilgileri etik kurallar içinde elde ettiğimi, daha önce üretilmiş olan ve yararlandığım bütün bilgi, fikir ve yorumları akademik kurallar içinde kullandığım ve kaynak gösterdiğimi beyan ederim.

Çiğdem ÇELİK ÇÖP

İÇİNDEKİLER

SAYFA NO

TEZ ONAYI……i
ÖZET ii
ABSTRACT..... iii
ÖNSÖZ iv
BEYAN v
İÇİNDEKİLER vi
TABLO LİSTESİ..... viii
ŞEKİL LİSTESİ..... iix
KISALTMALAR LİSTESİ..... x
1. GİRİŞ 1
2. GENEL BİLGİLER..... 4
2.1. Bilgi Kavramı 4
2.2. Bilgi Güvenliği Kavramı..... 7
2.3. Tarihsel Süreçte Bilgi Güvenliğinin Gelişimi 8
2.4. Bilgi Güvenliğinin Kapsamı, Unsurları ve Uygulanması 10
2.5. Bilgi Sistemlerindeki Güvenlik Riskleri ve Açıkları..... 15
2.5.1. Personelden Kaynaklı Riskler..... 15
2.5.2. Bilgi Sisteminden Kaynaklı Riskler..... 16
2.5.3. İç Süreçlerdeki Aksaklıklar 16
2.5.4. Destek Süreçlerine İlişkin Riskler 17
2.5.5. Dış Etkenlere İlişkin Riskler 17
2.6. Gruplarına Göre Bilgi Güvenliği..... 18
2.6.1. Kişisel Bilgi Güvenliği..... 18
2.6.2. Kurumsal Bilgi Güvenliği..... 18
2.6.3. Ulusal Bilgi Güvenliği 21
2.7. Sağlıkta Bilgi Güvenliği 22
2.8. Türkiye'de Sağlık Sektöründe Bilgi Güvenliğine Dair Mevzuat..... 31
2.9. Sağlık Bakanlığı Bilgi Güvenliği Uygulamaları 33
2.9.1. Bilgi Güvenliği Politikası..... 34
2.9.2. Bilgi Güvenliği İhlal Yönetimi 36
2.9.3. Bilgi Güvenliği Denetimleri..... 36
2.9.4. Gizlilik Sınıfları ve Gizlilik Anlaşmaları 36
2.9.5. Kurumsal Gizlilik Sözleşmesi 38
2.10. Hastane Bilgi Yönetim Sistemi..... 38
2.11. Hastane Kalite Yönetim Direktörlerinin Rol ve Sorumlulukları 42
2.12. ISO /IEC 27001 Standartı 45
2.13. Bilgi Güvenliği Farkındalık Eğitimleri 46
3. GEREÇ ve YÖNTEM 47
3.1. Araştırmanın Modeli 47
3.2. Evren ve Örneklem 47
3.3. Araştırmanın Süresi ve Uygulama Şekli..... 48
3.4. Araştırmanın Hipotezleri 48
3.5. Veri Toplama Aracı 49
3.6. Verilerin İstatistiksel Analizi 50

3.7. Araştırmanın Sınırlılıkları 50
4. BULGULAR 51
4.1. Tanımlayıcı Özelliklerin Dağılımı 51
4.2. Bilgi Güvenliği Farkındalığına İlişkin Betimleyici Bulgular 52
4.3. Bilgi Güvenliği Farkındalığının Tanımlayıcı Özelliklere Göre Karşılaştırması 61
5. TARTIŞMA 69
6. SONUÇ ve ÖNERİLER 71
KAYNAKÇA 74
EKLER 81
EK-1: Anket Formu 81
EK-2: Etik Kurul Onayı 84
EK-3: İstanbul İli Anadolu Kuzey Kamu Hastaneler Birliği Genel Sekreterliği Araştırma İzni 85
EK-4: İstanbul İli Beyoğlu Kamu Hastaneler Birliği Genel Sekreterliği Araştırma İzni 86
EK-5: İstanbul İli Çekmece Bölgesi Kamu Hastaneler Birliği Genel Sekreterliği Araştırma İzni 87
EK-6: İstanbul İli Fatih Bölgesi Kamu Hastaneler Birliği Genel Sekreterliği Araştırma İzni 88
EK-7: İstanbul İli Anadolu Güney Kamu Hastaneler Birliği Genel Sekreterliği Araştırma İzni 89
EK-8: İstanbul İli Bakırköy Bölgesi Kamu Hastaneler Birliği Genel Sekreterliği Araştırma İzni 90
EK-9: Araştırma İzni Veren Hastaneler 92

TABLO LİSTESİ

SAYFA NO

Tablo 1. Tanımlayıcı Özelliklerin Dağılımı 51
Tablo 2. Direktörlerin Bilgi Güvenliği Farkındalığı İle İlgili İfadelere Verdiği Cevapların Dağılımları 52
Tablo 3. Bilgi Güvenliği Farkındalığı Puan Ortalamaları 60
Tablo 4. Bilgi Güvenliği Farkındalığının Cinsiyete Göre Ortalamaları 61
Tablo 5. Bilgi Güvenliği Farkındalığının Yaşa Göre Ortalamaları 62
Tablo 6. Bilgi Güvenliği Farkındalığının Eğitim Düzeyine Göre Ortalamaları . 62
Tablo 7. Bilgi Güvenliği Farkındalığının Göreve Göre Ortalamaları 63
Tablo 8. Bilgi Güvenliği Farkındalığının Çalışılan Hastane Türüne Göre Ortalamaları 64
Tablo 9. Bilgi Güvenliği Farkındalığının Toplam İş Tecrübesine Göre Ortalamaları 65
Tablo 10. Bilgi Güvenliği Farkındalığının Mevcut İş Yerinde Çalışma Süresine Göre Ortalamaları 65
Tablo 11. Bilgi Güvenliği Farkındalığının Kaç Yıldır Bilgisayar Kullanıldığına Göre Ortalamaları 66
Tablo 12. Bilgi Güvenliği Farkındalığının Kaç Yıldır İnternet Kullanıldığına Göre Ortalamaları 66

ŞEKİL LİSTESİ

SAYFA NO

Şekil 1. Araştırmanın Modeli..... 47

KISALTMALAR LİSTESİ

ABD : Amerika Birleşik Devletleri

AIDS : Acquired Immune Deficiency Syndrome

BGYS : Bilgi Güvenliği Yönetim Sistemi

HIPAA : Health Insurance Portability and Accountability Act

HIV : Human Immunodeficiency Virüs

IEC : The International Electrotechnical Commission

ISO : International Organization for Standardization

ORT : Ortalama

PUKÖ : Planla-Uygula-Kontrol Et- Önlem Al

S.B.Ü : Sağlık Bilimleri Üniversitesi

Ss : Standart Sapma

SPSS : Statistical Package for the Social Sciences

TS : Türk Standartları

TSE : Türk Standartları Enstitüsü

1. GİRİŞ

Bilgi yüzyıllar boyu insanlar açısından son derece kıymetli ve çok önemli bir unsur olmuştur. Bu unsur, insanların hayatta kalmasını sağlamak ve onlara belirli oranda bir güç sağlamak adına belki de kilit bir rol oynamıştır. Bilginin temel olarak sağladığı fayda, insanların ulaşmak istedikleri ufuklara odaklanmaları konusunda onların önünü açması ve onlara yeni bir öngörü kazandırmasıdır. Politika, ekonomi, kültür, bilim, sağlık vb. konuların hemen hepsinde değerini hiçbir zaman kaybetmeden son derece güçlü bir etki bırakan bilgi, bu sayede ona sahip olanların, onu göz ardı edenler karşısında daha avantajlı olmalarını sağlamıştır. Bu nedenle bilginin zaman içerisinde bir çatışma nedeni haline geldiğini görmek de mümkündür.

Bilginin bu denli ciddi ölçekli öneminin bulunması, onun kolay erişilebilir bir olgu olduğu anlamını taşımamaktadır. Aksine bilgi, insanlar açısından son derece gizli kalmasına çalışılan bir unsur olarak ortaya çıkmıştır. Taraflar arasında fark yaratması mümkün gözüken bir bilgi, geçmişte, saklanmayı da hak etmiş, bu vesile ile de kimi kıymetli bilgilerin saklanması adına insanoğlu amansız bir mücadele vermiştir. İnsanlar ve toplumlar arasında bir çatışma nedeni olarak da değerlendirilmesi mümkün olan bilgi, bu şekilde bir güç unsuru olma konusundaki konumunu da güçlendirmektedir. Fakat bilginin giderek daha kıymetli hale gelmesi, insanlığın belki de en gelişmiş çağlarından biri olan dijital çağda söz konusu olmuştur. Çeşitli kapıları açan, yönlendiren ve gizli olan bilgi, dijital ortamda saklanmaya başlandıkça, tıpkı geçmiş yıllarda olduğu gibi üzerindeki tehditler de artmıştır.

İnsanlığın yaşamış olduğu mevcut süreçte dijital yaşam, belki de hayatın devamlılığı adına en önemli unsurlardan biri olarak değerlendirilebilecektir. Gerek insanın sosyal yaşamı gerekse de bürokratik olarak yürüttüğü faaliyetler artık eskisinden daha fazla dijitaldir ve bu nedenle de insanın bireysel ve kurumsal anlamda sahip olduğu bilgiler dijital ortamlarda muhafaza edilmekte, kullanılmakta ve faydalanılmaktadır. Dijital yaşamın bu denli aktif olması ve içerisinde yoğun bir bilgi yükü bulundurması, onu potansiyel bir tehdit haline de getirmektedir. Çeşitli yollar aracılığıyla bu bilgileri elde ederek söz konusu bilgilerden farklı şekillerde fayda elde etmek isteyenler için dijital dünya birçok fırsat sunmaktadır. Bu fırsatların hemen hepsi de bilginin sahibi olan tarafların zararına sonuçlanacak türdendir. Bu nedenle bilgiye sahip olmak tıpkı

geçmişteki gibi hatta geçmiştekinden daha güçlü olmak kaydıyla bireylere ve kurumların çeşitli tehditler ile karşılaşmalarına sebebiyet vermektedir.

Bu sahiplik durumu, beraberinde bilginin korunması açısından gösterilen çabaların güçlendirilmesi gerektiğini de göstermektedir. Buna göre bilgi, artık güvenliği sağlanması gereken, hatta bu konuda, dönemin şartlarına uygun, nitelikli koruma mekanizmalarının gerçekleştirilmesini zorunlu kılan bir unsurdur. Aksi bir tutum, bilginin sahibi olan tarafların mutlak olarak zarara uğramalarına sebebiyet verebilecektir. Bu zarar hem maddi hem de manevi anlamda bireylerin ve kurumların yaşama mücadelelerine zarar verebilecektir.

Kişisel anlamda bilgi güvenliği konusunda verilen çabalar ne denli önemli olsa da aslında bilgiyi güvende tutma adına konu üzerinden en ciddi şekilde odaklanması gereken taraf kurumlar olmaktadır. Onların sahip oldukları bilgilerin hem kendilerine hem de çeşitli kademedeki paydaşlarına ait olması, konu üzerindeki odaklanma zorunluluklarını daha da güçlendirmektedir. Onların konu üzerindeki farkındalıkları kendileri, paydaşları, çalışanları ve müşterileri bazında büyük önem arz etmekle birlikte konunun hukuki boyutunda söz konusu kurumların hesap verme zorunluluklarının bulunması, onlar açısından son derece ciddi ölçekli bir öneme sahiptir. Bu nedenle de kurumlar, gün geçtikçe daha yüksek ölçekli olacak şekilde güvenlik önlemleri almakta, bunların arasında bilgi güvenliği belki de en yüksek ölçekli olandır.

Konu, kurumlar özelinde, temele indirgendiğinde, sağlık kuruluşları bu konuda en fazla önem arz eden bilgi güvenliği konusunda odaklanması gereken kurumlardır. Sağlık kuruluşlarının hastalara dair ellerinde bulundurdukları bilginin önemi ve söz konusu bilginin hastaların mahremiyeti adına taşımış olduğu önem göz önünde bulundurulduğunda sağlık kuruluşları, bilgi güvenliğini geçmiş yıllardakinden daha farklı olmak suretiyle, dijital ortamda barındırmak zorunluluğuna sahiptir. Gelişmiş ve gelişmekte olan ülkelerde sağlık kuruluşları arasında özel ve ulusal anlamda kurulan iletişim yapılarının da varlığı ve giderek artan önemi göz önünde bulundurulduğunda, bilgi güvenliği sağlık kuruluşları açısından son derece kritik bir değere sahiptir.

Sağlık kuruluşları açısından bilgi güvenliği konusunda en kritik unsuru hastaların sağlık bilgileri içermektedir. Söz konusu bilgiler, hastalar ve yakınları açısından bir mahrem durumu ifade etmesi neticesinde, kendilerine dair bilgilerin depolanması,

saklanması ve paylaşımı sürecinde konunun hukuki boyutuna odaklanıldığı gibi aynı zamanda konunun güvenlik boyutuna da kurumsal anlamda gereken yatırımların yapılması gerekmektedir. Bu durum hem hastaların kendi hayatlarına dair, sağlıkla ilintili unsurların gizli kalması hem de sağlık kuruluşlarının itibarları açısından önem arz etmektedir. Bu nedenle sağlık kuruluşları açısından bilgi güvenliği çok boyutlu bir konuyu arz etmektedir.

Bu tez çalışması kalite yönetim direktörleri ve kalite birim sorumlularının bilgi güvenliği farkındalığını belirlemek için yapılmıştır.

2. GENEL BİLGİLER

2.1. Bilgi Kavramı

Kavramsal olarak tarihine bakıldığında bilgi, insanoğlunun uzun yıllar boyunca uğruna mücadele ettiği ve elde ettiği süre zarfında da belirli bir zenginliğe eriştiği bir unsuru tanımlamıştır. Fakat zaman içerisinde bilginin bir bilim nesnesi olduğunun daha geniş çaplı olarak algılanmasıyla birlikte bilgiye dair bakış açısı değişmiş, aynı zamanda bilginin elde edilmesi, kullanılması, geliştirilmesi, depolanması ve paylaşılması geçmişten çok daha önemli bir hale gelmiştir. İnsanlığın modern döneminde yaşananlara bakıldığında bilgi, artık rekabetin ve üstünlüğün bir aracı haline gelmiştir. Temel olarak, bireysel açıdan bakıldığında bilgi, bireyin geçmişten bu yana öğrendikleri ile yaşadığı deneyimlerinin bir toplamı olmaktadır. Zaman içerisinde, insanlar arasında yaşanan iletişim bir akış meydana getirmiş ve bu akışın içerisindeki unsurlar bilgi halini almıştır. Kısacası bilgi deneyim, inanç, değer yargıları ve hissiyattan meydana gelmiştir (1). Kurumsal anlamda bakıldığında ise bilgi, içerisinde müşterileri, ürünleri, hizmetleri, süreçleri, yanlışları, doğruları, başarı ve başarısızlıkları barındıran bir birikimi ifade etmektedir. Söz konusu birikimin bir strateji haline getirilmesi ile birlikte de bilgi bir rekabet aracına dönüştürülmektedir (2).

Yine kurumsal anlamda bakıldığında bilgi şu fonksiyonlarıyla tanımlanmaktadır (2);

- Doğru karar vermek,
- Geleceğe dair öngörüler gerçekleştirmek,
- İletişimi nitelikli ve sağlıklı bir şekilde kurmak,
- Ürün ve hizmetler açısından bir standardizasyon gerçekleştirmek,
- Mevcut problemlerin çözümü, gelecekteki muhtemel problemlerin de ortaya çıkmasından önce bir adım atılmasının sağlamak.

Bu görüntüde bilgi, bir sorun çözücü unsur olarak tanımlanabilecektir. Bilginin sağladığı güç hem bireysel hem de kurumsal anlamda tarafların ne yöne doğru hareket etmeleri gerektiği konusunda bilgilendirilmesini sağlamak, hatta bunu çevre ile paylaşmak ve faaliyetlere nitelik kazandırmaktır. Bilgi, bu şekilde anlaşılabileceği üzere, özelden genele uzanan bir silsile içerisinde iletişimi de barındıracak şekilde rasyonel adımlar atılmasını sağlayacak unsurdur.

Değerli bir kaynak olarak kabul gören bilgi, günümüzde çoğunlukla teknolojinin mümkün kıldığı olanaklar ile üretilmekte, sınıflandırılmakta, işlenebilir ve ulaşılabilir kılınmaktadır. Bilgi; bireysel, toplumsal ve kurumsal stratejilerin belirlenmesi, hedeflerin gerçekleştirilmesi ile sorunların çözülmesi noktasında anlam ve değer kazanmaktadır. Günümüzde bilgi, en değerli kaynak, en etkin güç ve riskleri azaltmak noktasında en önemli unsur olarak görülmekte, sorunların çözülmesinde kullanılabilmektedir (3). Bilginin buradaki temel işlevi ve görevi, bireyler ve kurumlar açısından nitelikli bir yol haritasının nasıl olması gerektiği konusunda sürece ışık tutmaktır.

Bilgi, belirli bir sistem dahilin de elde edilen deneyimlerin, sahip olunan değerler bütününün, belirli bir hedefe yönelik enformasyonun ve sahip olunan uzmanlığa dair fikirlerin bir araya getirilerek değerlendirilmesi adına nitelikli ve bir o kadar da değişime açık bir bileşim olarak tanımlanmaktadır (4). Bir başka deyişle bilgi, farklı unsurları bir araya getiren, onlardan beslenen ve onların ortaya koymuş olduğu unsurlara istinaden de şekillendirilme şansı bulunan; yönetici ve yönlendirici niteliği de bulunan bir kavramdır.

Bir başka tanımlamada bilginin işlenmiş veri ya da verilerin bir toplamı olduğuna kanaat getirilmektedir. Buna göre bilgi, daha önceki süreçte bir kurum ya da bireyin mümkün olduğunca nitelikli bir şekilde, zaman içerisinde elde etmiş olduğu her türlü birikimin, kalıplaşmış bir yaklaşıma dönüştürülmesi sonucunda bireyin ya da kurumun bünyesinde, zihninde, deposunda vb. sakladıklarıdır (5). Bilgi, bu hali ile bir son aşama olarak nitelendirilebilecektir. Birey ya da kurum, zaman içerisinde her ne elde ettiyse bunu bir kenara ayırmakta, zamanı geldiğinde hepsini birleştirmekte ve bunu sahip olduğu, işlevsel ve paylaşılabilir bir bilgi haline getirmektedir.

Öte yandan bilgi tanımlanırken onun bazı özellikleri de ön plana çıkarılmaya çalışılmaktadır. Bunlar (6):

- Bilginin çok farklı kaynaklardan elde edilebileceği,
- Bilginin elde edilme şekline göre son derece zor ya da son derece kolay olarak elde edilebileceği,
- Bilginin toplama, işleme, depolama ve paylaşım faaliyetleri sonucu anlam kazandığı,
- Bilginin çok farklı amaçlar için kullanılabileceği,
- Bilginin herhangi bir şekilde, belirli bir kesim ya da tekil birey için kasıtlı olarak tahrip edilebileceği,
- Bilginin kolayca kaybolma riski taşıdığı,
- Bilginin kinetik bir şekilde, esnek olarak değişkenlik içerisinde olabileceğidir.

Bu hali ile bilgi son derece kıymetli bir unsur olmakla birlikte sürekli olarak değişim ve gelişim yaşaması onun çeşitli tehditler ile karşılaşmasına sebebiyet verdiği sürekli olarak koruma altında tutulması gerektiği konusunda bir fikir de vermektedir. Buna göre bilgi, değişkenliği göz önünde bulundurulduğunda onu elde eden, depolayan, işleyen ve paylaşan taraflar için çeşitli sorumlulukları da beraberinde getiren bir olguyu ifade etmektedir.

Bilgi ile birlikte literatürde sık olarak kullanılan kavramlar ise veri ve enformasyondur. Bu süreçte ilk aşama, çeşitli çevrelerden, farklı unsurları içerisinde barındıracak şekilde toplanan veri; ikinci aşama işlenerek bir anlama dönüşen ve bu sayede de çeşitli amaçlar için kullanılabilen enformasyon; son aşama ise genel geçer bir nitelik kazanan, açık, gizli ve yüksek ölçekli nitelikleri bulunan ve uzun süre belirli faydalar için kullanılabilen bilgidir (7). Buna göre bilgi erişilecek olan son aşamadır ve veri ile enformasyonun işlenerek ortaya çıkardığı faktör kesin olarak bir bilgiyi ortaya koymaktadır ki hem bireysel hem de kurumsal anlamda tüm taraflar, ellerindeki verilerden yola çıkarak net bir bilgiye erişmeye çalışmaktadırlar.

2.2. Bilgi Güvenliği Kavramı

Bilgiye sahip olunması her ne kadar ciddi ölçekli bir gücü temsil etse de ya da bilginin kolay erişilebilir olması insanlar açısından bir avantaj olarak gözükse de bilginin güvenliğinin sağlanması ve mümkün olduğunca da olumlu şekilde kullanılması büyük önem arz etmektedir. Özellikle son yıllarda bilginin internet aracılığıyla kolay erişilebilir bir hal alması her ne kadar bir avantaj olarak gözükse de aslında beraberinde ciddi riskleri de getirmektedir. Bu nedenle söz konusu bilginin kötü amaçlar için kullanımının engellenmesi adına bir güvenlik mekanizmasının varlığı son derece elzemdir.

Bilgi güvenliği, bu vesile ile ortaya çıkmış bir kavram olmakla birlikte bilgiye sahip olan bireysel ya da kurumsal kullanıcıların dışındaki bireyler ya da kurumlar tarafından söz konusu bilginin kullanılmasını, değiştirilmesini, yayılmasını, zarara uğratılmasını, manipüle edilmesini vb. engellemek amacıyla oluşturulan bir sistemi ifade etmektedir (8). Öte yandan bilgi güvenliği, belirli bir kesim ya da birey tarafından ciddi ölçekli bir değer yüklenen, bu vesile ile de kullanımı kısıtlanan bir bilginin ya da bilgi topluluğunun gizli tutulmasına çalışıldığı süre zarfında, söz konusu bilgiye erişim hakkına sahip olmayan bireyler ya da topluluklar tarafından kullanımının engellenmeye çalışılmasıdır (9).

Bu vesile ile bilgi güvenliğinin bir koruma mekanizmasını ifade ettiği görülmektedir. Bireysel ya da kurumsal anlamda taşıdığı öneme bakılmaksızın bilginin korunması, modern iletişim çağında büyük bir öneme sahiptir. Çünkü bilginin sahibi olmayan tarafların onu ne şekilde kullanacaklarının bilinmemesi, elde edilen bilgilerin mümkün olduğunca belirli kesimlerin çıkarlarına odaklı olarak kullanılması ve böylelikle de mutlak olarak bilginin sahibi olan tarafın zarara uğratılması durumunun ortaya çıkması bilginin güvenliğinin sağlanması konusunda tetikleyici ve yönlendirici bir durumun ortaya çıkışını sağlamaktadır.

Başka bir yaklaşımla ele alındığında ise bilgi güvenliği, bir tarafın sahip olduğu bilginin diğer tarafa iletimi süre zarfında, üçüncü kişiler tarafından söz konusu bilginin gayri ahlaki ve hukuk dışı olarak ele geçirilmesini ve yine aynı şekilde kullanılmasını engellemek amacıyla geliştirilen uygulama ya da sistemlerdir (10). Buna paralel olarak bilgi güvenliği, bilginin taraflar arasında geçişi ve iletimi sırasında, taraflar arasında herhangi bir anlaşmazlığa diğer tarafların etkisi ile sebebiyet verilmemesi ve bilginin

sağlayıcıdan alıcıya değişime uğramamış, ilk anki amaca uygun ve bu vesile ile de nitelikli olarak aktarımını sağlamak adına verilen çabayı tanımlamaktadır (11).

Modern iletişim çağının genel şartları dahilinde ele alındığı süreçte ise bilgi güvenliğinin kurumsal bazda daha çok değerlendirmeye tabi tutulduğu görülmektedir. Kurumsal açıdan bakıldığında bilgi güvenliği, bir kurumsal yapı içerisindeki işlere süreklilik getirilmesi, muhtemel iş aksaklıklarının en aza indirgenmesi ve yatırımlardan elde edilebilecek faydanın düzeyinin arttırılması adına bilginin en geniş ölçekli olarak çeşitli ve kuvvetle muhtemel tehditlerden uzak tutulması adına kullanılan sistemi ifade etmektedir (12). Yine kurumsal bazda değerlendirildiği süre zarfında bilgi güvenliği, iş sürekliliği, kaçınılması zor kriz dönemlerinde kayıpların en alt düzeye indirgenmesi, işletmelerin bazıları için temel hammadde olan bilginin ulaşılabilir olduğu kadar gizliliğinin sağlanması adına sahip olunan amaçların bütününe işaret etmektedir (13).

Bu bakımdan bilgi güvenliğinin aslında en fazla önemsendiği alanın iş dünyası olduğu görülmektedir. Bu vesile ile ortaya çıkan tabloda kurumlar açısından bilgi güvenliği, kendilerine bir sermaye teşkil ettiği süre zarfının dışında kalan tüm süreçler için dahi bilginin korunması adına geliştirilen tüm yöntemleri kapsamaktadır. Genellikle işletmeler bu konuda belirli önlemleri almış olsalar da özellikle bilginin temel sermaye unsuru olduğu işletmelerin yönlendirmesi ile ortaya çıkan tabloda güvenlik unsuru en az bilginin kendisi kadar değerli hale gelmiştir.

Genele bakıldığında ise bilgi güvenliği konusunda endişelerin en fazla olduğu, buna istinaden de en fazla önlemin alındığı alanların bankacılık operasyonları, e-ticaret işlemler, eğitim sistemleri ve büyük veri depolama alanları olduğu görülmektedir. Bu tür aktif olarak, insanların gündelik hayatında kullanılan alanların bilgi güvenliğine en çok ihtiyaç duyulan alan olduğunu anlamak mümkündür. Çünkü söz konusu alanlar hem maddi hem de manevi anlamda bireylerin hayatlarını en yakından ilgilendiren işlemlerin gerçekleştirildiği alanlar olmaktadır (14).

2.3. Tarihsel Süreçte Bilgi Güvenliğinin Gelişimi

Bilgi güvenliği, kavramsal olarak yeni bir olguyu ifade ediyor gibi gözükse de aslında daha geniş çaplı değerlendirildiğinde, tarihsel akış içerisinde insanoğlunun bireysel ve toplumsal olarak sürekli göz önünde bulundurduğu bir unsur olduğunu görmek mümkündür. Her ne dönemde olursa olsun bilgi, insanların korumak ve mümkün

olduğunca da geniş kitlelerce kullanımını sağlamak adına üzerine odaklandıkları bir unsur olmuştur. Zaman içerisinde değişen ve gelişen teknoloji ile bu durum çok daha kolay hale gelirken bilginin korunmasına dair ilk adımlar da o dönemde etkili olmuştur.

Bu tarihsel akışında içerisinde belki de ilk ciddi ölçekli bilgi güvenliği örneği, Eski Mısır'da sık kullanılan özel alfabelerdir. Hiyeroglif alfabenin dışında, özel ve gizli yazışmaların kontrol altına alınması ve üçüncü taraflar nezdinde anlaşılmasının engellenmesi adına alınan önlemlerdir. Bu çabanın etkililiği göz önünde bulundurulduğunda ancak 19. yüzyılın başlarında Jean-François Champollion tarafından bu alfabenin çözümünün mümkün hale gelmesi dönemsel olarak bilgi güvenliğine dair ne denli nitelikli olarak hareket edildiğini göstermektedir (15).

Bu sürecin bir başlangıç olduğu düşünüldüğünde, tarih içerisinde birçok farklı devlet ve medeniyet, bilgilerinin ve taşıdıkları mesajların güvenliği açısından bugün için ilkel, ancak geçmiş dönemler için son derece modern sistemler kullanmışlardır. Fakat belki de insanoğlunun bilgi güvenliği konusundaki en ciddi ölçekli adımı, İkinci Dünya Savaşı sırasında hem savaşın taraflarının kendi iç mekanizmaları dahilinde hem de müttefikleri ile olan iletişimlerinde kullanmış oldukları bilginin güvenliğinin sağlanmasına dair çalışmalarla atılmıştır. Aynı dönemde kriptolu mesajların çözümlenmesi ve düşman kuvvetlerinin kendi içlerinde yazışmaların, haberleşmenin ve bilgi akışının çözümlenmek istemesi ile birlikte bilgi güvenliğinin önemi daha iyi bir biçimde anlaşılmıştır (16). İkinci Dünya Savaşı'nın bir milat olduğu düşünülecek olursa, onun ardından gelen dönemler, bilgiye erişimin illegal yollardan sağlanması ve gizli bilgilerin deşifre edilmesine yönelik çalışmaların daha da hız kazandığını görmek mümkündür. Özellikle 1960'lı yıllardan başlamak üzere, 1980'li yılların sonuna dek hızlı bir şekilde ilerleyen bilgi teknolojilerine paralel olarak bilgiye illegal yoldan erişme arzusu, ABD başta olmak üzere birçok ülkede bir hobi, bir meslek haline gelmiş ve zaman içerisinde belirli grupların çıkarları adına da kullanılmaya başlamıştır (17).

1990'lı yıllardan bugüne dek uzanan silsilede ise dikkati çeken en önemli unsur, internetin kullanıma başlanması ve bu kullanımın küresel bir alanda yaygınlaşmasıdır. Bu sayede insanların ve kurumların küresel alanda birbirleri ile iletişim kurmaları daha kolay hale gelirken, aynı zamanda bu durum bir güvenlik tehdidinin de ortaya çıkmasına sebebiyet vermiştir. Bilginin kullanılabilirliğinin yanı sıra güvenliğinin de sağlanması

ulusal ve uluslararası anlamda bir zorunluluk haline gelmiş ve konu teknik olarak hukuki boyutu ile de ele alınmıştır (15).

Özellikle internetin kişisel bilgisayar kullanımının yaygınlaşmasına sağlamış olduğu katkı neticesinde kurumsal olduğu kadar bireysel anlamda da bilginin illegal yolla elde edilmesine çalışan çok sayıda bireyin ve topluluğun olduğu gözlemlenmiştir. Tüm bu taraflar, çeşitli yazılımlar aracılığıyla, bireylerin ve kurumların hem kendi bünyelerinde barındırdıkları hem de transfer ettikleri bilginin ele geçirilmesi adına birbirinden farklı yollar izlemişlerdir. Özellikle 2005 yılı itibari ile ivme kazanan ve bilgisayar üzerinden gerçekleşen siber saldırıların hemen hepsinin temelinde, bireysel ve kurumsal bilginin illegal olarak elde edilmesine dair gösterilen çaba söz konusudur (11).

Gelişim süreci açısından bakıldığında bilgi güvenliğinin acil anlamda önem arz etmeye başladığı dönem, internet kullanımının yaygınlaşması ve buna paralel olarak da bilgisayar kullanımının giderek kişiselleşmesidir. Bu sayede bilginin daha fazla kişi tarafından kullanılması, aynı zamanda onu kendi çıkarları için kullanmak isteyen taraflar için ciddi ölçekli bir hedef haline gelmiş ve bu vesile ile sadece kurumların bilgi depoladıkları ya da bilgi aktardıkları noktalara değil, bireylerin de sahip oldukları en alt düzeydeki bilgi ya da bilgi topluluğuna da erişebilmek adına illegal çabalar söz konusu olmuştur. Bilgi güvenliği, bu noktada tüm bireyler ve kurumlar adına ortak bir amaç ve hedefi ifade etmektedir.

2.4. Bilgi Güvenliğinin Kapsamı, Unsurları ve Uygulanması

Bilgi güvenliği, içerik olarak bireyselden uluslararası platforma kadar uzanan, geniş bir silsilede birçok farklı faktörü barındırmaktadır. Özellikle de bilgi güvenliğine yönelik saldırıların bireysel kullanıcılar açısından çok daha fazla bir şekilde ortaya konması, konuya dair güvenlik önlemleri alınırken çok sayıda aktörün göz önünde bulundurulması zorunlu hale getirmektedir. Aynı zamanda bilgi güvenliği sürecinde, söz konusu güvenliği tehdit eden teknolojik unsurların sayısının artmasıyla birlikte, artık bireysel ve kurumsal bazda, konuya dair üzerine odaklanılması gereken unsur sayısında da gözle görülür bir artış yaşanmıştır. Bu nedenle de bilgi güvenliği konusu ele alınırken bireysel, kurumsal ve ulusal aktörler, çevrelerindeki tüm faktörleri dikkatle incelemek durumundadırlar.

Bilgi güvenliğinin kapsamı, temel olarak uygulama bazında ele alınabilecektir. Bilişim faaliyetlerinin sorgulanması, erişimlerin ve erişim izinlerinin kontrolü, süreç içerisindeki değişikliklerin kayıt altına alınarak bu kayıtlardaki farklılıkların incelenmesi, veriye erişme ile birlikte onu değiştirme ve silme işlemlerine belirli sınırlamalar getirilmesi vb. faaliyetler, bilgi güvenliği kapsamında ele alınması gereken hususları teşkil etmektedir. Bir güvenlik mühendisliği olarak görülebilecek olan bu süreçte bireyler, kurumlar ve hükümetler, bilginin mümkün olduğunca uzun süre boyunca güvenli, erişimi, düzenlenmesi, silinmesi ve değiştirilmesi zor hale gelmesi adına çabalamak durumunda olmalıdırlar. Sürecin içerisine bu görev kapsamı dahil olmakta ve yukarıda sıralanan tüm aktörleri ilgilendirmektedir (18).

Bunların dışında bilgi güvenliğinin kapsamı içerisine dâhil olan unsurları aşağıdaki gibi sıralamak mümkündür (17):

- Fiziksel ve Çevresel Güvenlik: Bilginin depolandığı alanlara giriş konusunda, kimlik kontrolü alınmalı farklı uygulamaların söz konusu olması sonucunda bireyler ve kurumlar, mümkün olduğunca fiziksel ve çevresel bir güvenlik ortamı yaratmaya çalışmalıdırlar. Bu tür önlemlerin temelinde, fiziksel anlamda bilgiye erişilecek alanın korunmasının da büyük bir önemi bulunmaktadır.

- İletişim Güvenliği: Bireyler ya da kurumlar arasında cereyan edilmesine bakılmaksızın iletişim, güvenli bir şekilde gerçekleşmesine imkan verilmediği zaman, gizliliğin bulunduğu unsurlar dahil çeşitli güvenlik ihlalleri, bilginin bir taraftan diğerine erişimi sürecinde ortaya çıkması söz konusudur. Özellikle sesli haberleşme konusunda, kurumsal bazda alınan önlemler iletişimin kalitesi kadar güvenliği konusunda da önem vermeleri gerekmektedir.

- Bilgisayar Güvenliği: Modern iletişim çağında bilginin sıklıkla depolandığı alanların başında gelen bilgisayarların güvenlikli bir şekilde kullanılması, bilginin depolanması, değiştirilmesi ve aktarılması konusunda daha rahat hareket edilmesine imkan sağlamaktadır. Özellikle çeşitli kurumlarda sürekli ve aktif olarak kullanılan bilgisayarların içerisinde bulunan kişisel ve

kurumsal, kıymetli bilgilerin korunması çok daha fazla önlem alınmasını zorunlu hale getirmektedir.

- Ağ Güvenliği: Özellikle kurumsal bazda daha yoğun olarak kullanılan ağ odaklı uygulamalar, bilginin transferi konusunda çeşitli riskleri de beraberinde taşımaktadır ve bu vesile ile de ağ üzerinden iletişim gerçekleştiren tarafların, mutlak olarak bilgiden ziyade ağ sistemlerine güvenlik getirmeleri gerekmektedir. Gerek kamusal alanda gerekse de özel sektörde bilginin aktarımı açısından kullanılan ağların temel olarak güvenlik odaklı, güvenlik duvarına sahip ve sürekli olarak kontrol altında tutulduğu bir yapının bulunması gerekmektedir.

Aşamalar halinde gerçekleşen bu güvenlik şeklinde, bireysel ve kurumsal anlamda sahip olunan bilginin, mümkün olduğunca çeşitli elemelerden geçerek erişiminin sağlanması amaçlanmaktadır. Kurumsal anlamda daha çok önemsenen bu silsile, son yıllarda giderek daha fazla bireyin de kendi önemli bilgilerini korumak adına önemsedikleri bir hal almıştır. Buna göre bireysel kullanıcılar, mümkün olduğunca geniş ve kademeli güvenlik önlemleri ile kimi zaman kendileri için bile zorlu olan bir sistem oluşturmaya çalışmaktadırlar.

Bu kapsam dahilin de, bilgi güvenliğine dair temel olarak karşılaşılabilecek sorunları ise aşağıdaki unsurlar ile sıralamak mümkündür (19):

- Düzen bozma: Dışarıdan sisteme yapılan müdahaleler ile sistemin içerisinde yer alan bilginin alışılan düzen dahilin de elde edilmesi, depolanması ve düzenlenmesi zorlaşmakta ve bu şekilde de gerekli veri işlemleri gerçekleştirilememektedir.

- Durdurma: Bilgilere erişmesine izin verilmeyen tarafların söz konusu bilgilere erişebilmesi ve onları istedikleri gibi yönlendirmesi anlamına gelen durdurma, özellikle ağ üzerindeki bilgilere ulaşılarak söz konusu bilgilerin zarara uğratılması ya da çalınmasını ifade etmektedir.

- Değiştirme: Çoğunlukla bilgiye zarar verme amaçlı kullanılan bu yöntemde sistemin içerisinden ya da dışarısından yapılan müdahaleler ile normal

zamanda, sıklıkla kullanılan ve belirli bir formu bulunan bilginin, sisteme ve tüm kullanıcılarına zarar vermek amaçlı değiştirildiği gözlemlenmektedir.

- Fabrikasyon: Çeşitli kanun dışı yollarla bilginin kopyalanarak bir benzerinin yapılması anlamını taşıyan fabrikasyon yoluyla kötü niyetli kullanıcılar, bilginin bir benzerini üreterek onun üzerinden çeşitli getiriler sağlamayı amaçlamaktadırlar.

Bu zarar verme yöntemlerinin neredeyse hepsi gerek bilgiyi zarara uğratma gerekse de bilgi üzerinden herhangi bir getiri elde etme amacıyla uygulanmaktadır. Sistemin kontrol mekanizmasında bulunan ya da sisteme dışarıdan müdahale etmeye çalışan tarafların hemen hepsi, bilginin sahip olduğu değere ve taraflara sağlayacağı fayda ya da getireceği zarara göre bir yöntem belirlemekte ve buna göre bilgi üzerinde çeşitli oynamalar ve müdahaleler gerçekleştirmektedir.

Bilgi güvenliğinin sahip olduğu ve onu oluşturan unsurları ise aşağıdaki şekilde açıklamak mümkündür (18):

- Gizlilik: Bilginin güvenliğinin sağlanması hususunda ön plana çıkan unsur olarak gizlilik, gerek kişisel gerekse de kurumsal anlamda korunması ve gizli bir şekilde varlığını sürdürmesi gerekmektedir.

- Bütünlük: Bilgi, verilerden başlayarak enformasyona, en sonunda da bilgi haline geldiğinde, kendisini besleyen ve yaratan unsurlar ile bir bütünlük arz ederek varlığını ve geçerliliğini koruyabilmektedir.

- Kullanılabilirlik: Bilgi ne kadar kusursuz işlenmiş olursa olsun, mutlak olarak kullanılabilir hale getirilmiş ve bu vesile ile de ondan faydalanmak isteyen taraflar için her an ondan faydalanmaya hazır konumda olmalıdır.

- Kimlik ispatı: Bilgiye sahip olan taraf, onun kendisine has olması vesilesi ile onu diğer taraflara sunduğunda sadece bilgi paylaşımı gerçekleştirmemekte, aynı zamanda bilgiye sahip olan tarafın kimliğini de ispat etmektedir.

- İnkâr edilemezlik: Bir bakıma teyit görevi de gören inkâr edilemezlik, bilgiye sahip olan ve paylaşan taraf ile bilgiyi edinen tarafın herhangi birinin bunu inkâr edememesi, artık o bilgi ile yaşaması anlamını taşımaktadır.

Bu unsurların geneline bakıldığında, bilgiyi var ve canlı tutabilmek adına bilginin bu unsurlara sahip olmasının beklendiği anlaşılmaktadır. Gizlilik ile başlayan ve bireye ya da kuruma mal olan bilginin zamanla dışa çıkması sonucunda ortaya çıkan tabloda, bilginin varlığını kabullenme ve onun işlevsel olmasına verilen önem de göze çarpmaktadır. Bu şekilde bilginin unsurları onu var etme, kullanma, gerektiğinde gizleme ve yine gerektiğinde paylaşılmasıyla oluşmakta, buna istinaden de bilgi kabullenilen ve üzerinde odaklı olarak hareket edilen bir olgu olmakta ve güvenliğinin de bu süreçte öneminin, bilgi her ne kadar paylaşılsa da ön planda olduğunu göstermektedir.

Uygulama açısından bakıldığında ise bilgi güvenliği, üç farklı aşamada ortaya çıkmakta ve gerçek anlamda bir güvenlik mekanizması oluşturulmasına çalışılmaktadır (20):

- Sorumlu ekip oluşturulması: Sürece dair yetkinliği bulunan bireylerin varlığı ve bu bireylerin kullanıma başlamasıyla birlikte bilgi güvenliği sistemleri beklenen etkililiği sağlayabilecek, bununla birlikte de gereken güvenlik önlemleri, yine konuya dair yeterli düzeyde bilgisi bulunan kişiler tarafından alınabilecektir.

- Strateji adaptasyonu: Bilgi güvenliği açısından uygulanan ve daha önceki süreçte başarı elde etmiş olan stratejilerin uygulanması, bilgi güvenliği konusunda atılacak adımların ve takip edilecek yolun kısaltılması anlamını taşımaktadır. Bu nedenle benzer alanlarda, daha önce başarılı olmuş örneklerin adaptasyonu, güvenlik başarısının artmasına yardımcı olacaktır.

- Bilgi-güvenlik düzeyi karşılaştırması: Başarılı bir bilgi güvenliği mekanizmasının kurulabilmesi açısından öncelikli olarak ön plana çıkarılan konu elde var olan bilginin düzeyi ile onun ihtiyaç duymuş olduğu güvenliğin düzeyidir. Bu şekilde, taraflar arasında bir uyum sağlanabildiği süre zarfında nitelikli ve bilginin kapasitesi ile uyumlu, bir o kadar da aşılması zor bir güvenlik mekanizması oluşturulabilecektir.

Bu şekilde bilgi güvenliği, herhangi bir yol haritası ya da strateji olmadan uygulanamayacak bir sistemi ifade etmektedir. Özellikle de kurumsal bazda bakıldığında, bir kurumun dışında, başarılı olarak daha önceki süreçte uygulanmış sistemlerin kullanımı, bilgi güvenliğinin mümkün kılınması açısından ciddi ölçekli bir

destek ve kolaylık sağlayacaktır. Bu nedenle de gerek bireysel gerekse de kurumsal düzeyde olsun, önemli olan noktaların başında, en iyi ve en güvenli sistemin hangisinin olduğunun keşfi gelmektedir ki bu keşif sürecin başarıyla sonuçlanmasına giden kısa yolu ifade etmektedir.

2.5. Bilgi Sistemlerindeki Güvenlik Riskleri ve Açıkları

Bilgiyi koruma adına ileri teknoloji yöntemleri kullanılsa da bilgi sistemlerindeki risk ve güvenlik açıklarının önüne geçilememektedir. Kurumların bu risklerden haberdar olması bilgi güvenliği açısından önem arz etmektedir.

2.5.1. Personelden Kaynaklı Riskler

Bilgi yönetim sistemlerinin başında bulunan sorumlular ya da bilgiyi sürekli olarak kullanan çalışanlar açısından değerlendirildiğinde, bu bireylerin hemen hepsinin en düşükten en yükseğe kadar hata yapma imkânları bulunmaktadır. Buna göre söz konusu bireyler gerek dikkat eksikliği gerekse de bilerek ve isteyerek bilgi güvenliğinin ihlal edilmesine sebebiyet verebilmektedirler. Bilmeden, istem dışı hatalar, yanlış uygulamalar, iletişim kopuklukları vb. sorunlar bilgi yönetimine kontrol dışında bir risk teşkil edebilecekken, sabotaj, bilginin para karşılığında üçüncü kişilere satışı, bilginin tahrip edilmesi vb. uygulamalar görevlilerin bilerek ve isteyerek gerçekleştirdikleri eylemleri ifade etmektedir. Bunun yanı sıra bilginin zarar görmesi konusunda farkındalığı bulunan, ancak duruma bilerek müdahale etmeyen bireyler de bilgi güvenliğine karşı risk teşkil etmektedirler (15).

Süreç genel olarak ele alındığında, kurumlarda görev alan personelin bilgi güvenliğine dair farkındalığının yerleşik olması, farklı açılardan önem arz etmektedir. Buna göre söz konusu personelin, bilginin ne denli önemli olduğu konusunda fikrinin olması, buna göre hareket etmesi ve konunun güvenlik boyutuna odaklanması, sürecin daha güvenli olarak işlemesi adına bir dayanak teşkil etmektedir (21). Bir çalışma ortamında, sürekli olarak bilgi ile iletişim içerisinde olan tarafın görevli personel olduğu düşünüldüğü süre zarfında bu personel grubu, sadece belirli görevlerin yerine getirilmesi açısından değil, aynı zamanda kurumun elinde tuttuğu bilginin de nitelikli hale getirilmesi adına yardımcı olmaktadır.

Personel dışında, bireysel olarak insanın teknolojik ürünleri kullanıyor olması, güvenlik açıklarının daha kolay bir şekilde ortaya çıkmasına sebebiyet vermektedir. Bu vesile ile de bireyler, her ne kadar son teknoloji ürünler ve yüksek güvenlik sağlayan destekler alsalar da sistemin kullanıcısının yine insan olması, beraberinde ciddi ölçekli güvenlik zafiyetlerini de getirmekte ve bireyler ile kurumların bilgilerinin çalınmasını kolaylaştırmaktadır (22). Bu nedenle de sistemsel anlamda güvenlik düzeyi arttırılmakla birlikte bireylerin konuya dair farkındalıklarının, özellikle de kurumlar nezdinde, çalışan personel açısından arttırılması gerekmektedir.

2.5.2. Bilgi Sisteminden Kaynaklı Riskler

Bilginin depolandığı sistemler, tıpkı onun başında bulunan ve onu kontrol eden bireyler gibi çeşitli hatalara sebebiyet verme konusunda riskler taşımaktadırlar. Buna göre bilgi sisteminin depolanması, tasnifi ve transferi gibi konularda yardımcı olan yazılım, donanım ve genel sistemin kendi içerisinde taşıdığı riskler, zaman içerisinde bilginin kullanımı ve güvenliği konusunda çeşitli riskler doğurabilecektir. Özellikle yazılımsal olarak söz konusu olan hataların ya da eksikliklerin yaratmış olduğu riskler, bilginin güvenli bir şekilde saklanmasını ve iletimini zorlaştırmaktadır. Aynı zamanda sistemden sorumlu bireylerin sistemi öğrenme ve kullanma konusunda yaşadıkları ya da yaşayabilecekleri sorunların sebebi ile bilginin güvenliği açık bir tehdit oluşturabilecektir (15). Bu nedenle de bilgiyi çoklu olarak ve işine uzun vadeli olarak yarayacak şekilde depolayan tarafların, mutlak olarak bilgiyi güçlü bir şekilde ellerinde bulundurmalarına yarayacak bir yöntem benimseyerek söz konusu yöntemi kullanmayı bir zorunluluk olarak görmek durumundadırlar.

2.5.3. İç Süreçlerdeki Aksaklıklar

Bilginin kullanımı konusunda sistematik anlamda bir yapı oluşturulsa da bu yapının içerisinde görev olacak olan bireylerin yeterliliği çok daha büyük bir önem taşımaktadır. Görevlilerin kontrol hâkimiyeti ve neyin güvenlik riski taşıyıp neyin güvenlik riski teşkil etmediğini bilmeleri, sistematik olarak sürecin işleyişine dair fikir vermektedir. Öte yandan güvenliğin ne şekilde işlediğinin ve işleyeceğinin kararlaştırılması konusunda iç yapıdaki iletişim süreçleri, tarafların birbirlerini tam olarak anlayıp anlamamalarına bağlı olarak bilgi güvenliğinin varlığına ya da karşılaşması muhtemel risklere zemin oluşturabilecektir (15). Bu nedenle de özellikle kurumsal yapılar içerisinde bilginin edinilmesi, kullanılması, depolanması ve

değiştirilmesi adına sorumluluğu bulunan tarafların arasında güçlü ve konuya dair yetkinliklerinin bulunduğunu ispat eden bir iletişim sürecinin yaratılması gerekmektedir.

2.5.4. Destek Süreçlerine İlişkin Riskler

Bilginin sahibi olan taraflar için onun güvenliğini sağlamak, her zaman kendileri tarafından söz konusu olmamakta, bu noktada dışarıdan bir destek alınması zorunlu hale gelmektedir. Buna istinaden de bireysel ya da kurumsal bilgi depolayan taraflar, konuya dair güvenlik desteği almaya çabalamaktadırlar, ancak bu durum, desteği sağlayacak tarafın niteliğine bağlı olarak bilginin sahibi tarafları yönlendirmektedir. Buna göre bilgi güvenliği konusunda destek verecek tarafların konuya dair yetkinlik düzeyi bilginin ne denli güvenli bir şekilde saklanabileceği konusunda fikir vermektedir (15). Eğer ki bir bilgi güvenliği destekçisi yardımcı olduğu tarafında ne şekilde bilgi depoladığını ve transfer ettiğini bilmez ve sürece dair yeni gelişmeleri takip etmezse, mutlak olarak sistemde yaşanan açıkları fark edemeyecek ya da kendisi yeni güvenlik açıkları yaratarak bireyin ya da kurumun sahip olduğu bilgiye zarar verecektir.

2.5.5. Dış Etkenlere İlişkin Riskler

Bilginin sahip olunması konusunda güvenlik unsuruna bireyler ve kurumlar en üst düzeyde önem veriyor olsalar da herhangi bir iç ya da dış tehdit söz konusu olmadan yaşanan çeşitli sorunlar bilgi güvenliğini riske atabilmektedirler. Yaşanan afetler, hukuki anlamda ortaya çıkan sorunlar sonucunda bilgi paylaşım zorunluluğu, iş dünyasında, finansal anlamda ortaya çıkan sorunlar vb. olaylar dış etkenler ile ilgili risklerin bir kısmını oluşturmaktadırlar (15). Bu sorunların hemen hepsi, özellikle kurumsal anlamda bilgi güvenliği konusunda alınan tedbirlerin ortadan zorunlu olarak kaldırılmasına, buna istinaden de bilginin kolay bir şekilde dışarıya sunulmasının zorunluluğuna sebebiyet vermektedir. Bu durumların hiçbiri önceden kolaylıkla tahmin edilememekte ve karşılık verilememektedir.

2.6. Gruplarına Göre Bilgi Güvenliği

Bilgi güvenliği bireysel olduğu kadar kurumsal ve ulusal anlamda da büyük bir öneme sahiptir.

2.6.1. Kişisel Bilgi Güvenliği

Bireyler gerek birer insan olmaları gerekse de birer tüketici olmaları vesilesi ile artık çok daha fazla bilgiyi ellerinde bulundurmakta ve bu bilgilerin bir kısmı onların kimliği ile ilintili olurken bir kısmı ise onların kişisel olarak sakladıkları ve mahremiyetleri ile ilintili olmaktadır. Fakat her iki şekilde de kişisel anlamda sahip olunan bilgiler, bireylerin koruma altına alınmasının zorunluluğunu ortaya koymaktadır. Bu noktada bireyler kendi başlarına bir bilgi güvenliği mekanizması gerçekleştirebilecekleri gibi resmi kurumlar açısından da böyle bir sorumluluk söz konusudur. Kurumlar sahip oldukları bilgiyi korumak ve kollamak açısından çok farklı yöntemler geliştirebiliyor olsalar da bireysel anlamda, kişisel verilerin korunması çok daha fazla büyük önem arz etmekte ve bu vesile ile de konuya dair bir farkındalık oluşturulmaya çalışılmaktadır (23).

Her ne kadar kişisel verilerin güvenliği açısından bireylerin kendilerini koruma altına alma çabası bulunsa da bu noktada en önemli otorite devlet yönetimlerine ait olmakta ve onların hukuki bazda geliştirecekleri uygulamalar sayesinde bireylerin kişisel bilgilerinin koruma altına alınması daha güçlü ve etkin bir şekilde sağlanmaktadır (24). Bireysel anlamda bilgi güvenliğinin sağlanması adına alınan önlemler gün geçtikçe çeşitlenirken, öte yandan bilgi güvenliğinin hukuki bazda sağlamlaştırılması, bireylerin güçlerinin yetmediği noktalarda, sahip oldukları ya da transfer ettikleri bilginin güçlü bir şekilde korunması adına nitelikli bir destek sağlamaktadır.

2.6.2. Kurumsal Bilgi Güvenliği

Bireysel bilgi güvenliği son derece kritik bir önem taşımakla birlikte kurumsal anlamda söz konusu olan bilgi güvenliği ulusal ve uluslararası bazda çok daha büyük bir önem taşımaktadır. Buna göre kurumlar hem kendi çıkarlarını düşünmek hem de kendileri ile ortak olarak çalışan diğer kurumların ve müşterilerinin bilgiye dair güvenliklerini düşünmek durumundadırlar. Bilgi güvenliğinin kurumsal anlamda bu denli geniş çevreyi etkileyen bir yapısının bulunması beraberinde birçok riski de getirmektedir. Bu risk, kurumların bünyesinde barındırdığı ve transfer ettiği bilginin maddi ve manevi anlamda kurumun niteliklerine zarar verme riskinin bulunmasıdır ki kurumlar bilgi güvenliğini finansal kayıplar yaşamamak kadar prestij kayıpları yaşamamak adına da önemsemektedirler (12).

Kurumsal bilgi güvenliği konusunda en fazla ihtiyaç duyulan noktaların başında, kurumsal anlamda konunun önemsenmesi ve buna uygun olarak çeşitli şekillerde hareket edilmesi gelmektedir. Her ne kadar kurumların bu konuda bazı uygulamaları olsa da bunların sürekli olarak değişim yaşamasının gerekliliği teknolojinin gelişimine paralel olarak birer zorunluluktur. Aynı zamanda kurumsal yönetim anlayışının da bu sürece uyumluluğunun bir zorunluluğu bulunmaktadır ve kurum yönetimleri, kurumsal bilgi güvenliği konusunda gereken, yeterli önlemleri almak durumundadırlar (25).

Kurumların neredeyse tamamı, bilgi güvenliği konusunda teknik departmanlarına bağlı olarak hareket etmekte ve bu durum, söz konusu departmanın çalışanlarının mutlak olarak bu konuda yetkin olması zorunluluğunu beraberinde getirmektedir. Bununla birlikte teknik departmanların yetkinliği ve tecrübesi, bilgi güvenliğinin kurumsal bazda sağlanması adına kritik bir konuyu işaret etmektedir (26). Teknik departmanların asıl sorumluluk üstlenmesini gerektiren durum, kurumsal iletişim ve ortaklıkların çerçevesi genişledikçe, bilgi paylaşım düzeyinin artması ve genişleyen iş çevresi ile birlikte bilgi hırsızlığına dair tehditlerin de aynı düzeyde artış göstermesidir. Bu nedenle kurumsal anlamda, özel bir bilgi güvenliği sisteminin kurulması ya da nitelikli bir sistemin dışarıdan temin edilmesi gerekmektedir (27). Bu açıdan teknik departmanlar, kurumsal anlamda bilgi güvenliğinin sağlanması konusunda önemli bir role sahip olmaktadırlar. Kurumsal yönetimlerin fark edemedikleri ya da geri planda bırakmış oldukları bir konu olarak görülebilecek olan bilgi güvenliği, teknik departmanlar tarafından göz önünde bulundurularak gereken önlemlerin alınması mümkün kılınabilecektir.

Kurumsal anlamda bilgi güvenliğinin ortaya çıkışında etkili olan unsurları aşağıdaki gibi sıralamak mümkündür (28):

- Bilgi güvenliği risklerinin kurumsal açıdan bir itibar sorununa sebebiyet verme durumunun olması,
- Bilgi güvenliği konusunun kurumsal anlamda bir sürekliliğe ihtiyaç duyması,
- Bilginin, kurumsal bazda sürekli bir denetime ihtiyaç duyan bir unsur haline gelmesi,
- Bilgi yönetimi ve güvenliği konusunda sadece kurum yönetiminin değil, kurumun tüm paydaşlarının katılımının zorunluluğu,

- Bilginin depolanması ve kullanımı konusunda bir kurumsal bütünlüğe ihtiyaç duyulması,

- Kurumsal bilginin, mutlak olarak kötüye kullanılma ihtimaline karşı her an hazırlıklı olunmasının bir zorunluluk haline gelmesi,

- Kurum dışında bilginin sunulacağı taraflara sağlanacak destekte kurumun güvenliğe dair sorumluluğunun bitmeyecek olması,

- Kişisel hatalardan dolayı ortaya çıkabilecek sorunların her ana yaşanabilme ihtimalinin varlığı.

Kurumsal anlamda bilgi güvenliğinin mümkün kılınabilmesi adına önemli olan konuların başında, kurumun bir güvenlik politikasının bulunmasının gerekliliği anlaşılmaktadır. Buna göre kurumlar, ellerinde yeterli derecede etkili bir teknik departman söz konusu olsa bile bu departmanın çalışma sistemini bir düzene oturtmak durumundadır. Bu güvenlik politikalarının nitelikli olması adına sahip olması gereken içeriğe dair noktaları da aşağıdaki gibi sıralamak mümkündür (29):

- Güvenlik politikalar açık ve ilintili olduğu kesimlerin kolayca anlayabileceği türden olmak durumundadır.

- Teknik kavramların sadece konuya hakim taraflar için kullanılmasına; geri kalan kesimlerin ise gündelik kullanımlarında neler yapmaları gerektiğini anlayabilecekleri türden bir politika benimsenmelidir.

- Güvenlik politikalarının içeriği ile güvenlik prosedürünün içeriği birbirinden ayrılmalıdır.

- Güvenlik politikalarıyla birlikte güvenlik sistemi, sistemin kullanıcılarının gerekli gördükleri süre zarfında danışabilecekleri bir mercii işaret etmelidir.

- Güvenlik politikalarıyla birlikte erişilmek istenen noktanın ne olduğu, politika ile ilgili olarak paylaşılan bilgiler içerisinde yer almalıdır.

- Güvenlik politikalarının özellikle web üzerinde kolaylıkla ulaşılabilir ve sürekli olarak görüntülenebilir olması gerekmektedir.

- Güvenlik politikaları dahilinde, sistemin içerisinde yer alan tüm birim, unsur ve bireylerin görev ve sorumluluk tek tek açıklanmalıdır.

- Güvenlik politikalarının uygulanmadığı durumlarda ne tür bir prosedürün izleneceği net bir şekilde açıklanmalıdır.

Buna göre bilgi güvenliği politikalarının uygulanması süre zarfında, kurumsal açıdan belki de en fazla ön planda olan konu bu hususta söz konusu olan prosedür ve uygulamaların pratikteki durumu için kurumun tüm unsurlarını bir araya getirebilmektir. Bu şekilde de sistem, mümkün olduğunca sağlıklı bir şekilde işleyebilecek ve sistemden de uygulama bazında en yüksek verim elde edilebilecektir. Bilgi güvenliği, büyük ölçüde, sistemin içerisindeki unsurların dikkatine dayalı olarak çalışmakta, bu nedenle de kurumsal bilgi güvenliği politikalarının dikkat çekici ve dikkatli olmaya yönlendiren bir yapısının olması gerekmektedir.

Kurumsal anlamda bilgi güvenliğinde, kurumun yönetici kesiminin konuya eğilimi de büyük önem arz etmektedir. Sadece konuyla teknik açıdan ilgilenen kesim değil, kurumun yöneticileri açısından da bilgi güvenliğini önemsemek ve konuya ciddiyetle eğilmek büyük bir önem taşımaktadır. Bu sayede kurumlar, yöneticileri aracılığıyla konunun ciddiye alınması açısından bir disiplin yapısına kavuşabileceklerdir (30).

2.6.3. Ulusal Bilgi Güvenliği

Bilgi güvenliği bireysel ve kurumsal anlamda kazandığı önemle birlikte artık devlet yönetimleri açısından da büyük bir öneme sahiptir. Toplumun fertlerinin ve vergiye tabi olan tüm tarafların sahip olduğu bilgiler ile devlet kurumlarının sahip olduğu bilgilerin saklanması ve korunması artık bir devlet politikası konumundadır. Devletlerin hem kendi iç yapıları hem de diğer devletler ile olan iletişimlerinde bilginin güvenliğine ihtiyaç duyulması, konunun bir devlet politikası haline gelmesini zorunlu kılmaktadır. Genel olarak bakıldığında ulusal bilgi güvenliğinin kapsamı içerisine giren unsurları aşağıdaki gibi sıralamak mümkündür (31):

- Çeşitli alanlarda bireysel ve kurumsal anlamda, devlet yönetimine bağlı taraflara karşı söz konusu olacak siber saldırıların engellenmesi adına bir koruma alanı,

- Söz konusu güvenlik ile birlikte daha nitelikli operasyonların gerçekleştirilmesi ve toplumsal refah ve huzurun teşviki,
- Bilişim ve iletişim teknolojilerinin ulusal bazda sahip olduğu kapasite kadar sahip olduğu risklerin de incelenmesi ve değerlendirilmesi,
- Prototip ya da tamamlanmış olmasına bakılmaksızın tüm bilişim altyapılarının daha dirençli hale getirilmesi.

Bilgi güvenliği ulusal bazda ele alındığında hem bireysel hem de kurumsal anlamda sorumluluk gerektiren bir konuyu ifade etmektedir. Buna göre ülke içerisinde herkesin, bilgi güvenliği konusunda farkındalığı ve profesyonel düzeyde olmasa bile konunun ciddiyetini anlayacak şekilde ya eğitim alması ya da kendisini geliştirmesi gerekmektedir (32). Gerek kişisel bilgisayarların gerekse de mobil iletişim araçlarının günlük kullanımdaki düzeyinin artması, bilgi güvenliği konusunu daha ciddi bir boyuta taşımıştır. Buna göre bireysel ve kurumsal kullanıcıların hemen hepsi kendilerine ait temel bilgiler ile hayati önem taşıyan bilgilerinin hepsini mümkün olduğunca güçlü bir şekilde korumak durumundadırlar (33).

2.7. Sağlıkta Bilgi Güvenliği

Bilgi güvenliği, kişisel verilerin korunmasından başlamak sureti ile neredeyse kurumsal yönetimin söz konusu olduğu tüm alanlara dek uzanan bir silsilede, üzerinde fazlasıyla odaklanılması gereken bir konu olmaktadır. Buna göre ölçeğine bakılmaksızın tüm kurumlar, sahip oldukları kurumlarına, kurumlarıyla ortak çalışan diğer kurumlara ve kurumlarının içerisinde ve dışarısında bulunan tüm bireylere dair sahip olunan bilgileri korumakla yükümlüdürler. Artık ulusal ve uluslararası alanda da kanunlarla koruma altına alınan bu konu, tüm kuruluşlar açısından, gerçek anlamda bir sorumluluk yükü oluşturmaktadır. Bu nedenle de kurumsal yapılar altında mümkün olduğunca geniş güvenlik önlemleri ile korunan bilgi merkezlerinin bulundurulması neredeyse bir zorunluluk haline gelmiştir.

Sağlık sektörü, bu konuda en üst düzeyli olarak güvenliğe ihtiyaç duyan alanlardan biridir. 2000'li yılların başında, dünya genelinde sağlık kuruluşlarının elektronik veri tabanı kullanarak hastalarının bilgilerini gizleme konusunda ciddi ölçekli çalışmalar gerçekleştirmelerine rağmen söz konusu veri tabanlarına gerçekleştirilen saldırılar ciddi oranda artış göstermiş ve yıllar içerisinde milyonlarca hastanın özel

bilgileri yasadışı yollarla üçüncü kişilerin eline geçmiştir (34). Bu bilgilere dijital ortamda gerçekleştirilen bu saldırıların temel sebebi, hastalara dair bazı gizli ve önemli bilgilerin, üçüncü kişiler tarafından kullanımının maddi ve manevi anlamda çeşitli getirilerinin bulunmasıdır. Hastaların kimlik bilgileri, sağlık sorunlarına dair geçmişleri, medikal anlamda görüntüler, mevcut rahatsızlıklar, rahatsızlık tehditleri, tedavi içerikleri ve geçmişleri, diyet programları, cinsel sağlık sorunları, genetik bilgileri, psikolojik profilleri, fiziksel anlamdaki eksiklikleri vb. birçok veri ve bilgi kötü amaçlı olarak çeşitli kişiler tarafından kullanılabilecek durumdadır (35).

Söz konusu bilgilerin kötüye kullanımı, sağlık kurumlarının güvenilirliği kadar hastaların sağlık kurumlarıyla iletişim kurmaları konusunda da son derece büyük bir engel teşkil etmekte ve endişeye sebebiyet vermektedir. Bu nedenle sağlık kuruluşları, illegal yöntemler ile üçüncü kişilerin eline, hastaların ve genel sağlık bilgilerinin geçmemesi konusunda yüksek ölçekli güvenlik sistemleri kullanmak durumunda kalmaktadırlar. Bu bilgi güvenliği sistemleri, kullanıcılar açısından kendilerini güvende hissetmeleri kadar tanı ve tedavi süreçlerinin niteliği açısından da büyük bir önem taşımaktadır.

Hastalara dair tıbbi merkezlerin, hastanelerin ve kliniklerin hemen hepsi, hastaların birbirleri arasında gidip gelmeleri sonucunda, mutlak olarak bir bilgi paylaşımı içerisinde olmaktadırlar. Buna göre söz konusu yerlerde bulunan veri toplanan mecralar, ciddi ölçekli olarak hastalara dair tanı ve tedavi bilgileri içermekte ve bu durum hastalara dair sahip olunan bu değerli bilgilerin mutlak olarak, dikkatli bir şekilde korunmasını zorunlu kılmaktadır (36). Bu şekilde, sağlık kuruluşlarının sadece ellerinde bilgileri bulundurmaları açısından değil, aynı zamanda bu bilgilerin paylaşımı konusunda da mümkün olduğunca bilgi güvenliği odaklı düşünmekte fayda bulunmaktadır.

Çeşitli çıkarlara odaklı olarak hareket eden bilgi korsanlığı gruplarının bulunduğu mevcut süreçte, sağlık sektörü de bu korsanların saldırılarından etkilenirken, süreç sadece bilgilerin çalınması ekseniyle işlememekte, aynı zamanda hastalara dair bilgilerin deşifre edilmesi ya da tahrip edilmesi durumudur. Her iki konuda ciddi birer güvenlik tehdidi oluşturmakla birlikte bilgilerin tahrip edilmesi, hastalara doğru tedavi yöntemlerinin uygulanması konusunda sağlık kuruluşlarının önündeki en büyük engeldir (37).

Doktorların ve geri kalan sağlık personelinin giderek daha kolay bir şekilde hastalara dair bilgilere erişmelerine karşın, ortaya çıkan tabloda, ellerinde var olan bilgilerin tahrip edilerek sisteme kaydedilip kaydedilmediğinin bilinememesi tedavi süreçleri için bir tehdit oluşturmaktadır.

Sağlık sektöründe, bilgi güvenliğine dair çerçeve netleştiği süre zarfında, güvenlik algısının ne şekilde gelişmesi gerektiğine dair bilgileri aşağıdaki unsurlar ile değerlendirmek mümkündür (38):

- Bilginin sahibi: Bilginin kurumsal ve kişisel olarak kimlerin elinde olduğu, bilgiye kimlerin erişebildiği, bilgiye dair değişiklik yapma hakkına kimlerin sahip olduğu, hastaların kendilerine ait bilgilere ne şekilde ulaşabildikleri vb. sorunların yanıtları, hastalara dair bilgilerin güvenliğinin sağlanması hususunda da bilgi vermekte, yönlendirici olmaktadır.

- Bilginin türü ve miktarı: Hastalara dair tanı ve tedavi bilgileri ile tanı ve tedavilerinin geçmişi üzerine odaklanan bilgiler ile bu bilgilerin ne kadar detaylı olarak sistemin içerisinde kendisine yer bulacağı, bu aşamada kesinleştirilmeli ve gereken kısıtlamalara tabi olmak durumunda olmalıdır.

- Bilginin saklanacağı yer: Şüphesiz, en kritik konulardan biri olan bilginin nerede saklanacağı, hastanelerin ve çeşitli sağlık merkezlerinin kendileri için belirledikleri ya da kendilerine başka kurumlardan sağlanan veri tabanı merkezlerinin kararlaştırılması ile netleşmektedir.

- Bilgilerin görüntülenmesi: Doktorların ve tedavi süreçlerini üstlenecek sağlık personelinin dışında kimlerin hastalara dair tanı ve tedavi bilgilerini görme şansının bulunduğunda dair alınacak kararlar, bilginin güvenli bir şekilde saklanması kadar güvenli bir şekilde, gereken birey ve birimlere sunulması konusunda yardımcı olmaktadır.

Bu şekilde sağlıkta bilgi güvenliğinin sağlanabilmesi adına sorumluluk alanlarının ve sorumluluk şekillerinin belirlenmesi mümkün hale gelebilecektir. Özellikle sağlık personelinin hangi kesiminin hastalara dair bilgilere erişme hakkına sahip olduğunun ya da olacağının bilinmesi ve bildirilmesi, bu şekilde bilginin güvenliğinin sağlanması adına bir çizginin çekilmesine de yardımcı olmaktadır. Nihai noktada da

hastalara dair bilgiler, sınırlar çerçevesinde olan bireyler dışındaki kimse ile paylaşılmamaktadır.

Sağlık konusundaki bilgilerin nitelikli bir şekilde depolanması ve saklanması, kullanım sürecinde, bu bilgilerden faydalanan tarafların işlerinin kolaylaşmasıyla birlikte zamandan tasarruf sağlayabilecektir. Bu nedenle de sağlık konusundaki bilgilerin mümkün olduğunca iyi bir ortam sağlandığı ve saklandığı gibi erişim konusunda da kimlerin, hangi oranda ve nerede bu bilgilerden faydalanabileceklerinin belirlenmesi gerekmektedir. Bu sayede sistemin fonksiyonelliğinin arttırılması da mümkün olabilecektir (37).

Bunun dışında sağlık sektöründe bilgi güvenliğinin genel çerçevesi içerisinde içeriğe dair belirli unsurlar söz konusudur ve bu unsurları aşağıdaki gibi değerlendirmek mümkündür (39):

- Güvenlik bileşenleri: Yazılı ve dijital ortamda olmaları herhangi bir fark yaratmaksızın hastalara dair bilgilerin ve genel sağlık ile ilgili bilgilerin korunması açısından fiziki ve sanal ortamda sistem ve dosya erişimi ön plandadır.

- Güvenlik prensipleri: Sorumluluk, farkındalık, etik, multidisipliner olma, ölçülülük, entegre olma, vakitlilik, yeniden değerlendirilebilirlik ve adil olma prensiplerinin ön plana çıkarıldığı süreçte, bilgiye ulaşım konusunda roller ve sınırlılıklar söz konusu prensiplerine kime, nerede, nasıl ve ne zaman uygulanacağının bilinmesi ile ortaya çıkmaktadır.

- Tehditler, kontrol ölçüsü ve bilgi güvencesi: Bilgisayar sistemleri üzerinden sürekli olarak tehditlerin söz konusu olduğu mevcut teknoloji çağında, bilginin güvence altına alınabileceği yardımcı programların varlığına ihtiyaç duyulmakta, aynı zamanda da bilgiye erişimin kontrolünün kime, nerede, ne zaman ve nasıl sorularına cevap verebilecek, ancak bilginin miktarına göre bir ölçüsü bulunması gerekmektedir.

- Güvenlik yönetimi: Sağlık birimlerinin dışında, bilginin yönetimi, denetlenmesi ve güvenliğinin sağlanması hususunda, sağlık personelinin dışında, konuya hâkim, uzman kişilerin görev alması önem arz etmektedir.

- Kanunlar ve düzenlemeler: Sağlık kuruluşları hem ulusal hem de uluslararası anlamda belirlenmiş olan bilgi güvenliği standartlarına uygun bir yapı kurarak bilgi depolaması, yönetimi ve paylaşımı gerçekleştirmek durumundadır.

Tüm bu uygulamalar elektronik sağlık kayıtlarının varlığına bağlı olarak ortaya çıkmakta ve sağlık kuruluşlarının sorumluluk düzeylerini arttırmaktadır. Söz konusu kayıtların sadece hastalar ile sağlık personeli arasında, sınırlı bir çevrede geçerli olması beklenen ve gereken bu bilgilerin saklanması, değerlendirilmesi ve paylaşılması, bilgilerin kullanımına izni olmayan taraflar için illegal bir duruma işaret ederken sağlık kuruluşlarının bu duruma sebebiyet verecek şekilde hareket etmemeleri beklenmektedir.

Elektronik sağlık kayıtları, hastalara dair geniş ölçekli bilgileri içerisinde bulunduran bir sistem olmakla birlikte taşıdığı öneme paralel olarak bu sistemin kullanımında nitelikli çalışanların varlığına ihtiyaç duyulmaktadır. İster sağlık personeli olsun isterse de sistemin başındaki çalışanlar olsun, sağlık kuruluşları açısından önemli olan sürecin yetkin bireylere bırakılması ve bu bireylerin konuya dair hukuki ve etik odaklı yaklaşımlarının sorgulanması gerekmektedir (40). Konunun hukuki ve etik boyutu söz konusu olduğunda, sağlık personeli ve konuyu sistematik olarak takip eden taraflar için mahremiyet konusu da ön plana çıkmaktadır. Hastalara dair bilgiler ciddi ölçekli birer mahremiyet içermekle birlikte bu bilgilerin üçüncü kişiler ile paylaşımı sürecinde hastaların rızalarının alınmadan gerçekleştirilecek her eylem, büyük ölçüde mahremiyet ihlaline girebilecek ve hastaların istemedikleri şekilde rahatsızlıklarının, tedavi süreçlerinin, kullanmış olduğu ilaçların vb. deşifre edilmesine sebebiyet verebilecektir (41).

Sağlık süreçlerinde, sağlık kuruluşların hastalara dair toplamış oldukları bilgiler açısından ciddi bir önem taşıyan etik ile mahremiyet, tarafların birbirleri arasındaki güven olgusunun gelişimi ve güçlenmesi adına da önem arz etmektedir. bu konuda, özellikle mahremiyeti ön plana çıkarmak sureti ile ciddi bir değere sahip olan bilgi kullanımı ve paylaşımı konusu, hastaların izni olmadan gerçekleştirilememektedir. Söz konusu izinler, hastaların kendilerine ait bu mahrem durumu sorumluluklarının dışına çıkmadan, kendi istedikleri şekilde yönlendirmek adına bir koruma görevi görmektedir (42).

Mahremiyet konusu göz önünde bulundurulduğu süre zarfında, sağlık sektöründe bilgilerin gizliliği konusu hem maddi hem de manevi bir boyut kazanmaktadır. Konunun maddi boyutunda hastaların bilgilerinin üçüncü kişilere, izinsiz bir şekilde aktarılmasıyla hukuki bir yaptırım zorunluluğu ortaya çıkmaktadır. Manevi açıdan bakıldığında ise rahatsızlığı ya da gördüğü/görmüş olduğu tedavi sonucunda hali hazırda psikolojik olarak zarar görmüş olan bir hastanın daha da ciddi sorunlar ile karşılaşması kuvvetle muhtemeldir. Bu nedenle sağlık sektöründeki bilgi güvenliği, son derece hassas bir nitelik taşımaktadır.

Bireyin normal hayatının akışı içerisinde, kendisinin özel ve mahrem olarak görmüş olduğu alan dokunulmazdır. Bu durum, bireyin kendisini, çevresini ve bunlara dair tüm gizli, bireylerin arasında kalması arzulanan ve üçüncü kişilerle paylaşılması istenmeyen bilgilerin ve görüntülerin gizli kalması adınadır. Aynı durum, bireylerin sağlıkla ilgili verilerinin, bilgilerinin ve görüntülerinin gizlenmesi adına da bir beklentiyi doğurmaktadır. Fakat bu noktada hastalar süreci kendi başlarına yürütmemekle birlikte, sağlık kuruluşları ve personelinin de katılımı önem arz etmektedir (43). Bu süreçte sağlık işletmelerinin ve sağlık personelinin önemsemesi ve üzerine düşmesi gereken temel konu, mahremiyet ve etik temelinde gerçekleşmemekte ve sadece hastaların bilgilerinin üçüncü kişiler tarafından izinsiz ve kanun dışı kullanımı olmamaktadır. Bunun dışında sorumlular doğal afetler, yangın, çeşitli hırsızlık girişimleri, şebeke sorunları, sunucu problemleri, elektrik kesintileri vb. konularda da hastaların sağlık bilgilerinin korunması ve yedeklerinin bulundurulması konusunda sorumludurlar (44). Bu nedenle de sağlık sektöründe bilgi güvenliği sadece bilgilerin kopyalanması ya da çalınmasıyla ilintili olarak bir gereklilik arz etmemekte, bunun ötesinde, mutlak olarak teknik ve teknik olmayan sebeplerden kaynaklı olarak ortaya çıkabilecek bilgi güvenliği sorunları konusunda sağlık kuruluşlarının ve sağlık personelinin sorumluluk alması gerekmektedir.

Sağlık kuruluşlarında bilgi güvenliği konusunda ön plana çıkarılması gereken konu başlıklarını aşağıdaki gibi sıralamak mümkündür (28):

- Sunucu güvenliği: Sağlık kuruluşlarının ellerindeki tıbbi bilgileri ve hastalarına dair bilgileri, hastalarının sayısı arttıkça daha nitelikli bir ortamda ve güvenlik odaklı olarak barındırabilmek adına sunucu ya da sunuculara ihtiyaçları bulunmaktadır. Bu sunucuların içerisindeki bilgilerin düzenli

olarak yerleştirilmesi, yedeklenmesi ve sunucu dışından söz konusu olan saldırılara karşı korunması gerekmektedir.

- İstemci erişim kontrolü: Sağlık kuruluşunun kendi iç sunucusunda, bilgilere erişme hakkı bulunan tarafların kimler olduğu ve ne gibi bir şifre ile korunacağı konusunda karar verilmesi gerekmektedir. Bu şekilde sistem, sistem dışından tarafların, izinsiz bir şekilde erişimi engellenebilecektir.

- Sistemsel saldırılara karşı koruma: Sağlık kuruluşunun sahip olduğu bilgi depolama sisteminin sadece belirli kişiler tarafından, şifre korumalı olarak erişiminin mümkün kılınması yeterli bir güvenlik önlemi olmamaktadır. Bunun ötesinde, sistemleri dış saldırılara karşı koruyacak ve çeşitli yazılım firmaları tarafından geliştirilen koruma sistemlerine ihtiyaç duymaktadırlar.

Görüntü itibari ile sağlık kuruluşları sadece sağlıkla ilgili operasyonlardan sorumlu bir yapıya sahip gibi görünseler de giderek daha fazla teknoloji ile iç içe hareket etmeleri gerektiği ve buna uygun bir teknik yapılanmayı benimsemeleri gerektiği anlaşılmaktadır. Konunun manevi anlamda hastaların ve sağlık kuruluşunun kendisine ait bilgilerinin mahremiyeti de göz önünde bulundurulduğu süre zarfında konu çok boyutlu bir hal almaktadır.

Bu açıdan bakıldığında, sağlık kuruluşlarının bilgi güvenliğini sağlamak adına uygun bir çalışan ve teknik yapı kurmasının zorunluluğu ortaya çıkmaktadır. Buna göre sağlık kuruluşları, bilgi güvenliği konusunda, aşağıda sıralanan uygulamaları benimsemesi gerekmektedir (28):

- Kuruluşa ait bir bilgi güvenliği politikasının bulunması,

- Kuruluş dahilinde bir bilgi güvenliği organizasyonunun oluşturulması,

- Kuruluşun kendisine ve sahip olduğu hasta profillerine uygun bir bilgi yönetim sisteminin kurulması,

- Kuruluş çalışanları açısından da bir insan kaynağı güvenliğinin bulunması,

- Kuruluşun sağlık sisteminin fiziksel ve çevresel güvenliğinin oluşturulması,

- Kuruluşun iç ve dış iletişim sisteminin güvenlikli hale getirilmesi,

- Kuruluş içerisinde, bilgilere erişim konusunda denetim güvenliğinin getirilmesi,
- Kuruluşun bilgi sisteminin sürekli gelişimine ve bakımına odaklanılması,
- Kuruluş içerisinden ve dışından gerçekleşen bilgi güvenliği ihlallerinin yönetimi,
- Kuruluş içerisinde sağlıkta bilgi güvenliğine dair bir kültürün oluşturulması ve sürekliliğinin sağlanması.

Bu görüntüde sağlık kuruluşları için baştan sona, güçlü ve etkin bir şekilde örgütlenmiş olan bir çalışma mekanizmasına ihtiyaç duyulmaktadır. Bu mekanizma, bilgi güvenliği açısından sağlık kuruluşlarının işlerini kolaylaştırmakla birlikte güvenilirlik ve etik konularda uyumluluk gibi birçok avantajı da beraberinde getirebilecektir. Söz konusu bilgi güvenliği mekanizmasının içerisinde yeterli ekipman ve sistem unsuruyla birlikte yetkinliği bulunan bireylerin de istihdam edilmesi büyük bir öneme sahiptir.

Sağlık kuruluşlarında, bilgi güvenliğinin sağlanması adına uygulanan koruma mekanizmalarını, genel olarak üç şekilde ele almak mümkündür (45):

- Fiziksel koruma: Sağlık kuruluşu içerisinde kimlerin hasta bilgilerine erişebileceği ile kimlerin bu bilgilere erişemeyeceklerinin bilinmesi fiziksel anlamda sistemin korunmasını ve sistemin istenmeyen tarafların kullanımına açılmasını engellemektedir. Bu şekilde üçüncü kişilerin sisteme doğrudan erişimleri engellendiği gibi aynı zamanda onların sistemin bir parçası olarak çeşitli şekillerde, bilgi ortamlarına yapılacak zararların önüne geçilmektedir. Erişim izinleri, şifreler vb. bu koruma türündendir.
- Teknik koruma: Sistem korumaları ve iletişim korumalarını içeren bu tür korumada, sistemin dışından gerçekleşecek olan erişimlerin önüne geçilmeye çalışılmaktadır. Aynı zamanda bu koruma şeklinde sistemin sadece onu kullanma izni olanların birbirleri ile iletişim kurmalarına izin veren yapı söz konusudur. Bu şekilde dışarıdan gizli ve izin dışı erişimler engellenirken, bununla birlikte bilgilerin çözümlenerek açılmasının da önüne geçilmektedir.

- Yönetimsel koruma: Büyük ölçüde bilgi sisteminin yönetimine ve korunmasına dair kuralların ve yaptırımların neler olduğunun sağlık kuruluşundaki çevre ile paylaşılmasını içeren bu koruma şeklinde, hasta bilgileri ile sürekli olarak iç içe olan sağlık personelinin ve teknik personelin bu süreçte gizli bilgileri kötü amaçlı olarak kullanmalarının hukuki olarak ortaya çıkarabileceği durumlar, yasal bir çerçevede açıklanmaktadır.

Söz konusu koruma şekillerinin her biri, bilgi güvenliğinin sağlanması adına yeterli düzeyde etkiye sahip olmakta ve kademeli olarak bilgilerin, sadece yetkili kişiler tarafından kullanılmasını kolaylaştırmaktadır. Bu yöntem, bilgilerin kullanımı açısından kimin, hangi düzeyde ve ne düzeyde sorumluluğunun bulunduğunu da ortaya koymaktadır. Genellikle sağlık sektöründe bilgi yönetimine ve güvenliğine dair algı, söz konusu bilgilerin sadece sağlık kuruluşları ve sağlık personeli tarafından kontrol altında tutulabileceği düşünülse de artık mevcut sistemlerin hastaların da sürece katılmasına izin verdiği görülmektedir.

Teknik anlamda konu incelendiğinde ise dünya genelinde sağlık kuruluşlarının benimsemiş olduğu bazı temel bilgi güvenliği sistemlerinin bulunduğu görülmektedir. Bunların hepsini şu şekilde sıralamak mümkündür (41):

- Hastane Bilgi Yönetim Sistemi: Hastanenin çalışma sistemi ile birlikte hastaların tanı ve tedavilerinin yönetiminin gerçekleştirildiği bu sistem sağlık personelinin, çeşitli kademelere ayrılmak sureti ile erişimine açılmakta ve hastaneler içerisindeki tüm genel ve detaylı bilgiler bu sistemin içerisinde saklanmaktadır.

- Health Level 7 Protokolü: Medikal sistemlerin, dünya genelinde birbirleri ile iletişiminde kullanılan bu sistemde tanı, tedavi ve ilaç kullanımı gibi temel bilgilerin taraflar arasında erişimi sağlanmakta ve gereksiz olarak sağlık kuruluşunun yönetimine dair bilgiler ekrandan çıkarılmaktadır.

- HIPAA Güvenlik Standardı: İlk olarak 1996 yılında ABD'de kullanılmaya başlanan bu güvenlik standardı sağlık sigortasına dair bilgiler eşliğinde, sadece hastalara ait bilgilerin bir ulusal ağ üzerinde konuşlandırılmasını sağlamaktadır.

Koruma ihtiyacının ortaya çıkışı, büyük ölçüde, hastaların ciddi ölçekli önem verdikleri, sağlıklarıyla ilintili konularda kendilerini mümkün olduğunca çevresel yorum ve yönlendirmelerden koruma istekleri ile ilintilidir. Zira bazı rahatsızlıklar, hastalar açısından son derece hassasiyet içerikli olabilmekte, buna istinaden de hastalar bu konuda üst düzeyli bir korumaya ihtiyaç duyabilmektedirler. Özellikle cinsel sorunlar, HIV/AIDS, genetik bozukluklar ve mental rahatsızlıklar gibi bireyi toplumdan ayıracak sağlık sorunlarına dair bir bilgi gizliliğine etkili bir şekilde ihtiyaç duyulmaktadır (46). Hastaların bu noktada beklentisi, mevcut sistemin mümkün olduğunca kendilerinin de kullanabileceği ve güvenlik düzeyi yüksek bir hale getirilmesidir. Söz konusu güvenlik algısının içerisinde, hastaların, kendilerine ait bilgileri, mümkün olduğunca kolay bir şekilde görüntüleyebilmeleri, belirli ölçüde güncelleyebilmeleri ve gerektiğinde, sağlık kuruluşları ve sağlık personeli ile iletişim kurarak değiştirmeleri de bulunmaktadır (47).

Bilgilerin yeterli düzeyde bir güvenlik durumlarının olmaması, her anlamda bir ihlali ifade ederken, sağlık kuruluşlarının bu konuya eğilmesi kadar aynı zamanda hukuki makamların ve genel ulusal ve uluslararası hukuki yapının özel olarak bu konu üzerine odaklanmış olması gerekmektedir. Her ne zeminde olursa olsun, bu konuda gerekli korumanın hastalara sağlanması onların bir yasal hakkı olduğu kadar kendilerine özel olan bir durumun dışa vurulmasını engelleme adına istekleri olmaktadır (48).

Sağlık sektöründe bilginin önemini sadece hastalara dair bilgilerin üçüncü kişiler tarafından ele geçirilme tehlikesi ile ilintili olduğunu düşünmek de yanlış olacaktır. Çünkü hastalara dair bilgiler, bir sorun yaratma ya da gizlilik içerme hususunun da ötesinde, hastalara acil müdahale gereken durumlarda onların sağlık detaylarına erişim konusunda da önem arz etmektedir. Buna göre sağlık sektöründe bilgi, hastalara dair tanı ve tedavilerin neler olduğunu içermesi ile birlikte, anlık müdahale süreçlerinde de önem arz etmektedir (49).

2.8. Türkiye'de Sağlık Sektöründe Bilgi Güvenliğine Dair Mevzuat

Bilgi teknolojilerinin ve bilgi saklama konusundaki çalışmaların dünya genelinde gelişimi ile birlikte Türkiye de sağlık kuruluşlarında bilgi teknolojilerinden aktif bir şekilde yararlanmaya başlayan bir ülke olarak bilgi güvenliği konusunda uygulamalarını geliştirmeye başlamıştır. Fakat konunun hukuki boyutunun daha büyük bir önem arz ettiği süreçte Türkiye özellikle 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca sağlık bilgilerinin korunması konusunda da bireyleri koruma altına

almaya çalışmaktadır. Bu noktada, sağlık sektörü üzerinde uygulanan ve Türkiye Cumhuriyeti Sağlık Bakanlığı tarafından Kişisel Sağlık Verilerinin İşlenmesi Ve Mahremiyetinin Sağlanması Hakkında Yönetmelik'in genel çerçevesini incelemek gerekmektedir (50):

- Yönetmelik, Sağlık Bakanlığı'ndan başlamak üzere en küçük yerleşim birimlerinde sorumlu olan sağlık personeli ve teknik personele kadar herkesi kapsamaktadır (Madde 4/1),

- Yönetmelik, her türlü sağlık birimine, yeterli bilgi birikimi ve yetkinliğe sahip olan bir teknik ekip kurulmasını zorunlu kılmaktadır (Madde 4/1[l]),

- Yönetmelik, kişisel sağlık verilerinin sadece sorumlu kişiler tarafından incelenerek depolanmasını, gerekli izinler alındığı süre zarfında ve yetkili kişilerin kontrolü altında paylaşılması ve işlenmesini mümkün kılmaktadır (Madde 5/1-9),

- Yönetmelik, verilerin korunmasıyla sorumlu olan kimseleri verilerde ortaya çıkabilecek olan tahribat ve genel saldırıları yetkili birimlere bildirmekle ve veriler ile iletişim içerisinde olabilecek kimse ve tarafların kayıt altına alınarak gerekli hallerde kontrol edilmesi ile yetkilendirmektedir (Madde 6/1-8),

- Yönetmelik, ilgili sağlık kuruluş ve kurullarına, gerekli görülen ve sağlık bilgilerinin sahibi olan tarafların haklarının zarara uğramasına izin vermeyecek şekilde söz konusu bilgilerin kullanılması, işlenmesi ve paylaşılması konusunda yetki tanımaktadır (Madde 7/1-4),

- Yönetmelik, ilgili sağlık kuruluş ve kurullarına, gerekli görülen ve sağlık bilgilerinin sahibi olan tarafların haklarının zarara uğramasına izin vermeyecek şekilde söz konusu bilgilerin aktarılması hususunda, genellikle anonim veri aktarımı temelinde, bir hukuki sözleşmeye, protokole vb. dayandırılmak sureti ile yetki tanımaktadır (Madde 8/1-4),

- Yönetmelik, sağlık bilgisinin sahibi olan kimselere, daha doğrusu bireylere, yetkili kimselere eşliğinde, kendilerine dair bilgileri görme, izleme, işleme,

değiştirme ve gerektiğinde bir kopyasını elde etme hakkını sunmaktadır (Madde 10/1-3),

- Yönetmelik, veri sorumlusu olan kimselerin, verinin sisteme girişinden sistem aracılığıyla, diğer kimselerle, kanuni hükümlerle paylaşılmasına kadar geçen süre zarfı içerisinde, sürekli olarak verilerin kontrolü, korunması, hukuki normlara uygun olarak paylaşılması ve buna istinaden de çeşitli siber saldırıların ve bilgilerin zarara uğratılmasına dair uygulamalara dair yetkililerin haberdar edilmesi konusunda sorumluluk vermektedir (Madde 11/2-7),

- Yönetmelik, merkezi sağlık veri sistemi ve kişisel sağlık kaydı sistemi dahilinde, sağlık verilerinin ne şekilde saklanması, paylaşılması ve sistem üzerinde hangi hukuki sorumluluklar dahilinde çalışmalar yürütülebileceğine dair bilgilendirmede bulunmaktadır (Madde 14, Madde 15).

2.9. Sağlık Bakanlığı Bilgi Güvenliği Uygulamaları

Sağlık Bakanlığı bilgi güvenliği çalışmalarını iki temel unsur üzerine kurmuştur. Sağlık kuruluşlarının hukuki ve idari işleyişlerini düzenleme adına Bilgi Güvenliği Politikaları Yönergesi ve Bilgi Güvenliği Politikaları Kılavuzu kurumlara yol gösterici olmaktadır (51).

Bilgi Güvenliği Politikaları Kılavuzu 28/02/14 tarih 5181.1272 sayılı onay eki ile yürürlüğe giren "Bilgi Güvenliği Politikaları Yönergesine'' istinaden Sağlık Bilgi Sistemleri Genel Müdürlüğü'nce hazırlanmıştır. Sağlık bakanlığına bağlı tüm kuruluşlara resmi olarak bildirilmiş olup; bilgiguvenligi.saglik.gov.tr adresinde yayınlanmıştır (52).

Bilgiyi toplama, değerlendirme, raporlama, paylaşma süreçlerinde gerekli önlemleri almak, bilgiyi kasıtlı veya kasıtsız tüm tehditlerden korumak, yönetici ve personelin duyarlılık ve farkındalığının artırılmasını sağlamak, güvenlik zafiyetlerinin ortadan kaldırılması böylelikle bilginin bütünlük, gizlilik, ulaşılabilirlik ilkelerinin sağlanması, ekonomik zararın önlenmesi ve kurum imajının olumlu devam etmesi, kurumda bilgi birikimi oluşturmak Sağlık Bakanlığı bilgi güvenliği amaçları arasında yer almaktadır.

Sağlık Bakanlığı bilgi güvenliği uygulamaları merkez ve taşra teşkilatında yer alan tüm bilişim sistem kullanıcıları, paydaşları, tedarikçileri kapsamaktadır. Kurumlarda koordinatör bilgi güvenliği yetkilisi görevlendirilmelidir. Bu yetkili kurumlardaki bilgi güvenliğinden sorumlu olmalıdır. Sağlık Bakanlığı bilgi güvenliği yaklaşımlarının temel standartı TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi ile belirlenmiştir. Bu standart kurumlara sistematik ve doküman anlamında yol gösterici olmaktadır. Bakanlığın Sağlık Bilgi Sistemleri Genel Müdürlüğü bu aşamada kurumlara alt yapı destek sağlama ve geliştirme çalışmaları yapmaktadır (51,52).

2.9.1. Bilgi Güvenliği Politikası

Sağlık Bakanlığı nüfusun tamamıyla ilgili önemli kişisel ve sağlık bilgilerinin mevcut olduğu stratejik bir kurumdur. Hastalar, hastaneye müracat ettiğinden itibaren en gizli ve mahrem bilgileri kurumun verilerine işlenmektedir. Sağlık kuruluşları bu mahrem bilgilerin kendisine emanet edilmiş olması sorumluluğuyla bilgilerin güvenliği ve korunması sürecine idari, teknik ve hukuki boyutuyla gereken önemi vermekle yükümlüdür (51,52):

Sağlık Bakanlığı bilgi güvenliği politikalarını aşağıdaki şekilde sıralamak mümkündür.

- Çalışanların kişisel dosyaları güvenli alanlarda saklanmalı, gizlilik içeren belgeler için kilitli dolap kullanılmalıdır.
- Tüm personelin kimlik kartı takması zorunlu hale getirilmelidir.
- Fiziksel ve çevresel güvenlik önlemleri alınmalıdır.
- Hassas bilgileri içeren alanlar için yetkili kişilere izin verilmelidir.
- Doğal felaketler (Deprem, yangın, sel, patlama) hasarlara karşı önlemler alınmalıdır.
- Temiz masa prensibi her zaman uygulanmalıdır. Bu kapsamda; üzerinde çalışılmayan evrak, form, fiş, fatura, dosya gibi her türlü yazılı doküman masa üzerlerinde, hasta veya ziyaretçilerin erişilebileceği yerlerde bırakılmamalıdır. Bu dokümanlar güvenli bir şekilde saklanmalıdır. Ayrıca, bilgisayar ve sunucu gibi veriye doğrudan erişim sağlayabilecek her türlü cihaz kullanılmadığı

zamanlarda tamamen veya ekran kilidiyle yetkisiz kişilerin erişimine kapatılmalıdır. Özellikle masa başında olunmadığı zamanlarda kişisel bilgisayarlar kilitlenmelidir.

- Şifreler kesinlikle başkalarıyla paylaşılmamalıdır. Belirli aralıklarla sistem, çalışanların şifrelerini değiştirmesine yönlendirmelidir. Kişiler sisteme kullanıcı adları ve şifreleri ile bağlanmalıdır.

- Bilgisayarlarda güncel virüs programları bulunmalıdır. Bu programlar düzenli olarak güncellenmeli, korsan yazılımlar kullanılmamalıdır.

- Parola standartları belirlenmeli, uygun parolalar seçilirken kolay ele geçirilen nitelikte olamamalıdır.

- Hassas bilgilerin korunması için kriptolama yönteminden faydalanılmalıdır.

- Kimliği belirsiz, zararlı olduğu düşünülen, spamlar, E-postalar açılmamalı ve yanıt verilmemelidir.

- Bilgiler mutlaka yedeklenmelidir.

- Kullanılan bütün ağlar için güvenlik tedbirleri alınmalıdır. Hastaların sağlık bilgilerinin ulaştırıldığı ağlar için de güvenlik tedbirleri alınmalı ve kesinti olması durumunda eylem planları hazırlanmalıdır.

- Bilgi güvenliğinin ihlal edildiği durumlarda kayıt altına alınıp, raporlanmalıdır. İhlale sebep olan kişi ve kişiler hakkında kınama, para cezası, uyarma, sözleşme feshine kadar uzanan yaptırımlar uygulanır.

- Kurumlar bilgi güvenliği iç denetim süreçlerini oluşturmalıdır. Denetimler sertifikalı,yetkin kişilerce yapılmalıdır.

- Acil durumlar için eylem planları oluşturulmalı ve aralıklarla bu planların etkin işleyip işlemediği test edilmelidir.

2.9.2. Bilgi Güvenliği İhlal Yönetimi

Bilgi güvenliği ihlali oluşması durumunda bakanlığa olay raporlanır. Bu sürece neden olan kişi ve kişiler hakkında hukuki süreç başlatılır. Çalışanlar bilgi güvenlik ihlallerini önlemek için gördükleri güvenlik açığı ve zafiyetlerini yönetimlerine bildirmek ve raporlamak zorundadırlar (50).

2.9.3. Bilgi Güvenliği Denetimleri

Genel müdürlük yönerge kapsamında gerekli denetimlerini yapar. Bu denetimlerde bilişim güvenliği ve sosyal mühendislik testleri kullanılır . Denetimleri yapacak personelin eğitimleri de bakanlıkça yürütülür. Denetim yetkin kişilerce yapılmalıdır (51).

2.9.4. Gizlilik Sınıfları ve Gizlilik Anlaşmaları

Genellikle sağlık işletmelerinde "Gizli", "İç Kullanım" ve "Kamuya Açık" olmak üzere üç adet gizlilik sınıfı kullanılmaktadır. Gizli, işletmenin menfaatlerini doğrudan etkileyebilecek, özellikle rakiplerin ulaşmaması gereken özel, kritik ve hassas bilgiyi ifade etmektedir. (Örneğin: Hasta kredi kartı numaraları, yayınlanmamış finansal tablolar, hasta kimlik ve adres bilgileri). İç Kullanım, hizmete özel, sadece iş tanımı gereği yetki verilen kişilere açık olan bilgiyi ifade eder. Sağlık işletmesi dışındakiler tarafından görülmemesi gereken veya resmi otorite tarafından talep edildiğinde sadece söz konusu bilgi varlığının sahibinin onayı ile bu makamların erişimine açılan bilgidir (Örneğin: Sağlık işletmesi iç mevzuatı, elektronik ve fiziki arşivde saklanan dokumanlar, süreç dokümanları). Kamuya Açık Bilgi ise sağlık işletmesi yetkilileri tarafından kamuya açılan bilgiyi ifade eder. Yetkisiz kişiler tarafından değişiklik yapılmaması gerekli olan bilgidir (Örneğin: Sağlık işletmesi hisselerinin borsalarda işlem görmesi nedeniyle açıklanması gereken bilgiler, işletmenin internet sitesinde yayınlanan bilgiler, ürün tanıtımı amaçlı broşür, afiş vb. materyal) (52,53).

Basılı veya elektronik ortamdaki bilgilerin sınıflaması gizlilik derecesinin tanımları dikkate alınarak, bilgi varlığının sahipleri tarafından yapılmalıdır. Varlığın gizlilik sınıfını gösteren işaretleme sistemi, farklı ortamlar için ayrı ayrı ele alınmaktadır. Basılı ortamdaki bilgilerin sınıfı, doküman üzerine uygun işaretlerin konulması (kamuya açık bilgi için işaret gerekli değildir) yoluyla, elektronik ortamdaki bilgilerin sınıfı ise dokümanların "başlık" kısmına gizlilik sınıfının yazılması yoluyla belirlenmelidir.

Sınıflandırılmış bilgi içeren sistemlerin çıktıları da sınıflarına uygun şekilde işaretlenmelidir.

Elektronik ortamda yer alan "Gizli" bilgiler sadece yetkili kişilerin erişebileceği ortamlarda şifreli olarak saklanmalıdır. "İç Kullanım" bilgileri ise sadece yetkili kişilerin erişebileceği alanlarda tutulmalıdır. Gizli veya iç kullanım bilgilerinin prensip olarak mobil cihazlarda taşınmaması, özel durumlarda ise şifreli olarak taşınması faydalı olacaktır. Tüm kurumsal kayıtlar yasal yükümlülüklerin gerektirdiği süre kadar, gizlilik sınıflarına uygun önlemler alınarak saklanmalıdır.

"Gizli" ve/veya "İç Kullanım" bilginin dış taraflarca görülmesini gerektiren durumlarda, gizlilik anlaşmaları imzalanması faydalı olacaktır. Anlaşmada, kimin hangi koşullarda bilgiye erişeceği, erişilen bu bilginin ifşa edilmemesi için yapılması gerekenler, anlaşmanın süresi, anlaşma sonlandığında bilginin ne şekilde geri alınacağı/imha edileceği ve anlaşma kurallarına uyulmaması durumunda uygulanacak yaptırımlar yer almalıdır. Ayrıca çalışılacak firmaların seçiminde, bu firmaların ilgili uluslararası standartları sağlaması tercih nedenidir (53).

Gizlilik anlaşmaları, gizli bilgilerin korunabilmesi ile ilgili gereksinimleri ve yasal yaptırımları içerir. Anlaşmalar, kurumun bilgiyi koruma ihtiyacına uygun olarak belirlenir ve düzenli olarak gözden geçirilir (53):

- Kurum, çalışanlara gizlilik sözleşmesi imzalatarak kurumda edinilen bilgilerin güvenliğini ve gizliliğini güvence altına alır.
- Çalışan kurumda edindiği bilgileri herhangi bir kişi ve grupla paylaşamaz, hiçbir kuruluşun çıkarları için kullanamaz.
- Kişi kurumda edindiği bilgiler hakkında yazılı ve sözlü açıklama yapamaz.
- Verileri silemez, çoğaltamaz,değiştiremez, nakledemez.
- İhlali sonucu doğacak tüm hukuki ve cezai yaptırımları çalışanlar peşinen kabul eder.

2.9.5. Kurumsal Gizlilik Sözleşmesi

Sağlık Bakanlığının bilgi güvenliğini sağlama adına kurumlarla yaptığı anlaşmadır. Sağlık kuruluşlarının kendi kurumsal bilgilerini korumada gösterdikleri hassasiyeti Sağlık Bakanlığına karşı taahhüt etmeleridir (54).

2.10. Hastane Bilgi Yönetim Sistemi

Hastaneler birbiriyle bağlantılı uzmanlık dallarını barındıran karmaşık yapıda olan sistemlerdir. Hastane Bilgi Yönetim Sistemi hastanelerin tıbbi ve idari işlemlerini bilgisayar üzerinden farklı modüller ve farklı kullanıcılar aracılığıyla yapmalarını sağlayan, birbirine entegre edilmiş bir sisteme veri ve bilgilerin işlenmesi, gerekli bilgilerin istenildiğinde anlamlı bir şekilde geri çağrılması için arşivleyen, hastanelere işgücü, zaman, maddi kazanç, güvenilir ve doğru istatistiki bilgi sağlayan yazılımlardır (55,56):

Hastane Bilgi Yönetim Sisteminin kuruluşlara katkısı;

- Hastanın tıbbi bilgilerine en kısa sürede ulaşılmasını sağlayan bu sistem tanı ve tedavi sürecine katkı sağlar.
- Hasta bakım kalitesi arttırarak, hizmet kalitesinin artmasına olanak sağlar.
- Sağlık kurumları ve diğer kurumlar arasında bilgi akışını sağlar.
- Hasta ve çalışan bilgi mahremiyetini sağlar.
- Hata ve riskleri azaltır. Gereksiz işlemleri ortadan kaldırır.
- Zaman, maliyet ve işgücünden tasarruf sağlar.
- Verimliliği artırır.
- Kırtasiye giderlerinden tasarruf sağlar.
- Doğru ve güvenilir istatistiki bilgi oluşur. Yeni bilgilerin ortaya çıkmasına kaynak sağlar.

Sağlık kuruluşlarının tüm faaliyetlerinde üretilen veya yararlanılan bilgi varlıklarının yanlış kullanımına, yetkisiz ifşaatına, kaybedilmesine, zarar görmesine

neden olacak eylemler, müşteriler, hissedarlar, iş ortakları ve kamu otoritesi karşısında kurumun karlılığını, hizmet kalitesini, bilançosunu, kurumsal itibarı ve imajını olumsuz yönde etkileyebilecek riskler taşımaktadır. Sağlık kurumlarının bilgi varlıklarının ve bunların güvenliğine yönelik risklerin tespit edilerek, uluslararası standartlara uygun olarak yönetilebilmesi için ilgili sağlık kurumları bünyesinde Bilgi Güvenliği Yönetim Sistemi BGYS kurulması gerekmektedir (57).

Bilgi güvenliğine ilişkin gereksinimlerin uluslararası kabul gören ISO 27001 standardına uygun olarak karşılandığı bir yapının oluşturulması, kurumsal bilgi güvenliği politikaları ile BGYS prosedür ve talimatların hazırlanması, gözden geçirilmesi ve yönetiminin sağlanabilmesinin temel hedefleridir (11).

BGYS çalışmaları kapsamında sağlık kurumlarının sahip olduğu tüm bilgi varlıklarının envanteri oluşturulmalı ve bilgi varlıklarının sahipleri belirlenmelidir. Varlık sahipleri tarafından gizlilik, bütünlük ve erişilebilirlik açısından söz konusu bilgi varlığının kurum için önemi saptanmalıdır. Bu bilgi varlıklarının maruz kalabilecekleri tehditler ve bu tehditlere ne kadar açık oldukları belirlenmeli, risklerin gerçekleşme olasılıkları değerlendirilmelidir. Söz konusu değerlendirme çalışmasına periyodik olarak devam edilmelidir (11).

Sağlık işletmesi bünyesinde görev yapan her kademedeki yönetici, tüm çalışanlar, firma çalışanları ve yardımcı kuruluşlar bilginin gizliliğini, doğruluğunu ve bütünlüğünü korumakla, bilgi kaynaklarını her zaman ayakta tutabilmek konusundaki sorumluluklarını yerine getirmekle yükümlü olduklarının, aksaklıklardan sorumlu tutulacaklarının bilincinde olmalıdırlar (58).

Sağlık işletmesinde farklı koruma gerektiren bilgi varlıklarının saptanması ile bu bilgi varlıklarının her aşamadaki işaretleme, koruma ve imha yöntemlerinin tanımlanması gerekmektedir. Bu süreç gizlilik, önem ve ivedilik açısından farklılık gösteren bilgilerin değişik aşamalarda ne şekilde ele alınacağını belirler. Günlük çalışma hayatındaki küçük kararları dahi etkileyebileceğinden farkındalık düzeyinin oldukça yüksek olması gereken bir süreçtir. ISO 27001 standardı bilgi güvenliğini; bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması olarak tanımlamaktadır (52):

- Gizlilik ilkesi; önemli ve hassas bilgilerin yetkisi olmayan kişilerin erişimine karşı korunarak sağlanmaktadır.

- Bütünlük ilkesi; bilginin değiştirilmesine karşı korunarak sağlanmaktadır.
- Erişilebilirlik ilkesi; bilginin ihtiyaç duyulduğu anda ve yerde hazır bulundurularak, bilgiye kolay ulaşabilmesi sağlanmaktadır

Hastanelerin organizasyonu hastanelerde görev yapan çalışanlara sağlık ekibi üyesi, sağlık personeli, sağlık çalışanı ya da sağlık insan gücü denilmektedir. Hastanelerde görev yapan personelin en ayırt edici özelliklerinden birisi, görevlerini ekipler halinde gerçekleştirmeleridir. Sağlık ekibi; hastanelerde, hasta ve yaralılara detaylı, kapsamlı ve kaliteli sağlık hizmetinin verilmesini ortak gaye olarak gören, farklı sağlık meslek çalışanlarının toplu olarak görev yaptıkları bir takımdır. Sağlık ekibi, her bir çalışanın koordinasyon içerisinde kendi eğitimine uygun görevlerini yerine getirdiği, bilgi, tecrübe ve deneyimlerin paylaşıldığı, ortak kararların alındığı ve uygulandığı bir ekip olarak açıklanmaktadır (59).

Sağlık personelinin sayısı, kalitesi, fiziki dağılımı ve eğitim seviyesi gibi özellikleri hastanelerde ve toplumun bütününde sunulan sağlık hizmetinin kalitesini belirleyen en önemli faktördür. Sağlık personeli, bakım ve tedavi hizmetlerini en iyi şekilde sunmak amacıyla beceri ve bilgilerini bir araya getirerek, birbirini tamamlayıcı nitelikte ve kendine özgü faaliyetler gerçekleştirerek hizmet vermektedir. Bununla birlikte günümüzde sağlık hizmetinin direkt olarak sunan personel dışında, Kalite Yönetim Direktörü, Pazarlama Uzmanı, İnsan Kaynakları Yöneticisi, Satın Alma Uzmanı gibi görevler de kritik düzeyde önem kazanmıştır. Bilgi güvenliği sistemi kapsamında da direkt olarak sağlık hizmetini sunanların sorumluluğu olduğu gibi en öncelikli sorumluluk bu anılan ve günümüzde önem kazanmış olan idari kadrolarındır (60).

Bilgi sistemlerine ilişkin en temel sorumluluk sağlık işletmesi çalışanlarındadır. En öncelikli sorumlulukları ise kurumsal güvenlik politikalarına, prosedür ve standartlarına uygun hareket etmek ve bilgi güvenliğiyle ilgili eğitim eksikliği duyduğu durumlarda bu durumu Birim Güvenlik Sorumlusu'na bildirmektir. Sorumluluğu altındaki bilgi varlıklarını uygun şekilde korumak, güvenlikle ilgili bir ihlal tespit ettiğinde, bu durumu bildirmek ve güvenlik politika, prosedür ve standartlarına ilişkin değişiklik önerilerini aktarmak da öncelikli çalışan sorumlulukları arasındadır.

Ancak her ne kadar temel sorumluluk çalışanlarda olsa da sağlık işletmesinde bulunması durumunda Bilgi Sistemleri ve Güvenliği Yönetimi Komitesi üyelerinin sorumlulukları en öncelikli ve büyüktür. Genellikle komite tüzüklerinde ilgili rol ve sorumluklar açıklanmaktadır. Komitenin ardından bilgi güvenliğinden sorumlu yöneticilerin sorumlukları başlamaktadır. Söz konusu sorumluluklara, sağlık işletmesi bünyesinde güvenlik politikasının tüm mekanizmalarıyla işler halde olduğunu denetlemek, gerektiğinde ilgili hukuksal süreçlerin devreye alınmasını ve güvenlikle ilgili kasıtlı veya kasıtsız ortaya çıkan vakaların incelenmesini sağlamak örnek olarak gösterilebilir. Ayrıca, BGYS politikalarını ve politikalardaki değişiklikleri onaylamak, politikaların güncel durumlarıyla ilgili bilgi sahibi olmak, sağlık işletmesi içinde çalışanların bilgi güvenliği yönetimi süreçlerine katkısı için gereken önlemleri alınmak, ödül ve ceza mekanizmalarının tanımlanmasını sağlamak da bilgi teknolojilerinden sorumlu yöneticilerin bilgi güvenliği kapsamındaki sorumluluklarındandır (61).

Sağlık işletmesinde ideal koşullarda her birim için bir bilgi güvenlik sorumlusu ataması yapılmış olmalıdır. Böylece birimlerde muhatap belirlenir ve gerektiğinde hızla bilgilendirme yapmak ya da aksiyon almak tüm çalışanlar yerine, çalışanlara aktarılmak üzere tek bir personel ile iletişime geçilebilmesi nedeniyle daha kolay olmaktadır. Birim güvenlik sorumluları genellikle birim yöneticileri ya da bunların yardımcıları olmaktadır. Birim güvenlik sorumlularının bilgi güvenliği sistemi içerisindeki rolleri, birim çalışanlarının politika ve prosedürlere uygun çalışmasını sağlamak, sorumluluğu altında bulunan bilgi varlıklarında bilgi güvenliği risklerini etkileyecek bir değişiklik olduğunda, risk değerlendirmesi yapılması için Bilgi Sistemleri ve Güvenliği Yönetimi Komitesini bilgilendirmek ve bilgi güvenliği eğitimlerine gerekli katılımı sağlamaktır. Ayrıca, birimine bağlı kullanıcılar ile birimine ait varlıklara erişim talebinde bulunan kullanıcılara verilen yetkileri, ayrıcalıkları ve yetki seviyelerinde talep edilen değişiklikleri onaylamak da önemli bir görevleridir. Buna ek olarak, birimiyle ilgili güvenlik ihlal ve vakalarını, Bilgi Sistemleri ve Güvenliği Yönetimi Komitesine bildirmek ve biriminin diğer kurumlarla yaptığı çalışmalarda/anlaşmalarda bilgi güvenliği ile ilgili gereksinim ve kuralları Bilgi Sistemleri ve Güvenliği Yönetimi Komitesinden görüş alarak belirlemek de birim yöneticilerinin bilgi güvenliği kapsamındaki sorumluluklarıdır (61).

Sağlık işletmelerinin insan kaynakları yöneticilerinin de bilgi güvenliği kapsamında önemli sorumlulukları bulunmaktadır. BGYS'nin kapsamını, politikalar çerçevesindeki yetki ve sorumlulukları oryantasyon programı dahilinde işe yeni başlayan personele tebliğ etmek ve BGYS politikalarına uygun davranmayan personel ile ilgili yaptırımların belirlenmesini ve uygulanmasını sağlamak bunlardan önemli olanlarıdır. Ayrıca, personelle ilgili işe başlama, tayin, terfi, işten çıkarma, görev değişikliği, istifa, izin gibi durum değişikliklerinin bilişim sistemlerine hızla yansıtılmasını ve bilgi Sistemleri ve Güvenliği Yönetimi Komitesinden gelen bilgi güvenliği farkındalık eğitimlerinin düzenlenmesi taleplerini değerlendirerek bu eğitimlerin gerçekleştirilmesini sağlamak da insan kaynağı yöneticisine atanmış rol ve sorumluklardandır (28).

Konunun doğası gereği bilgi güvenliği bilgi sistemleri yöneticilerine de temel sorumluluklar getirmektedir. Bilgi sistemleri yöneticisinin, sorumlu olduğu bilgi sistem ve servislerinin güvenli yapılandırılmasını, kurulmasını ve işletilmesi ile sorumlu olduğu bilgi sistem ve servislerinin izlenmesini ve BGYS'ye aykırı durumların tespitini sağlamalıdır. Ayrıca, sorumluluğu altında bulunan bilgi varlıklarında bilgi güvenliği risklerini etkileyecek bir değişiklik durumunda, risk değerlendirmesi yapılması için Bilgi Sistemleri ve Güvenliği Yönetimi Komitesini bilgilendirmelidir. Buna ek olarak, teknolojik gelişmeleri takip ederek kuruma yarar sağlayacak yeniliklerle ilgili bilgi derlemek ve bilgi güvenliği ile ilgili olabilecek hususlar hakkında yine Bilgi Sistemleri ve Güvenliği Yönetimi Komitesini bilgilendirmek de atanan rollerdendir. Ayrıca, sorumluluğu altındaki sistemlerin yetki yönetimlerinin Bilgi Güvenliği Politikaları çerçevesinde yapılmasını sağlamak, kurumsal bilgilerin yedeklenmesini ve yedeklerin kullanıma hazır olmasını sağlamak, tespit ettiği güvenlik açık ve olayları ile alınan önlemleri Bilgi Sistemleri ve Güvenliği Yönetimi Komitesine rapor etmek ve BGYS Acil Durum Ekibi'nin yöneticilik görevini üstlenmek de bilgi sistemleri yöneticisinin sorumluluklarındandır (61).

2.11. Hastane Kalite Yönetim Direktörlerinin Rol ve Sorumlulukları

Sağlık işletmelerinde kalite yönetim direktörleri işletmenin sağladığı tüm hizmetlerini devamlı olarak iyileştirmek, kaliteli, etkin ve verimli hizmet sunumunun sağlandığına ilişkin güvence vermekten sorumludurlar. Sunulan hizmetin kalitesinin analizi ve yorumlanmasıyla elde edilen verileri sağlık işletmesinin ilgili birimlerine iletmek, oluşturulan tüm kalite yönetim sistemlerinin amaçlandığı şekilde işlemesine

ilişkin kurum içi organizasyonu sağlamak, ayrıca kalite yönetim sistemlerinin çalışma usul ve yöntemlerini belirlemek üzere gerekli kural ve esasları oluşturmaktır (62).

Kalite yönetim direktörlerinin kalite yönetim birimlerinin belirlenen faaliyet alanı içerisinde görev yaptıkları dikkate alındığında kalite yönetim direktörlerinin rol ve sorumluluklarının ilgili birim görev tanımı üzerinden değerlendirilmesi de faydalı olacaktır. Örneğin, Kalite Yönetim Birimi, sağlık işletmesinin performans ve kalite çalışmalarına ilişkin kararları almaktan ve alınan kararların uygulanması için gerekli yürütme ve denetim çalışmalarını gerçekleştirmekten sorumludur. Bu kapsamda gerekli çalışma kural ve araçlarını belirler, politika ve stratejileri oluşturur. Bilgi güvenliğine ilişkin politika ve prosedürler ile standartlar kapsamında hazırlanarak sağlık işletmesine duyurulan yönetmelikler de bu görev kapsamında oluşturulan metinlerdir. Zaman zaman kalite yönetim direktörleri ve Kalite Yönetim Birimi personeli dışında özellik arz eden kalite ve performansın takibine ilişkin konularda çalışma grupları oluşturulabilmektedir.

Kalite yönetimi direktörü sağlık işletmesinin genel ve toplam performans ve kalite (bilgi güvenliği, müşteri hizmet seviyesi, vb.) hedeflerini oluşturmak, söz konusu hedeflerin gerçekleştirilmesi amacıyla gerekli faaliyetleri planlamak, izlemek, denetlemek ve sonuçlarını değerlendirmekten sorumludur. Kalite yönetimi direktörü hasta tedavi hizmet ve süreçleri ile hasta ve personel güvenliğinin geliştirilmesi doğrultusunda ihtiyaç duyulan kaynakların belirlenmesi, sınıflandırılması, uygun bulunanların temini ve bu kaynakların en etkin şekilde yönetilmesini sağlamak için çalışmalıdır. Bu sorumluluk kapsamında da bilgi güvenliğine ilişkin gerekli teknik alt yapının oluşturulması, bilgi sistemlerinin satın alınması, personele yönelik eğitim ve bilgilendirme etkinliklerinin düzenlenmesi faaliyetleri gerçekleştirilmelidir (62).

Kalite yönetim direktörü sağlık işletmesinin birimlerinin süreçlerini tanımlamak, süreç ve alt süreçlerinin sorumlularını tespit etmek, görev yönetmeliklerini oluşturmak ve sağlık hizmetlerinin belirlenen standartlar çerçevesinde daha üst kalite seviyelerine taşınması amacıyla kurum içi ve gerekirse danışmanlık yoluyla kurum dışı ekipleri oluşturmalıdır. Bu kapsamda bilgi güvenliği kapsamında sağlık işletmesi birimlerinin sorumluluklarının belirlenmesi, görevler kapsamında yetki ve sorumlulukların atanması ve bunların izlenmesi kalite yönetim direktörünün sorumluluğundadır. Ayrıca bilgi güvenliğine ilişkin mevcut ya da potansiyel problemleri saptamak, sorunları öncelik ve risk sırasına sokmak, kalite yönetim birimine aktarılan problemlere yönelik düzeltici ve

önleyici aksiyonların alınması ile geliştirme çalışmaları yapmak da bilgi güvenliği sistemine kalite yönetim direktörünün sağladığı önemli katkılardandır. Bilgi güvenliğine ilişkin farkındalık düzeyinin artması da kalite yönetim direktörlerinin sorumlulukları arasındadır. Şöyle ki, sağlık işletmesi personelinde risk yönetimi ve bilgi güvenliği anlayış ve farkındalığının oturması için çeşitli faaliyetler yapmalı, farkındalık seviyelerini ölçmelidir. Sağlık işletmesinin bilgi güvenliği seviyesinin belirlenmesi, standart anket testlerinin ya da mülakatların uygulanması, sisteme ilişkin öneri ve şikayetlerin değerlendirilmesi, mevzuata uyumun sağlanması ve yasal denetimlerde denetçiler ile iletişim sağlanması da yine kalite yönetim direktörü ve yardımcılarının görev alanı içerisinde kalmaktadır (63).

Bilgi Güvenliği Sistemimin tam olarak işleyebilmesi için tanımlı ve düzenli olarak uygulanan bir denetim sürecine de ihtiyaç duyulmaktadır. Söz konusu süreç ile sağlık işletmesi tarafından belirlenen politika ve prosedürlerin uygulanıp uygulanmadığı kontrol edilmeli, bilgi sisteminin güvenilirlik ve tutarlığı sorgulanmalıdır. Ayrıca dönem içerisinde yaşanması muhtemel bilgi güvenliği ihlallerini ortaya çıkartabilecek risklerin önlenmesi amacıyla da çalışmalar yürütülmelidir. Kurumsallık seviyesi belli bir seviyeye ulaşmış kurumlarda bilgi güvenliği faaliyetleri "Bilgi Sistemleri ve Güvenliği Yönetimi Komitesi" tarafından koordine edilmektedir. Söz konusu komite tarafından gerçekleştirilebilecek faaliyetlerden bazıları aşağıda sunulmuştur (62,63):

- Bilgi güvenliği faaliyetlerinin bilgi güvenliği politikalarına uygun yürütülmesini sağlamak, uygunsuzlukların çözüm yöntemlerinin belirlenmesi.
- Bilgi güvenliği kontrollerinin etkinliğinin değerlendirilmesi ve kurum çapında uygulanmasının koordine edilmesi.
- Bilgi güvenliği ile ilgili risk değerlendirmesi, bilgi sınıflaması gibi yöntem ve süreçler komite tarafından onaylanmalı ve belirlenen sorumlular tarafından uygulanmalıdır.
- Tehditlerdeki önemli değişiklikler ile bilgi ve bilgi işlem tesislerinin maruz kaldığı tehditlerin belirlenmesi. Komitenin yönlendirmesi ile gerekli kontrol planlarının oluşturulması ve uygulanması.

- Güvenlik olaylarının izlenmesi ve gözden geçirilmesi sonucunda derlenen bilgiler Komite tarafından değerlendirilmeli ve uygun eylemler önerilmelidir.

- Kurum bünyesinde bilgi güvenliğini ihlal eden ya da ihlal edilmesine neden olanlar şirket içi ve ilgili yasal mevzuat çerçevesinde ilgili birime raporlanmalıdır.

2.12. ISO /IEC 27001 Standartı

Bilgi güvenliği yönetimini etkin hale getiren standarttır. TSE (Türk Standartları Enstitüsü) tarafından Türkçeye çevrilmiş olup; Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri–Gereksinimler tanımlanmıştır. ISO /IEC 27001 standardı teknik bir standart değildir. İşletme, kurum ve kuruluşların güvenlik gereksinimleri nelerdir tanımlar fakat bu konuda ki yaklaşımlarını kurumlara ve işletmelere bırakır. Bu standardın amacı; kurumlar da ve işletmelerde bilgi güvenliği sistemini etkin bir şekilde kurmak, uygulamak, sürdürmek, gözden geçirmek, kontrol etmek, denetlemek ve iyileştirmek için kılavuz olmaktır. ISO /IEC 27001 standartı kurumların bilgi güvenliği yönetiminde uymaları gereken kuralları gösterir. Tüm dünyada kabul edilen bu standart Bilgi güvenliğini sağlamak için bilginin gizlilik, bütünlük, erişebilirlik ilkelerinin yerine getirilmesini öngörür (64,65).

Risklerin bulunup tamamen ortadan kaldırılması veya etkisinin asgari düzeye indirilmesini sağlar. Sistem içinde, Sürekli İyileştirme (PUKÖ) Planla, Uygula, Kontrol Et, Önlem Al modelinin bilgi güvenliği yönetim sistemine uygulanmasını sağlar. Planla; Bilgi Güvenliği Yönetiminin sisteminin kurulması, Uygula; Bilgi güvenliği yönetim sisteminin işletilmesi ve uygulanması, Kontrol et; Bilgi güvenliği yönetim sisteminin işletimi sırasında izlenip, eksik yönlerinin tanımlanmasıdır. Önlem al; Bilgi Güvenliği yönetim sisteminin iyileştirilmesidir (64,65,66):

ISO /IEC 27001 Standartının kuruma yararları şunlardır;

- Kurumun bilgi güvenliği politikalarını yürütür.

- Kurumsal bilgiyi korur ve maddi ve itibar kayıplarını önler.

- Hukuka ve yasalara uygunluk nedeniyle kurumu hukuki cezalardan kurtarır.

- Çalışanların ve yöneticilerin bilgi güvenliği farkındalığını artırır.

- Bilgi güvenliği politikaları sayesinde sistemin kötüye kullanımını ve suiistimal edilmesini önler.

- Bilgi güvenliği ihlal olaylarında kişiyi ve kurumu iç ve dış tehditlerden korur.

2.13. Bilgi Güvenliği Farkındalık Eğitimleri

Sağlık kurumları son teknolojiden yararlanarak güvenlik önlemlerini alsalar da, insan kaynaklı bilgi güvenliği açıklarının hiçbir zaman önüne geçemezler, çünkü sağlık kurumlarının bilgi güvenliği konusunun en zayıf halkası insan faktörüdür. Bilgi güvenliği farkındalığı oluşturmaktaki amaç; kişilerin bilgi eksikliğinden kaynaklı hata ve risklerini en aza indirmek ve çalışanların bu tehditlerden haberdar olmasını sağlamaktır (67).

Güvenlik teknolojilerinden önce sağlık kurumlarının en üst çalışanından en alt çalışanına kadar bilgi güvenliği farkındalık faaliyetlerinin benimsenmesi, geliştirilmesi önem arz etmektedir (52).

Sağlık kurumları yasal mevzuata uymak, standartları yerine getirmek, riskleri tespit etmek ve yönetmek, sistemi gözden geçirmek sürekli iyileştirmek, bilgi güvenliği farkındalığı oluşturmak için gereken eğitimleri düzenlemekle yükümlüdür. Bilgi güvenliği farkındalığı oluşturmak, yönetim kadrosundan, tüm personele, firma çalışanlarından, hizmet alan gruplara, destek firmalarından, stajyerlere ve diğer kurumların sürece katılmasıyla mümkün olur (52).

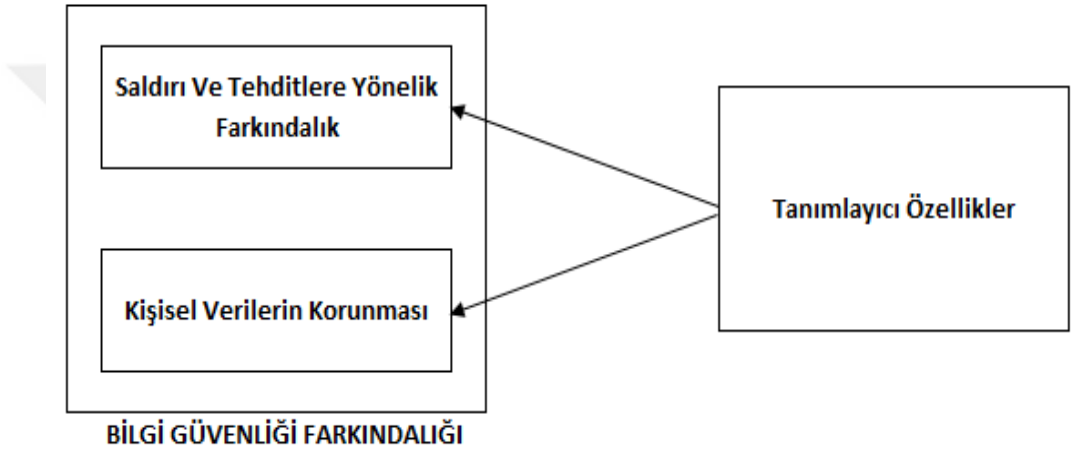
Bilgi güvenliği farkındalığı çalışmaları belirli zamanda başlayan ve biten bir süreç değildir. Kurumda bilgi güvenliği farkındalığı oluşturmak için; çalışanların, görev ve yetkileri dikkate alınarak, ihtiyaç ve beklentilerine uygun eğitimler düzenlenmeli ve belirli aralıklarla tekrar edilmelidir. Kuruma yeni başlayan personel için oryantasyon programına bilgi güvenliği eğitimi mutlaka dahil edilmelidir (67).

En etkili güvenlik önlemi, çalışanların bilgi güvenliği konusunda farkındalığından geçmektedir. En ufak ciddiyetsizlik ve sorumsuzluk kurumlar için maddi ve manevi, telafisi mümkün olmayan sorunlara yol açar (67).

3. GEREÇ ve YÖNTEM

3.1. Araştırmanın Modeli

Araştırma ilişkisel tarama modelinde tasarlanmıştır. İlişkisel tarama modelleri mevcut durumu değiştirme çabası olmayıp olduğu gibi ortaya koyan modellerdir. (68). Araştırmada kalite direktörlerinin bilgi güvenliği farkındalığı düzeylerini belirlemeye yönelik ve tanımlayıcı özelliklere göre farklılıklarını belirlemeye yönelik bir model belirlenmiştir.



Şekil 1. Araştırmanın Modeli

3.2. Evren ve Örneklem

Araştırmanın evrenini İstanbul ilinde faaliyet gösteren Kamu Hastaneler Birliğine bağlı 72 hastanenin kalite yönetim direktörleri ve kalite birim sorumluları oluşturmaktadır. Kamu Hastaneler Birliğine bağlı 6 genel sekreterliğe araştırma izni başvurusu yapılmış 67 hastane için çalışma onayı alınmıştır. Araştırma izni verilen; S.B.Ü İstanbul Dr. Siyami Ersek Göğüs Kalp ve Damar Cerrahisi Eğitim ve Araştırma Hastanesi, S.B.Ü İstanbul Ümraniye Eğitim ve Araştırma Hastanesi, İstanbul Medeniyet Üniversitesi Göztepe Eğitim ve Araştırma Hastanesi, S.B.Ü Sultan Abdülhamit Han Eğitim ve Araştırma Hastanesi, S.B.Ü Bakırköy Prof. Dr. Mazhar Osman Ruh Sağlığı ve Sinir Hastalıkları Eğitim ve Araştırma Hastanesi, S.B.Ü Bağcılar Eğitim ve Araştırma Hastanesi, S.B.Ü Bakırköy Dr. Sadi Konuk Eğitim ve Araştırma Hastanesi, S.B.Ü Süleymaniye Kadın Doğum ve Çocuk Hastalıkları Eğitim ve Araştırma Hastanesi, S.B.Ü Haseki Eğitim ve Araştırma Hastanesi, S.B.Ü Şişli Hamidiye Etfal Eğitim ve Araştırma

Hastanesi, S.B.Ü Okmeydanı Eğitim ve Araştırma Hastanesi, S.B.Ü Gaziosmanpaşa Taksim Eğitim ve Araştırma Hastanesi, İstanbul Sağlık Bakanlığı Marmara Üniversitesi Pendik Eğitim ve Araştırma Hastanesi, S.B.Ü Kartal Koşuyolu Yüksek İhtisas Eğitim ve Araştırma Hastanesi, S.B.Ü Kartal Dr. Lütfi Kırdar Eğitim ve Araştırma Hastanesi, S.B.Ü Zeynep Kamil Kadın ve Çocuk Hastalıkları Eğitim ve Araştırma Hastanesi, S.B.Ü Süreyyapaşa Göğüs Hastalıkları ve Göğüs Cerrahisi Eğitim ve Araştırma Hastanesi, S.B.Ü Kanuni Sultan Süleyman Eğitim ve Araştırma Hastanesi, S.B.Ü Mehmet Akif Ersoy Göğüs Kalp ve Damar Cerrahisi Eğitim ve Araştırma Hastanesi, S.B.Ü. İstanbul Yedikule Göğüs Hastalıkları ve Göğüs Cerrahisi Eğitim ve Araştırma Hastanelerinin kalite biriminde kalite yönetim direktörü ve kalite birim sorumlusu birlikte görev almaktadır. Kalan 47 hastanede ise kalite biriminde tek kalite yönetim direktörü bulunmaktadır. Belirtilen eğitim araştırma statüsündeki 20 hastanede kalite yönetim direktörü ve kalite birim sorumlusuna anket uygulayarak 40 katılımcıya ;diğer hastanelerde ise sadece kalite yönetim direktörlerine anket uygulanıp 47 katılımcıya ulaşılmıştır.Toplam 87 katılımcıdan veri toplanmış olup; örneklem seçilmemiş, evrende izin verilen hastanelerin tamamına ulaşılmıştır.

3.3. Araştırmanın Süresi ve Uygulama Şekli

Araştırma Kasım 2016-Ağustos 2017 tarihleri arasında 10 aylık bir sürede tamamlanması için etik kurul izni alınmış sonrasında Aralık 2016- Nisan 2017 tarihleri arasında 5 aylık bir sürede veri toplama süreci tamamlanmıştır. Hastanelerdeki 39 katılımcıya araştırmacı tarafından yüzyüze anket yöntemi uygulanmış, geri kalan 48 katılımcıya ise elektronik anket uygulaması yapılmıştır. Katılımcılar 4 gün içerisinde geri dönüş yapmıştır. Yüzyüze ve elektronik anket uygulamasıyla toplam 87 katılımcıya ulaşılmıştır.

3.4. Araştırmanın Hipotezleri

Hipotez 1:

H1: Kalite yönetim direktörleri ve kalite birim sorumlularının bilgi güvenliği farkındalığı ile demografik özellikleri(cinsiyet, meslek, yaş, eğitim düzeyi, çalışılan hastane türü, toplam iş tecrübesi, mevcut iş yerinde çalışma süresi, bilgisayar kullanma yılı, internet kullanma yılı) arasında ilişki vardır.

Hipotez 2:

H1: Kalite yönetim direktörleri ve kalite birim sorumlularının kişisel verilerin korunmasının sağlanması ile demografik özellikleri (cinsiyet, meslek, yaş, eğitim düzeyi, çalışılan hastane türü, toplam iş tecrübesi, mevcut iş yerinde çalışma süresi, bilgisayar kullanma yılı, internet kullanma yılı) arasında ilişki vardır.

Hipotez 3:

H1: Kalite yönetim direktörleri ve kalite birim sorumlularının saldırı ve tehditlere yönelik farkındalık düzeyleri ile demografik özellikleri (cinsiyet, meslek, yaş, eğitim düzeyi, çalışılan hastane türü, toplam iş tecrübesi, mevcut iş yerinde çalışma süresi, bilgisayar kullanma yılı, internet kullanma yılı) arasında ilişki vardır.

3.5. Veri Toplama Aracı

Araştırmada veriler kalite direktörlerinin tanımlayıcı özelliklerini belirlemeye yönelik form ve "Bilgi Güvenliği Farkındalık Ölçeği" ile toplanmıştır. Tanımlayıcı özellikler olarak direktörlerden bilgi güvenliği farkındalığı ile ilişkili olduğu düşünülen cinsiyet, yaş, eğitim düzeyi, görev, çalışılan hastane türü, toplam iş tecrübesi, mevcut iş yerinde çalışma süresi, kaç yıldır bilgisayar kullanıldığı, kaç yıldır internet kullanıldığına ilişkin yanıtlar toplanmaktadır.

Araştırmada Keser ve Güldüren (2015) tarafından geliştirilen bilgi güvenliği farkındalık ölçeği kullanılmıştır. Sorular 5'li Likert Tipi derecelendirme ölçeğine göre hazırlanmıştır. Derecelendirmeler 'Hiç Katılmıyorum (1)', 'Katılmıyorum (2)', 'Kararsızım (3)', 'Katılıyorum (4)', 'Tamamen Katılıyorum (5) arasında puan vermeleri istenmektedir (Ek 1).

Ölçek 34 madde olup; "saldırı ve tehditler" ile "kişisel verilerin korunması" olmak üzere 2 alt boyuttan oluşmaktadır. Ölçekte yer alan ilk 16 madde saldırı ve tehditlere yönelik farkındalıkları, 17 ile 34. maddeler arasında yer alanlar ise kişisel verilerin korunmasına yönelik farkındalıklarını belirlemeye yönelik sorulardır. Keser ve Güldüren ölçeğin genel olarak Cronbach alfa güvenirlik katsayısını 0.97; "saldırı ve tehditler" alt boyutu için 0.97; "kişisel verilerin korunması" alt boyutu için 0.94 olarak bulmuştur. Bu araştırmada ölçeğin genel güvenirliği Alpha=0.967 olarak; alt boyutların

güvenirlikleri ise 0.954 ile 0.950 olarak yüksek değerde bulunmuştur. Araştırmada Keser ve Güldüren'in orjinal faktör yapısı kullanılarak elde edilen bulgular yorumlanmaktadır (8).

3.6. Verilerin İstatistiksel Analizi

Araştırmada elde edilen veriler SPSS (Statistical Package for the Social Sciences) Windows 22.0 programı kullanılarak analiz edilmiştir. Verilerin değerlendirilmesinde tanımlayıcı istatistiksel yöntemleri olarak frekans, yüzde, ortalama, standart sapma kullanılmıştır.

Ölçek boyutlarının aldığı puanlar 1 ile 5 arasında değerlendirilmektedir. Dağılım aralığının hesaplanması amacıyla, Dağılım aralığı=En büyük değer- En küçük değer/ Derece sayısı formülü kullanılmıştır. Bu aralık 4 puanlık genişliğe sahiptir. Bu genişlik beş eşit genişliğe bölünerek 1.00-1.79 arası "çok düşük", 1.80-2.59 arası "düşük", 2.60-3.39 "arası orta", 3.40-4.19 arası yüksek, 4.20-5.00 arası çok yüksek olarak sınır değerleri belirlenmiş ve bulgular yorumlanmıştır (69).

İki bağımsız grup arasında niceliksel sürekli verilerin karşılaştırılmasında t-testi, ikiden fazla bağımsız grup arasında niceliksel sürekli verilerin karşılaştırılmasında Tek Yönlü (One way) Anova testi kullanılmıştır. Anova testi sonrasında farklılıkları belirlemek üzere tamamlayıcı post-hoc analizi olarak Scheffe testi kullanılmıştır.

Elde edilen bulgular %95 güven aralığında, %5 anlamlılık düzeyinde değerlendirilmiştir.

3.7. Araştırmanın Sınırlılıkları

Araştırma İstanbul ili Kamu hastaneler birliğine bağlı kurumlardaki kalite yönetim direktörleri ve kalite birim sorumlularına yapılmıştır. Çalışmanın sadece İstanbul ilinde yapılması ankete sadece kalite yönetim direktörleri, kalite birim sorumlularının dahil edilmesi araştırmayı sınırlamıştır.

Gelecekte yapılacak olan çalışmalarda daha fazla kurumda yapılması, tüm kalite yönetim biriminde çalışan kişilerin ve tüm çalışanların dahil edilerek yapılması çalışma açısından daha verimli olacağı düşünülmektedir.

4. BULGULAR

4.1. Tanımlayıcı Özelliklerin Dağılımı

Tablo 1. Tanımlayıcı Özelliklerin Dağılımı

Tablolar	Gruplar	Frekans (n)	Yüzde (%)
Cinsiyet	Erkek	11	12,6
	Kadın	76	87,4
	Toplam	87	100,0
Yaş	20-30 yaş arası	13	14,9
	31-40 yaş arası	49	56,3
	41-50 yaş arası	25	28,7
	Toplam	87	100,0
Eğitim Düzeyi	Ön Lisans	16	18,4
	Lisans	30	34,5
	Lisansüstü	41	47,1
	Toplam	87	100,0
Görev	Hekim	5	5,7
	Hemşire	61	70,1
	Ebe	10	11,5
	Teknisyen	11	12,6
	Toplam	87	100,0
Çalışılan Hastane Türü	Eğitim Araştırma Hastanesi	40	46
	Hizmet Hastanesi	25	28,7
	Dal Hastanesi	22	25.3
	Toplam	87	100,0
Toplam İş Tecrübesi	1-5 yıl arasında	7	8,0
	6-10 yıl arasında	26	29,9
	10 yıl üzeri	54	62,1
	Toplam	87	100,0
Mevcut İş Yerinde Çalışma Süresi	5 yıl ve altı	29	33,3
	6-10 yıl arasında	28	32,2
	10 yıl üzeri	30	34,5
	Toplam	87	100,0
Kaç Yıldır Bilgisayar Kullanıldığı	10 yıl ve altı	14	16,1
	11-15 yıl	36	41,4
	16-20 yıl	19	21,8
	20 yıl üzeri	18	20,7
	Toplam	87	100,0
Kaç Yıldır İnternet Kullanıldığı	10yıl ve altı	28	32,2
	11-15yıl	37	42,5
	15yıl üzeri	22	25,3
	Toplam	87	100,0

Direktörler cinsiyet değişkenine göre 11'i (%12,6) erkek, 76'sı (%87,4) kadın olarak dağılmaktadır.

Direktörler yaş değişkenine göre 13'ü (%14,9) 20-30 yaş arası, 49'u (%56,3) 31-40 yaş arası, 25'i (%28,7) 41-50 yaş arası olarak dağılmaktadır.

Direktörler eğitim düzeyi değişkenine göre 16'sı (%18,4) ön lisans, 30'u (%34,5) lisans, 41'i (%47,1) lisansüstü olarak dağılmaktadır.

Direktörler görev değişkenine göre 5'i (%5,7) hekim, 61'i (%70,1) hemşire, 10'u (%11,5) ebe, 11'i (%12,6) teknisyen olarak dağılmaktadır.

Direktörler çalışılan hastane türü değişkenine göre 40'ı (%46) eğitim araştırma hastanesi, 25'i (%28,7) hizmet hastanesi, 22'si (%25.3) dal hastanesi olarak dağılmaktadır.

Direktörler toplam iş tecrübesi değişkenine göre 7'si (%8,0) 1-5 yıl arasında, 26'sı (%29,9) 6-10 yıl arasında, 54'ü (%62,1) 10 yıldan fazla olarak dağılmaktadır.

Direktörler mevcut iş yerinde çalışma süresi değişkenine göre 29'u (%33,3) 5 yıl ve altı, 28'i (%32,2) 6-10 yıl arasında, 30'u (%34,5) 10 yıldan fazla olarak dağılmaktadır.

Direktörler kaç yıldır bilgisayar kullanıldığı değişkenine göre 14'ü (%16,1) 10 yıl ve altı, 36'sı (%41,4) 11-15 yıl, 19'u (%21,8) 16-20 yıl, 18'i (%20,7) 20 üzeri olarak dağılmaktadır.

Direktörler kaç yıldır internet kullanıldığı değişkenine göre 28'i (%32,2) 10 yıl ve altı, 37'si (%42,5) 11-15 yıl, 22'si (%25,3) 15 yıl üzeri olarak dağılmaktadır (Tablo 1).

4.2. Bilgi Güvenliği Farkındalığına İlişkin Betimleyici Bulgular

Araştırmaya katılan direktörlerin bilgi güvenliği farkındalığı ile ilgili ifadelere verdiği cevapların dağılımları aşağıda görülmektedir.

Tablo 2. Direktörlerin Bilgi Güvenliği Farkındalığı İle İlgili İfadelere Verdiği Cevapların Dağılımları

	Hiç Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Tamamen Katılıyorum			
	f	%	f	%	f	%	f	%	f	%	Ort	Ss
Kişisel Mahremiyet Nedir Biliyorum	1	1,1	2	2,3	6	6,9	46	52,9	32	36,8	4,218	0,769
Şüpheli Veya Bilinmeyen Kaynaklardan Gelen Özellikle Eklentisi Olan E-postaları Açmanın Taşıdığı Riski Biliyorum	2	2,3	4	4,6	4	4,6	43	49,4	34	39,1	4,184	0,896
İstenmeyen Elektronik Posta (Spam) Nedir Biliyorum	2	2,3	4	4,6	7	8,0	42	48,3	32	36,8	4,126	0,913
Bilgi Güvenliği İle İlgili Sorumluluklarımın Ne Olduğunu Biliyorum	1	1,1	5	5,7	7	8,0	50	57,5	24	27,6	4,046	0,834
Bilgi Güvenliğinin Ne Anlama Geldiğini Biliyorum	3	3,4	3	3,4	8	9,2	48	55,2	25	28,7	4,023	0,915
Kullandığım Bilgi Sistemlerinde Tanımlanmış Olan Kuralları Nasıl Uygulayacağımı Biliyorum	1	1,1	3	3,4	10	11,5	56	64,4	17	19,5	3,977	0,747
Usb Sürücülerini (usb Drives) Kullanırken Dikkat Edilmesi Gereken Hususları Biliyorum	3	3,4	5	5,7	10	11,5	50	57,5	19	21,8	3,885	0,933
Dijital İmza (Digital Signature) Nedir Biliyorum	6	6,9	2	2,3	9	10,3	49	56,3	21	24,1	3,885	1,028
Taşınabilir Cihazlara Yönelik Veri Güvenliği İle İlgili Dikkat Edilmesi Gereken Konuları Biliyorum	1	1,1	9	10,3	12	13,8	47	54,0	18	20,7	3,828	0,918
E-posta Gönderirken "gizli" (bcc) Alanının Sağladığı Avantajları Biliyorum	6	6,9	6	6,9	11	12,6	41	47,1	23	26,4	3,793	1,122
Taşınabilir Cihazlara (Portable Devices) Yönelik Fiziksel Güvenliği Sağlamak İle İlgili Dikkat Edilmesi Gereken Konuları Biliyorum	1	1,1	7	8,0	19	21,8	42	48,3	18	20,7	3,793	0,904
Çevrimiçi Güvenli Alışveriş Yapmak İçin Gerekli Olan Güvenlik Tedbirlerini Biliyorum	4	4,6	7	8,0	15	17,2	38	43,7	23	26,4	3,793	1,069
İstenmeyen Elektronik Posta Miktarını Azaltmak İçin Gerekli Bilgiye Sahibim	4	4,6	6	6,9	18	20,7	36	41,4	23	26,4	3,782	1,061
Bilgisayarımdaki Virüs Koruma Yazılımının Otomatik Güncelleştirme Yapmasını Sağlayabilirim	6	6,9	6	6,9	10	11,5	44	50,6	21	24,1	3,782	1,104
Sosyal Ağ Sitelerini (Social Networking Sites) Güvenli Olarak Nasıl Kullanacağımı Biliyorum	5	5,7	6	6,9	16	18,4	39	44,8	21	24,1	3,747	1,081
Bilgi Sistemlerinde Kullanılan Virüs Koruma Yazılımını Nasıl Kullanacağımı Biliyorum	4	4,6	9	10,3	14	16,1	41	47,1	19	21,8	3,713	1,066
Mavidiş (Bluetooth) Teknolojisi İle Veri Aktarımı Konusunda Bilgi Sahibiyim	9	10,3	7	8,0	12	13,8	40	46,0	19	21,8	3,609	1,214
Bilgisayarımdaki Virüs Koruma Yazılımının Gerçek Zamanlı Koruma (Realtime Protection) Özelliğini Kullanmaktayım	6	6,9	13	14,9	12	13,8	38	43,7	18	20,7	3,563	1,178
Kötü Niyetli Yazılımlara (Malware) Karşı Alınması Gereken Güvenlik Tedbirlerini Biliyorum	4	4,6	15	17,2	22	25,3	34	39,1	12	13,8	3,402	1,072
Bilgisayarıma Kötü Niyetli Kod (Malicious Code) Bulaşıp Bulaşmadığını Anlayabilirim	7	8,0	15	17,2	22	25,3	35	40,2	8	9,2	3,253	1,102
Kimlik Hırsızlığı (İdentity Theft) Nedir Biliyorum	8	9,2	19	21,8	17	19,5	35	40,2	8	9,2	3,184	1,157
Zincir E-postalara (Chain E-mail) Karşı Nasıl Hareket Etmem Gerektiğini Biliyorum	10	11,5	23	26,4	20	23,0	26	29,9	8	9,2	2,989	1,186
Sahte Virüs Koruma Yazılımının Ne Olduğunu Biliyorum	8	9,2	30	34,5	16	18,4	27	31,0	6	6,9	2,920	1,143
Siber Zorbalığa Karşı Çocuklarımı Nasıl Koruyacağımı Biliyorum	9	10,3	30	34,5	23	26,4	15	17,2	10	11,5	2,851	1,177
Aldatmaca (Hoax) Nedir Biliyorum	12	13,8	27	31,0	20	23,0	19	21,8	9	10,3	2,839	1,219
Kimlik Hırsızlığına Karşı Alınması Gereken Güvenlik Tedbirlerini Biliyorum	11	12,6	29	33,3	16	18,4	25	28,7	6	6,9	2,839	1,180
Bilgisayarıma Casus Yazılım Yüklenmesini Engelleme Yöntemlerini Biliyorum	12	13,8	29	33,3	17	19,5	23	26,4	6	6,9	2,793	1,183
Sosyal Mühendislik (Social Engineering) Saldırısı Nedir Biliyorum	11	12,6	35	40,2	13	14,9	21	24,1	7	8,0	2,747	1,193
Siber Zorbalık (Cyberbullying) Nedir Biliyorum	13	14,9	35	40,2	14	16,1	17	19,5	8	9,2	2,678	1,215
Kimlik Avı (Phishing) Saldırısı Nedir Biliyorum	13	14,9	31	35,6	20	23,0	21	24,1	2	2,3	2,632	1,080
Siber Zorbalığa Karşı Kendimi Nasıl Koruyacağımı Biliyorum	11	12,6	34	39,1	24	27,6	13	14,9	5	5,7	2,621	1,070
Bilgisayarımda Casus Yazılım (Spyware) Olup Olmadığını Anlayabilirim	16	18,4	28	32,2	21	24,1	17	19,5	5	5,7	2,621	1,164

	Hiç Katılmıyorum		Katılmıyorum		Kararsızım		Katılıyorum		Tamamen Katılıyorum			
	f	%	f	%	f	%	f	%	f	%	Ort	Ss
Hizmet Aksatma (Denial Of Service - Dos) Saldırısı Nedir Biliyorum	9	10,3	41	47,1	19	21,8	14	16,1	4	4,6	2,575	1,030
Sosyal Mühendislik Saldırısına Uğramamak İçin Nasıl Hareket Etmem Gerektiğini Biliyorum	13	14,9	42	48,3	12	13,8	14	16,1	6	6,9	2,517	1,140

Araştırmaya katılan direktörlerin bilgi güvenliği farkındalığı ile ilgili ifadelere verdiği cevaplar incelendiğinde;

"*Kişisel Mahremiyet Nedir Biliyorum*" ifadesine direktörlerin, %1,1'i (n=1) hiç katılmıyorum, %2,3'ü (n=2) katılmıyorum, %6,9'u (n=6) kararsızım, %52,9'u (n=46) katılıyorum, %36,8'i (n=32) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "kişisel mahremiyet nedir biliyorum" ifadesine çok yüksek (4,218±0,769) düzeyde katıldıkları saptanmıştır.

"*Şüpheli Veya Bilinmeyen Kaynaklardan Gelen Özellikle Eklentisi Olan E-postaları Açmanın Taşıdığı Riski Biliyorum*" ifadesine direktörlerin, %2,3'ü (n=2) hiç katılmıyorum, %4,6'sı (n=4) katılmıyorum, %4,6'sı (n=4) kararsızım, %49,4'ü (n=43) katılıyorum, %39,1'i (n=34) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum" ifadesine yüksek (4,184±0,896) düzeyde katıldıkları saptanmıştır.

"*İstenmeyen Elektronik Posta (spam) Nedir Biliyorum*" ifadesine direktörlerin, %2,3'ü (n=2) hiç katılmıyorum, %4,6'sı (n=4) katılmıyorum, %8,0'ı (n=7) kararsızım, %48,3'ü (n=42) katılıyorum, %36,8'i (n=32) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "istenmeyen elektronik posta (spam) nedir biliyorum" ifadesine yüksek (4,126±0,913) düzeyde katıldıkları saptanmıştır.

"*Bilgi Güvenliği İle İlgili Sorumluluklarımın Ne Olduğunu Biliyorum*" ifadesine direktörlerin, %1,1'i (n=1) hiç katılmıyorum, %5,7'si (n=5) katılmıyorum, %8,0'ı (n=7) kararsızım, %57,5'i (n=50) katılıyorum, %27,6'sı (n=24) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "bilgi güvenliği ile ilgili sorumluluklarımın ne olduğunu biliyorum" ifadesine yüksek (4,046±0,834) düzeyde katıldıkları saptanmıştır.

"*Bilgi Güvenliğinin Ne Anlama Geldiğini Biliyorum*" ifadesine direktörlerin, %3,4'ü (n=3) hiç katılmıyorum, %3,4'ü (n=3) katılmıyorum, %9,2'si (n=8) kararsızım, %55,2'si (n=48) katılıyorum, %28,7'si (n=25) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "bilgi güvenliğinin ne anlama geldiğini biliyorum" ifadesine yüksek (4,023±0,915) düzeyde katıldıkları saptanmıştır.

"*Kullandığım Bilgi Sistemlerinde Tanımlanmış Olan Kuralları Nasıl Uygulayacağımı Biliyorum*" ifadesine direktörlerin, %1,1'i (n=1) hiç katılmıyorum, %3,4'ü (n=3) katılmıyorum, %11,5'i (n=10) kararsızım, %64,4'ü (n=56) katılıyorum, %19,5'i (n=17) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum" ifadesine yüksek (3,977±0,747) düzeyde katıldıkları saptanmıştır.

"*Usb Sürücülerini (Usb Drives) Kullanırken Dikkat Edilmesi Gereken Hususları Biliyorum*" ifadesine direktörlerin, %3,4'ü (n=3) hiç katılmıyorum, %5,7'si (n=5) katılmıyorum, %11,5'i (n=10) kararsızım, %57,5'i (n=50) katılıyorum, %21,8'i (n=19) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "usb sürücülerini (usb drives) kullanırken dikkat edilmesi gereken hususları biliyorum" ifadesine yüksek (3,885±0,933) düzeyde katıldıkları saptanmıştır.

"*Dijital İmza (Digital Signature) Nedir Biliyorum*" ifadesine direktörlerin, %6,9'u (n=6) hiç katılmıyorum, %2,3'ü (n=2) katılmıyorum, %10,3'ü (n=9) kararsızım, %56,3'ü (n=49) katılıyorum, %24,1'i (n=21) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "dijital imza (Sigital signature) nedir biliyorum" ifadesine yüksek (3,885±1,028) düzeyde katıldıkları saptanmıştır.

"*Taşınabilir Cihazlara Yönelik Veri Güvenliği İle İlgili Dikkat Edilmesi Gereken Konuları Biliyorum*" ifadesine direktörlerin, %1,1'i (n=1) hiç katılmıyorum, %10,3'ü (n=9) katılmıyorum, %13,8'i (n=12) kararsızım, %54,0'ı (n=47) katılıyorum, %20,7'si (n=18) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum" ifadesine yüksek (3,828±0,918) düzeyde katıldıkları saptanmıştır.

"*E-posta Gönderirken "gizli" (Bcc) Alanının Sağladığı Avantajları Biliyorum*" ifadesine direktörlerin, %6,9'u (n=6) hiç katılmıyorum, %6,9'u (n=6) katılmıyorum, %12,6'sı (n=11) kararsızım, %47,1'i (n=41) katılıyorum, %26,4'ü (n=23) tamamen

katılıyorum yanıtını vermiştir. Direktörlerin “e-posta gönderirken "gizli" (bcc) alanının sağladığı avantajları biliyorum” ifadesine yüksek (3,793±1,122) düzeyde katıldıkları saptanmıştır.

“*Taşınabilir Cihazlara (portable Devices) Yönelik Fiziksel Güvenliği Sağlamak İle İlgili Dikkat Edilmesi Gereken Konuları Biliyorum*” ifadesine direktörlerin, %1,1'i (n=1) hiç katılmıyorum, %8,0'ı (n=7) katılmıyorum, %21,8'i (n=19) kararsızım, %48,3'ü (n=42) katılıyorum, %20,7'si (n=18) tamamen katılıyorum yanıtını vermiştir. Direktörlerin “taşınabilir cihazlara (portable devices) yönelik fiziksel güvenliği sağlamak ile ilgili dikkat edilmesi gereken konuları biliyorum” ifadesine yüksek (3,793±0,904) düzeyde katıldıkları saptanmıştır.

“*Çevrimiçi Güvenli Alışveriş Yapmak İçin Gerekli Olan Güvenlik Tedbirlerini Biliyorum*” ifadesine direktörlerin, %4,6'sı (n=4) hiç katılmıyorum, %8,0'ı (n=7) katılmıyorum, %17,2'si (n=15) kararsızım, %43,7'si (n=38) katılıyorum, %26,4'ü (n=23) tamamen katılıyorum yanıtını vermiştir. Direktörlerin “çevrimiçi güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini biliyorum” ifadesine yüksek (3,793±1,069) düzeyde katıldıkları saptanmıştır.

“*İstenmeyen Elektronik Posta Miktarını Azaltmak İçin Gerekli Bilgiye Sahibim*” ifadesine direktörlerin, %4,6'sı (n=4) hiç katılmıyorum, %6,9'u (n=6) katılmıyorum, %20,7'si (n=18) kararsızım, %41,4'ü (n=36) katılıyorum, %26,4'ü (n=23) tamamen katılıyorum yanıtını vermiştir. Direktörlerin “istenmeyen elektronik posta miktarını azaltmak için gerekli bilgiye sahibim” ifadesine yüksek (3,782±1,061) düzeyde katıldıkları saptanmıştır.

“*Bilgisayarımdaki Virüs Koruma Yazılımının Otomatik Güncelleştirme Yapmasını Sağlayabilirim*” ifadesine direktörlerin, %6,9'u (n=6) hiç katılmıyorum, %6,9'u (n=6) katılmıyorum, %11,5'i (n=10) kararsızım, %50,6'sı (n=44) katılıyorum, %24,1'i (n=21) tamamen katılıyorum yanıtını vermiştir. Direktörlerin “bilgisayarımdaki virüs koruma yazılımının otomatik güncelleştirme yapmasını sağlayabilirim” ifadesine yüksek (3,782±1,104) düzeyde katıldıkları saptanmıştır.

“*Sosyal Ağ Sitelerini (Social Networking Sites) Güvenli Olarak Nasıl Kullanacağımı Biliyorum*” ifadesine direktörlerin, %5,7'si (n=5) hiç katılmıyorum, %6,9'u (n=6) katılmıyorum, %18,4'ü (n=16) kararsızım, %44,8'i (n=39) katılıyorum,

%24,1'i (n=21) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "sosyal ağ sitelerini (social networking sites) güvenli olarak nasıl kullanacağımı biliyorum" ifadesine yüksek (3,747±1,081) düzeyde katıldıkları saptanmıştır.

"*Bilgi Sistemlerinde Kullanılan Virüs Koruma Yazılımını Nasıl Kullanacağımı Biliyorum*" ifadesine direktörlerin, %4,6'sı (n=4) hiç katılmıyorum, %10,3'ü (n=9) katılmıyorum, %16,1'i (n=14) kararsızım, %47,1'i (n=41) katılıyorum, %21,8'i (n=19) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "bilgi sistemlerinde kullanılan virüs koruma yazılımını nasıl kullanacağımı biliyorum" ifadesine yüksek (3,713±1,066) düzeyde katıldıkları saptanmıştır.

"*Mavidiş (Bluetooth) Teknolojisi İle Veri Aktarımı Konusunda Bilgi Sahibiyim*" ifadesine direktörlerin, %10,3'ü (n=9) hiç katılmıyorum, %8,0'ı (n=7) katılmıyorum, %13,8'i (n=12) kararsızım, %46,0'ı (n=40) katılıyorum, %21,8'i (n=19) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "mavidiş (bluetooth) teknolojisi ile veri aktarımı konusunda bilgi sahibiyim" ifadesine yüksek (3,609±1,214) düzeyde katıldıkları saptanmıştır.

"*Bilgisayarımdaki Virüs Koruma Yazılımının Gerçek Zamanlı Koruma (Realtime Protection) Özelliğini Kullanmaktayım*" ifadesine direktörlerin, %6,9'u (n=6) hiç katılmıyorum, %14,9'u (n=13) katılmıyorum, %13,8'i (n=12) kararsızım, %43,7'si (n=38) katılıyorum, %20,7'si (n=18) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "bilgisayarımdaki virüs koruma yazılımının gerçek zamanlı koruma (realtime protection) özelliğini kullanmaktayım" ifadesine yüksek (3,563±1,178) düzeyde katıldıkları saptanmıştır.

"*Kötü Niyetli Yazılımlara (Malware) Karşı Alınması Gereken Güvenlik Tedbirlerini Biliyorum*" ifadesine direktörlerin, %4,6'sı (n=4) hiç katılmıyorum, %17,2'si (n=15) katılmıyorum, %25,3'ü (n=22) kararsızım, %39,1'i (n=34) katılıyorum, %13,8'i (n=12) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "kötü niyetli yazılımlara (malware) karşı alınması gereken güvenlik tedbirlerini biliyorum" ifadesine yüksek (3,402±1,072) düzeyde katıldıkları saptanmıştır.

"*Bilgisayarıma Kötü Niyetli Kod (Malicious Code) Bulaşıp Bulaşmadığını Anlayabilirim*" ifadesine direktörlerin, %8,0'ı (n=7) hiç katılmıyorum, %17,2'si (n=15) katılmıyorum, %25,3'ü (n=22) kararsızım, %40,2'si (n=35) katılıyorum, %9,2'si (n=8)

tamamen katılıyorum yanıtını vermiştir. Direktörlerin "bilgisayarıma kötü niyetli kod (malicious code) bulaşıp bulaşmadığını anlayabilirim" ifadesine orta (3,253±1,102) düzeyde katıldıkları saptanmıştır.

"*Kimlik Hırsızlığı (İdentity Theft) Nedir Biliyorum*" ifadesine direktörlerin, %9,2'si (n=8) hiç katılmıyorum, %21,8'i (n=19) katılmıyorum, %19,5'i (n=17) kararsızım, %40,2'si (n=35) katılıyorum, %9,2'si (n=8) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "kimlik hırsızlığı (identity theft) nedir biliyorum" ifadesine orta (3,184±1,157) düzeyde katıldıkları saptanmıştır.

"*Zincir E-postalara (Chain E-mail) Karşı Nasıl Hareket Etmem Gerektiğini Biliyorum*" ifadesine direktörlerin, %11,5'i (n=10) hiç katılmıyorum, %26,4'ü (n=23) katılmıyorum, %23,0'ı (n=20) kararsızım, %29,9'u (n=26) katılıyorum, %9,2'si (n=8) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "zincir e-postalara (chain e-mail) karşı nasıl hareket etmem gerektiğini biliyorum" ifadesine orta (2,989±1,186) düzeyde katıldıkları saptanmıştır.

"*Sahte Virüs Koruma Yazılımının Ne Olduğunu Biliyorum*" ifadesine direktörlerin, %9,2'si (n=8) hiç katılmıyorum, %34,5'i (n=30) katılmıyorum, %18,4'ü (n=16) kararsızım, %31,0'ı (n=27) katılıyorum, %6,9'u (n=6) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "sahte virüs koruma yazılımının ne olduğunu biliyorum" ifadesine orta (2,920±1,143) düzeyde katıldıkları saptanmıştır.

"*Siber Zorbalığa Karşı Çocuklarımı Nasıl Koruyacağımı Biliyorum*" ifadesine direktörlerin, %10,3'ü (n=9) hiç katılmıyorum, %34,5'i (n=30) katılmıyorum, %26,4'ü (n=23) kararsızım, %17,2'si (n=15) katılıyorum, %11,5'i (n=10) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "siber zorbalığa karşı çocuklarımı nasıl koruyacağımı biliyorum" ifadesine orta (2,851±1,177) düzeyde katıldıkları saptanmıştır.

"*Aldatmaca (Hoax) Nedir Biliyorum*" ifadesine direktörlerin, %13,8'i (n=12) hiç katılmıyorum, %31,0'ı (n=27) katılmıyorum, %23,0'ı (n=20) kararsızım, %21,8'i (n=19) katılıyorum, %10,3'ü (n=9) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "aldatmaca (hoax) nedir biliyorum" ifadesine orta (2,839±1,219) düzeyde katıldıkları saptanmıştır.

"*Kimlik Hırsızlığına Karşı Alınması Gereken Güvenlik Tedbirlerini Biliyorum*" ifadesine direktörlerin, %12,6'sı (n=11) hiç katılmıyorum, %33,3'ü (n=29) katılmıyorum, %18,4'ü (n=16) kararsızım, %28,7'si (n=25) katılıyorum, %6,9'u (n=6) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum" ifadesine orta (2,839±1,180) düzeyde katıldıkları saptanmıştır.

"*Bilgisayarıma Casus Yazılım Yüklenmesini Engelleme Yöntemlerini Biliyorum*" ifadesine direktörlerin, %13,8'i (n=12) hiç katılmıyorum, %33,3'ü (n=29) katılmıyorum, %19,5'i (n=17) kararsızım, %26,4'ü (n=23) katılıyorum, %6,9'u (n=6) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "bilgisayarıma casus yazılım yüklenmesini engelleme yöntemlerini biliyorum" ifadesine orta (2,793±1,183) düzeyde katıldıkları saptanmıştır.

"*Sosyal Mühendislik (Social Engineering) Saldırısı Nedir Biliyorum*" ifadesine direktörlerin, %12,6'sı (n=11) hiç katılmıyorum, %40,2'si (n=35) katılmıyorum, %14,9'u (n=13) kararsızım, %24,1'i (n=21) katılıyorum, %8,0'ı (n=7) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "sosyal mühendislik (social engineering) saldırısı nedir biliyorum" ifadesine orta (2,747±1,193) düzeyde katıldıkları saptanmıştır.

"*Siber Zorbalık (Cyberbullying) Nedir Biliyorum*" ifadesine direktörlerin, %14,9'u (n=13) hiç katılmıyorum, %40,2'si (n=35) katılmıyorum, %16,1'i (n=14) kararsızım, %19,5'i (n=17) katılıyorum, %9,2'si (n=8) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "siber zorbalık (cyberbullying) nedir biliyorum" ifadesine orta (2,678±1,215) düzeyde katıldıkları saptanmıştır.

"*Kimlik Avı (Phishing) Saldırısı Nedir Biliyorum*" ifadesine direktörlerin, %14,9'u (n=13) hiç katılmıyorum, %35,6'sı (n=31) katılmıyorum, %23,0'ı (n=20) kararsızım, %24,1'i (n=21) katılıyorum, %2,3'ü (n=2) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "kimlik avı (phishing) saldırısı nedir biliyorum" ifadesine orta (2,632±1,080) düzeyde katıldıkları saptanmıştır.

"*Siber Zorbalığa Karşı Kendimi Nasıl Koruyacağımı Biliyorum*" ifadesine direktörlerin, %12,6'sı (n=11) hiç katılmıyorum, %39,1'i (n=34) katılmıyorum, %27,6'sı (n=24) kararsızım, %14,9'u (n=13) katılıyorum, %5,7'si (n=5) tamamen katılıyorum

yanıtını vermiştir. Direktörlerin "siber zorbalığa karşı kendimi nasıl koruyacağımı biliyorum" ifadesine orta (2,621±1,070) düzeyde katıldıkları saptanmıştır.

"*Bilgisayarımda Casus Yazılım (Spyware) Olup Olmadığını Anlayabilirim*" ifadesine direktörlerin, %18,4'ü (n=16) hiç katılmıyorum, %32,2'si (n=28) katılmıyorum, %24,1'i (n=21) kararsızım, %19,5'i (n=17) katılıyorum, %5,7'si (n=5) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "bilgisayarımda casus yazılım (spyware) olup olmadığını anlayabilirim" ifadesine orta (2,621±1,164) düzeyde katıldıkları saptanmıştır.

"*Hizmet Aksatma (Denial Of Service - Dos) Saldırısı Nedir Biliyorum*" ifadesine direktörlerin, %10,3'ü (n=9) hiç katılmıyorum, %47,1'i (n=41) katılmıyorum, %21,8'i (n=19) kararsızım, %16,1'i (n=14) katılıyorum, %4,6'sı (n=4) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "hizmet aksatrma (denial of service - dos) saldırısı nedir biliyorum" ifadesine zayıf (2,575±1,030) düzeyde katıldıkları saptanmıştır.

"*Sosyal Mühendislik Saldırısına Uğramamak İçin Nasıl Hareket Etmem Gerektiğini Biliyorum*" ifadesine direktörlerin, %14,9'u (n=13) hiç katılmıyorum, %48,3'ü (n=42) katılmıyorum, %13,8'i (n=12) kararsızım, %16,1'i (n=14) katılıyorum, %6,9'u (n=6) tamamen katılıyorum yanıtını vermiştir. Direktörlerin "sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum" ifadesine zayıf (2,517±1,140) düzeyde katıldıkları saptanmıştır (Tablo 2).

Tablo 3. Bilgi Güvenliği Farkındalığı Puan Ortalamaları

	N	Ort	Ss	Min.	Max.
Kişisel Verilerin Korunması	87	3,875	0,744	1,830	5,000
Saldırı ve Tehditlere Yönelik Farkındalık	87	2,841	0,866	1,190	4,560
Bilgi Güvenliği Farkındalığı Genel	87	3,388	0,739	1,590	4,790

Araştırmaya katılan direktörlerin "Kişisel Verilerin Korunması" düzeyi yüksek (3,875±0,744); saldırı ve tehditlere yönelik farkındalık"" düzeyi orta (2,841±0,866); "bilgi güvenliği farkındalığı genel" düzeyi orta (3,388±0,739); olarak saptanmıştır (Tablo 3).

4.3. Bilgi Güvenliği Farkındalığının Tanımlayıcı Özelliklere Göre Karşılaştırması

Tablo 4. Bilgi Güvenliği Farkındalığının Cinsiyete Göre Ortalamaları

	Grup	N	Ort	Ss	t	p
Kişisel Verilerin Korunması	Erkek	11	4,242	0,658	1,774	0,080
	Kadın	76	3,822	0,745		
Saldırı ve Tehditlere Yönelik Farkındalık	Erkek	11	3,659	0,890	3,574	0,001
	Kadın	76	2,723	0,801		
Bilgi Güvenliği Farkındalığı Genel	Erkek	11	3,968	0,740	2,902	0,005
	Kadın	76	3,305	0,704		

Araştırmaya katılan direktörlerin saldırı ve tehditlere yönelik farkındalık puanları ortalamalarının cinsiyet değişkenine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla yapılan t-testi sonucunda grup ortalamaları arasındaki fark istatistiksel açıdan anlamlı bulunmuştur ($t(85)=3.574$; $p=0.001<0,05$). Erkeklerin saldırı ve tehditlere yönelik farkındalık puanları ($\bar{x}=3,659$), kadınların saldırı ve tehditlere yönelik farkındalık puanlarından ($\bar{x}=2,723$) yüksek bulunmuştur.

Araştırmaya katılan direktörlerin bilgi güvenliği farkındalığı genel puanları ortalamalarının cinsiyet değişkenine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla yapılan t-testi sonucunda grup ortalamaları arasındaki fark istatistiksel açıdan anlamlı bulunmuştur ($t(85)=2.902$; $p=0.005<0,05$). Erkeklerin bilgi güvenliği farkındalığı genel puanları ($\bar{x}=3,968$), kadınların bilgi güvenliği farkındalığı genel puanlarından ($\bar{x}=3,305$) yüksek bulunmuştur.

Araştırmaya katılan direktörlerin kişisel verilerin korunması puanları ortalamalarının cinsiyet değişkenine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla yapılan t-testi sonucunda grup ortalamaları arasındaki fark istatistiksel açıdan anlamlı bulunmamıştır ($p>0,05$).

Araştırmaya göre erkek katılımcıların bilgi güvenliği farkındalıkları ve saldırı ve tehditlere yönelik farkındalık kadın katılımcılardan yüksek olduğu görülmüştür (Tablo 4).

Tablo 5. Bilgi Güvenliği Farkındalığının Yaşa Göre Ortalamaları

	Grup	N	Ort	Ss	F	p
Kişisel Verilerin Korunması	20-30 Yaş Arası	13	3,855	0,737	0,696	0,502
	31-40 Yaş Arası	49	3,951	0,790		
	41-50 Yaş Arası	25	3,736	0,657		
Saldırı ve Tehditlere Yönelik Farkındalık	20-30 Yaş Arası	13	2,779	0,732	0,598	0,552
	31-40 Yaş Arası	49	2,929	0,882		
	41-50 Yaş Arası	25	2,703	0,909		
Bilgi Güvenliği Farkındalığı Genel	20-30 Yaş Arası	13	3,348	0,616	0,756	0,473
	31-40 Yaş Arası	49	3,470	0,777		
	41-50 Yaş Arası	25	3,249	0,723		

Araştırmaya katılan direktörlerin saldırı ve tehditlere yönelik farkındalık, kişisel verilerin korunması, bilgi güvenliği farkındalığı genel puanları ortalamalarının yaş değişkenine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla yapılan tek yönlü varyans analizi (Anova) sonucunda grup ortalamaları arasındaki fark istatistiksel açıdan anlamlı bulunmamıştır (p>0.05),(Tablo 5).

Tablo 6. Bilgi Güvenliği Farkındalığının Eğitim Düzeyine Göre Ortalamaları

	Grup	N	Ort	Ss	F	p
Kişisel Verilerin Korunması	Ön Lisans	16	4,000	0,755	0,558	0,575
	Lisans	30	3,769	0,726		
	Lisansüstü	41	3,904	0,761		
Saldırı ve Tehditlere Yönelik Farkındalık	Ön Lisans	16	2,809	0,947	2,711	0,072
	Lisans	30	2,575	0,772		
	Lisansüstü	41	3,049	0,864		
Bilgi Güvenliği Farkındalığı Genel	Ön Lisans	16	3,439	0,782	1,439	0,243
	Lisans	30	3,207	0,708		
	Lisansüstü	41	3,501	0,736		

Araştırmaya katılan direktörlerin saldırı ve tehditlere yönelik farkındalık, kişisel verilerin korunması, bilgi güvenliği farkındalığı genel puanları ortalamalarının eğitim düzeyi değişkenine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla yapılan tek yönlü varyans analizi (Anova) sonucunda grup ortalamaları arasındaki fark istatistiksel açıdan anlamlı bulunmamıştır (p>0.05),(Tablo 6).

Tablo 7. Bilgi Güvenliği Farkındalığının Göreve Göre Ortalamaları

	Grup	N	Ort	Ss	F	p	Fark
Kişisel Verilerin Korunması	Hekim	5	4,044	0,099	1,885	0,138	
	Hemşire	61	3,812	0,791			
	Ebe	10	3,678	0,594			
	Teknisyen	11	4,328	0,621			
Saldırı ve Tehditlere Yönelik Farkındalık	Hekim	5	3,763	0,128	6,826	**0,000**	**1>2 4>2 1>3 4>3**
	Hemşire	61	2,730	0,835			
	Ebe	10	2,319	0,636			
	Teknisyen	11	3,517	0,785			
Bilgi Güvenliği Farkındalığı Genel	Hekim	5	3,912	0,098	4,430	**0,006**	**4>2 1>3 4>3**
	Hemşire	61	3,302	0,748			
	Ebe	10	3,038	0,518			
	Teknisyen	11	3,947	0,663			

Araştırmaya katılan direktörlerin saldırı ve tehditlere yönelik farkındalık puanları ortalamalarının görev değişkenine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla yapılan tek yönlü varyans analizi (Anova) sonucunda grup ortalamaları arasındaki fark istatistiksel açıdan anlamlı bulunmuştur (F=6,826; p=0,000<0.05). Farklılıkların kaynaklarını belirlemek amacıyla tamamlayıcı post-hoc analizi yapılmıştır. Görev hekim olanların saldırı ve tehditlere yönelik farkındalık puanları (3,763±0,128), görev hemşire olanların saldırı ve tehditlere yönelik farkındalık puanlarından (2,730±0,835) yüksek bulunmuştur. Görev teknisyen olanların saldırı ve tehditlere yönelik farkındalık puanları (3,517±0,785), görev hemşire olanların saldırı ve tehditlere yönelik farkındalık puanlarından (2,730±0,835) yüksek bulunmuştur. Görev hekim olanların saldırı ve tehditlere yönelik farkındalık puanları (3,763±0,128), görev ebe olanların saldırı ve tehditlere yönelik farkındalık puanlarından (2,319±0,636) yüksek bulunmuştur. Görev teknisyen olanların saldırı ve tehditlere yönelik farkındalık puanları (3,517±0,785), görev ebe olanların saldırı ve tehditlere yönelik farkındalık puanlarından (2,319±0,636) yüksek bulunmuştur.

Araştırmaya katılan direktörlerin bilgi güvenliği farkındalığı genel puanları ortalamalarının görev değişkenine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla yapılan tek yönlü varyans analizi (Anova) sonucunda grup ortalamaları arasındaki fark istatistiksel açıdan anlamlı bulunmuştur (F=4,430; p=0,006<0.05). Farklılıkların kaynaklarını belirlemek amacıyla tamamlayıcı post-hoc analizi yapılmıştır. Görev teknisyen olanların bilgi güvenliği farkındalığı genel puanları

(3,947±0,663), görev hemşire olanların bilgi güvenliği farkındalığı genel puanlarından (3,302±0,748) yüksek bulunmuştur. Görev hekim olanların bilgi güvenliği farkındalığı genel puanları (3,912±0,098), görev ebe olanların bilgi güvenliği farkındalığı genel puanlarından (3,038±0,518) yüksek bulunmuştur. Görev teknisyen olanların bilgi güvenliği farkındalığı genel puanları (3,947±0,663), görev ebe olanların bilgi güvenliği farkındalığı genel puanlarından (3,038±0,518) yüksek bulunmuştur.

Araştırmaya katılan direktörlerin kişisel verilerin korunması puanları ortalamalarının görev değişkenine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla yapılan tek yönlü varyans analizi (Anova) sonucunda grup ortalamaları arasındaki fark istatistiksel açıdan anlamlı bulunmamıştır ($p>0.05$).

Araştırmaya katılan görevi hekim olan kalite yönetim direktörlerinin saldırı ve tehditlere yönelik farkındalıklarının diğer meslek gruplarına göre en yüksek iken, görevi ebe olan kalite yönetim direktörlerinin saldırı ve tehditlere yönelik farkındalıkları diğer meslek gruplarına göre en düşük olduğu görülmüştür.

Araştırmaya katılan görevi teknisyen olan kalite yönetim direktörlerinin bilgi güvenliği farkındalıkları diğer meslek gruplarına göre en yüksek iken, görevi ebe olan kalite yönetim direktörlerinin bilgi güvenliği farkındalıklarının diğer meslek gruplarına göre en düşük olduğu görülmüştür (Tablo 7).

Tablo 8. Bilgi Güvenliği Farkındalığının Çalışılan Hastane Türüne Göre Ortalamaları

	Grup	N	Ort	Ss	F	p
Kişisel Verilerin Korunması	Eğitim Araştırma Hastanesi	40	3,951	0,767	0,435	0,728
	Hizmet Hastanesi	25	3,978	0,599		
	Dal Hastanesi	22	3,792	0,851		
Saldırı ve Tehditlere Yönelik Farkındalık	Eğitim Araştırma Hastanesi	40	3,345	0,908	1,038	0,380
	Hizmet Hastanesi	25	2,908	0,730		
	Dal Hastanesi	22	1,972	0,920		
Bilgi Güvenliği Farkındalığı Genel	Eğitim Araştırma Hastanesi	40	3,498	0,750	0,745	0,528
	Hizmet Hastanesi	25	3,474	0,582		
	Dal Hastanesi	22	3,247	0,838		

Araştırmaya katılan direktörlerin saldırı ve tehditlere yönelik farkındalık, kişisel verilerin korunması, bilgi güvenliği farkındalığı genel puanları ortalamalarının çalışılan hastane türü değişkenine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla yapılan tek yönlü varyans analizi (Anova) sonucunda grup ortalamaları arasındaki fark istatistiksel açıdan anlamlı bulunmamıştır (p>0.05),(Tablo 8).

Tablo 9. Bilgi Güvenliği Farkındalığının Toplam İş Tecrübesine Göre Ortalamaları

	Grup	N	Ort	Ss	F	p
Kişisel Verilerin Korunması	1-5 yıl arasında	7	3,960	0,212	1,946	0,149
	6-10 yıl arasında	26	4,098	0,726		
	10 yıldan fazla	54	3,756	0,778		
Saldırı ve Tehditlere Yönelik Farkındalık	1-5 yıl arasında	7	2,741	0,528	1,415	0,249
	6-10 yıl arasında	26	3,079	0,727		
	10 yıldan fazla	54	2,740	0,947		
Bilgi Güvenliği Farkındalığı Genel	1-5 yıl arasında	7	3,387	0,341	1,910	0,154
	6-10 yıl arasında	26	3,619	0,606		
	10 yıldan fazla	54	3,278	0,812		

Araştırmaya katılan direktörlerin saldırı ve tehditlere yönelik farkındalık, kişisel verilerin korunması, bilgi güvenliği farkındalığı genel puanları ortalamalarının toplam iş tecrübesi değişkenine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla yapılan tek yönlü varyans analizi (Anova) sonucunda grup ortalamaları arasındaki fark istatistiksel açıdan anlamlı bulunmamıştır (p>0.05),(Tablo 9).

Tablo 10. Bilgi Güvenliği Farkındalığının Mevcut İş Yerinde Çalışma Süresine Göre Ortalamaları

	Grup	N	Ort	Ss	F	p
Kişisel Verilerin Korunması	5 yıl ve altı	29	3,906	0,740	0,056	0,945
	6-10 yıl arasında	28	3,879	0,628		
	10 yıldan fazla	30	3,841	0,863		
Saldırı ve Tehditlere Yönelik Farkındalık	5 yıl ve altı	29	2,754	0,782	0,291	0,748
	6-10 yıl arasında	28	2,931	0,839		
	10 yıldan fazla	30	2,842	0,981		
Bilgi Güvenliği Farkındalığı Genel	5 yıl ve altı	29	3,364	0,695	0,073	0,929
	6-10 yıl arasında	28	3,433	0,645		
	10 yıldan fazla	30	3,371	0,873		

Araştırmaya katılan direktörlerin saldırı ve tehditlere yönelik farkındalık, kişisel verilerin korunması, bilgi güvenliği farkındalığı genel puanları ortalamalarının mevcut iş yerinde çalışma süresi değişkenine göre anlamlı bir farklılık gösterip göstermediğini

belirlemek amacıyla yapılan tek yönlü varyans analizi (Anova) sonucunda grup ortalamaları arasındaki fark istatistiksel açıdan anlamlı bulunmamıştır (p>0.05),(Tablo 10).

Tablo 11. Bilgi Güvenliği Farkındalığının Kaç Yıldır Bilgisayar Kullanıldığına Göre Ortalamaları

	Grup	N	Ort	Ss	F	p
Kişisel Verilerin Korunması	10 yıl ve altı	14	3,853	0,871	0,778	0,510
	11-15 yıl	36	3,745	0,794		
	16-20 yıl	19	4,035	0,580		
	20 yıl üzeri	18	3,982	0,700		
Saldırı ve Tehditlere Yönelik Farkındalık	10 yıl ve altı	14	2,924	0,915	2,492	0,066
	11-15 yıl	36	2,561	0,821		
	16-20 yıl	19	3,161	0,776		
	20 yıl üzeri	18	3,000	0,902		
Bilgi Güvenliği Farkındalığı Genel	10 yıl ve altı	14	3,416	0,780	1,770	0,159
	11-15 yıl	36	3,188	0,752		
	16-20 yıl	19	3,624	0,624		
	20 yıl üzeri	18	3,520	0,743		

Araştırmaya katılan direktörlerin saldırı ve tehditlere yönelik farkındalık, kişisel verilerin korunması, bilgi güvenliği farkındalığı genel puanları ortalamalarının kaç yıldır bilgisayar kullanıldığı değişkenine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla yapılan tek yönlü varyans analizi (Anova) sonucunda grup ortalamaları arasındaki fark istatistiksel açıdan anlamlı bulunmamıştır (p>0.05),(Tablo 11).

Tablo 12. Bilgi Güvenliği Farkındalığının Kaç Yıldır İnternet Kullanıldığına Göre Ortalamaları

	Grup	N	Ort	Ss	F	p
Kişisel Verilerin Korunması	10 yıl ve altı	28	3,891	0,796	0,387	0,680
	11-15 yıl	37	3,802	0,795		
	15 yıl üzeri	22	3,977	0,591		
Saldırı ve Tehditlere Yönelik Farkındalık	10 yıl ve altı	28	2,933	0,938	0,938	0,395
	11-15 yıl	37	2,694	0,795		
	15 yıl üzeri	22	2,972	0,889		
Bilgi Güvenliği Farkındalığı Genel	10 yıl ve altı	28	3,440	0,780	0,728	0,486
	11-15 yıl	37	3,281	0,746		
	15 yıl üzeri	22	3,504	0,678		

Araştırmaya katılan direktörlerin saldırı ve tehditlere yönelik farkındalık, kişisel verilerin korunması, bilgi güvenliği farkındalığı genel puanları ortalamalarının kaç yıldır internet kullanıldığı değişkenine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla yapılan tek yönlü varyans analizi (Anova) sonucunda grup ortalamaları arasındaki fark istatistiksel açıdan anlamlı bulunmamıştır ($p>0.05$),(Tablo 12).

Araştırmanın sonucunda hipotezlerin durumu aşağıda verilmektedir;

Hipotez 1:

H1:’’Kalite yönetim direktörleri ve kalite birim sorumlularının bilgi güvenliği farkındalığı ile demografik özellikler (cinsiyet, meslek, yaş, eğitim düzeyi, çalışılan hastane türü, toplam iş tecrübesi, mevcut iş yerinde çalışma süresi, bilgisayar kullanma yılı, internet kullanma yılı)arasında ilişki vardır.’’

“Kalite yönetim direktörleri ve kalite birim sorumlularının bilgi güvenliği farkındalığı ile demografik özelliklerinden cinsiyet ve meslekleri arasında ilişki vardır.”

“Kalite yönetim direktörleri ve kalite birim sorumlularının bilgi güvenliği farkındalığı ile demografik özelliklerinden yaş, eğitim düzeyi, çalışılan hastane türü, toplam iş tecrübesi, mevcut iş yerinde çalışma süresi, bilgisayar kullanma yılı, internet kullanma yılı arasında ilişki yoktur.”

Hipotez 2:

H1:’’Kalite yönetim direktörleri ve kalite birim sorumlularının kişisel verilerin korunmasının sağlanması ile demografik özellikleri (cinsiyet, meslek, yaş, eğitim düzeyi, çalışılan hastane türü, toplam iş tecrübesi, mevcut iş yerinde çalışma süresi, bilgisayar kullanma yılı, internet kullanma yılı) arasında ilişki vardır.’’

“Kalite yönetim direktörleri ve kalite birim sorumlularının kişisel verilerin korunmasının sağlanması ile demografik özelliklerinden cinsiyet ve meslekleri arasında ilişki vardır.”

’’Kalite yönetim direktörleri ve kalite birim sorumlularının kişisel verilerin korunmasının sağlanması ile demografik özelliklerinden yaş, eğitim düzeyi, çalışılan

hastane türü, toplam iş tecrübesi, mevcut iş yerinde çalışma süresi, bilgisayar kullanma yılı, internet kullanma yılı arasında ilişki yoktur.’’

Hipotez 3:

H1: “Kalite yönetim direktörleri ve kalite birim sorumlularının saldırı ve tehditlere yönelik farkındalıkları ile demografik özellikleri(cinsiyet, meslek, yaş, eğitim düzeyi, çalışılan hastane türü, toplam iş tecrübesi, mevcut iş yerinde çalışma süresi, bilgisayar kullanma yılı, internet kullanma yılı) arasında ilişki vardır.”

“Kalite yönetim direktörleri ve kalite birim sorumlularının saldırı ve tehditlere yönelik farkındalıkları ile demografik özelliklerinden cinsiyet, meslek, yaş, eğitim düzeyi, çalışılan hastane türü, toplam iş tecrübesi, mevcut iş yerinde çalışma süresi, bilgisayar kullanma yılı, internet kullanma yılı arasında ilişki yoktur.”

5. TARTIŞMA

Sağlık işletmelerinde bilgi güvenliği farkındalığının başarılı olabilmesi için, yöneticilerin desteği, tüm çalışanların sürece dahil edilmesi ve bilgi güvenliğinin bir kurum kültürü olmasıyla mümkündür. Kalite yönetim direktörlerinin bilgi güvenliği farkındalığının belirlendiği bu çalışmada elde edilen bulgular ilgili literatür ile benzerlikler ve farklılıklar gösterebilmektedir.

Yılmaz, Şahin, Akbulut, (2016) Balıkesir ilindeki özel ve kamu okullarında görev yapan 1446 öğretmen üzerinde yapmış olduğu "Öğretmenlerin Digital Veri Güvenliği Farkındalığı'' çalışmasında; erkek öğretmenlerin digital veri güvenliği farkındalığının, kadın öğretmenlere göre daha yüksek olduğunu ortaya koymuştur (70). Yaptığımız çalışmada kalite yönetim direktörlerinin bilgi güvenliği farkındalığının cinsiyete göre değiştiği; erkek kalite yönetim direktörlerinin, kadın kalite yönetim direktörlerine göre bilgi güvenliği farkındalığının daha yüksek olduğu görülmüştür. Elde edilen sonuç, Yılmaz, Şahin, Akbulut'un (2016) çalışmasını destekler niteliktedir.

Çalışma bulgusuna göre erkeklerin kadınlara oranla daha fazla internet ve bilgisayar kullandığı ve bilgi güvenliği farkındalıklarının bu sebepten daha yüksek olduğu düşünülmektedir.

Ramachandran vd. (2012) bir kurumun 4 farklı (personel, muhasebe, bilgi işlem, pazarlama) departmanında yaptığı, farklı meslek gruplarının bilgi güvenliği farkındalığı ve güvenlik kültürlerini inceleyen çalışmasında mesleklerin bilgi güvenliği farkındalığı faktöründe etkisi olduğunu savunmuştur. Muhasebe departmanının bilgi güvenliği farkındalığı kültürü yüksek çıkarken, pazarlama departmanının bilgi güvenliği farkındalığı kültürü düşük çıkmıştır. Bilgi işlem ve personel departmanlarının bilgi güvenliği farkındalığı kültürü de iki birim arasında yer almıştır (71).

Yaptığımız çalışmada mesleği teknisyen ve doktor olan kalite yönetim direktörlerinin bilgi güvenliği farkındalığı, görevi hemşire ve ebe olan kalite yönetim direktörlerinin bilgi güvenliği farkındalığından yüksek bulunmuştur. Elde edilen sonuç ile bu çalışma, Ramachandran vd. (2012) çalışmasını destekler niteliktedir.

Hekim ve teknisyenlerin bilgi teknolojilerini daha etkin kullanmaları ve karşılaşılan risk, tehditlerden haberdar olmalarını gerektirdiği için bilgi güvenliği farkındalığının yüksek çıkmasının sebebi düşünülmektedir.

Gerçeker B. "Sağlık Kuruluşlarında Örgüt iklimi ve Bilgi Güvenliğinin İlişkisi" (2012) çalışması İzmir'de bulunan 13 hastanenin 107 yönetici görevinde bulunan kişilere yapılmıştır. Çalışmanın amacı sağlık kuruluşlarında örgüt iklimi ve bilgi güvenliği ilişkisini belirlemektir (72).

Eğitimi lisans ve lisansüstü olan katılımcıların bilgi güvenliği farkındalığı, eğitimi önlisans ve altı olan katılımcılardan yüksek çıkmıştır. Eğitim düzeyi arttıkça bilgi güvenliği farkındalığı artmaktadır. Yaptığımız çalışmada kalite yönetim direktörlerinin bilgi güvenliği farkındalığı eğitim düzeyine göre anlamlı bulunmamıştır ve Gerçeker B.'nin "Sağlık Kuruluşlarında Örgüt iklimi ve Bilgi Güvenliğinin ilişkisi" (2012) çalışmasını desteklememektedir.

Karadağ M, Abuhanoğlu H. "Sosyokültürel Özelliklerin Bilgi Güvenliği Farkındalığı Üzerine Etkisi: Gülhane Askeri Tıp Fakültesi Eğitim Hastanesi'nde Bir Çalışma." (2015) araştırmaya Gülhane Askeri Tıp Fakültesi Eğitim Hastanesi'nde görevli 314 çalışan katılmıştır. Yaşı büyük olan katılımcıların bilgi güvenliği farkındalığı, yaşı küçük katılımcılardan yüksek çıkmıştır (73).Yaptığımız çalışmada kalite yönetim direktörlerinin bilgi güvenliği farkındalığı katılımcıların yaşına göre anlamlı bulunmamıştır ve Karadağ M, Abuhanoğlu''Sosyokültürel Özelliklerin Bilgi Güvenliği Farkındalığı Üzerine Etkisi: Gülhane Askeri Tıp Fakültesi Eğitim Hastanesi'nde Bir Çalışma'nı desteklememektedir.

Araştırma İstanbul ili kamu hastaneler birliğine bağlı kurumlardaki kalite yönetim direktörleri ve kalite birim sorumlularına yapılmıştır. Çalışmanın sadece İstanbul ilinde yapılması ankete sadece kalite yönetim direktörleri, kalite birim sorumlularının dahil edilmesi araştırmayı sınırlamıştır.

Gelecekte yapılacak olan çalışmalarda daha fazla kurumda yapılması,tüm kalite yönetim biriminde çalışan kişilerin ve tüm çalışanların dahil edilerek yapılması önerilmektedir.

6. SONUÇ ve ÖNERİLER

Kalite Yönetim Direktörlerinin bilgi güvenliği farkındalıklarını belirlemek için yapılan çalışmanın sonuçlarına bakıldığında katılımcılar açısından farkındalık düzeyine dair net bilgiler elde edilmektedir. Konunun teknik boyutundan ziyade, gündelik kullandıkları bilgilerin katılımcılar tarafından daha bilinçli ele alındığı görülmektedir. Araştırma bölümünde yer alan, direktörlerin bilgi güvenliği farkındalığı ile ilgili ifadelere verdiği cevapların dağılımlarına bakıldığında, genel olarak katılımcıların bilgi güvenliği konusunda yerleşik bir farkındalıklarının bulunduğu görülmektedir. Bunun yanı sıra katılımcıların, bilgi güvenliği konusunda, kurum genelinde uyulması gereken kurallar ve takip edilmesi gereken prosedürler konusunda farkındalıklarının da yüksek olduğu izlenmiştir. Bu durum, katılımcıların kurumlarındaki prosedür ve kurallara uyum gösterme konusunda istekli oldukları ve bilgi güvenliği eksikliğinin ne gibi tehditler oluşturabileceğini bildiklerinin de bir göstergesidir.

Fakat yine aynı dağılım üzerindeki değerlendirmelere bakıldığında, ölçeğin Saldırı ve Tehditlere Yönelik Farkındalık alt boyutuna ait (Sosyal Mühendislik Saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum, Hizmet aksatma (Denial of Service-Dos) Saldırısı nedir biliyorum, Kimlik avı (Phishing) saldırısı nedir biliyorum, sosyal mühendislik (Social Engineering) saldırısı nedir biliyorum, Bilgisayarıma casus yazılım (Spyware) olup olmadığını anlayabilirim, Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum, aldatmaca (Hoax) nedir biliyorum) ifadelere en düşük düzeyde katıldıkları görülmektedir.

Buna göre katılımcılar çoğunlukla bilişim dünyasına dair teknik terimleri içeren ve bilgi güvenliği tehdidi oluşturan unsurlar üzerinde yeterli bilgi birikimi ve farkındalık sahibi değillerdir. Bu durum katılımcıların anlık olarak karşılaştıkları çalışmalarını engelleyen, illegal uygulama ve saldırılar karşısında yeterli bilgi ve sorun çözme kapasitesine sahip olmadıkları sorununu beraberinde getirmektedir. Bu sorun aynı zamanda katılımcılar açısından sürecin tam olarak anlaşılmasını ve gün içerisinde sık olarak tekrarlanan risklerde, yeterli refleksi göstermelerini, sorumlu teknik ekipleri harekete geçirmelerini ve gerektiğinde kendi başlarına, anlık güvenlik tehditlerine karşı tepki verebilmelerini de engellemektedir.

Kişisel Mahremiyet nedir biliyorum, şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum, istenmeyen elektronik posta (Spam) nedir biliyorum, bilgi güvenliği ile ilgili sorumluluklarımın ne olduğunu biliyorum, bilgi güvenliğinin ne anlama geldiğini biliyorum, kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum, Usb sürücülerini (Usb Drives) kullanırken dikkat edilmesi gereken hususları biliyorum, digital imza (Digital signature) nedir biliyorum gibi ölçeğin kişisel verilerin korunması alt boyutuna ait ifadelere katılımcıların en yüksek düzeyde katıldıkları görülmektedir.

Katılımcıların günlük hayatta sıklıkla kullanılan bilgilere yüksek düzeyde katıldıkları görülmüştür.

Öte yandan yine araştırma içerisinde, demografik özellikler bazında yapılan değerlendirmelerde, öncelikli olarak erkek katılımcıların, saldırı ve tehditlere yönelik farkındalıkları ve genel bilgi güvenliği farkındalığı konularında kadın katılımcılara göre farkındalıklarının yüksek olduğu gözlemlenmektedir. Bu durum dünya genelinde erkeklerin, teknoloji ürünlerini aktif olarak kullanma konusunda kadınlara göre bir adım önde oldukları düşünülürse, kadın ve erkek katılımcılar arasında ortaya çıkan fark, normal olarak algılanabilecektir.

Öte yandan katılımcıların bilgi güvenliği farkındalığının mesleğe göre ortalamaları ele alındığında, mesleği hekim olan katılımcıların, saldırı ve tehditlere yönelik farkındalıklarının diğer meslek gurubunda yer alan katılımcılara göre yüksek olduğu görülmektedir. Mesleği teknisyen olan katılımcıların genel bilgi güvenliği farkındalıklarının diğer meslek grubunda yer alan katılımcılara göre yüksek olduğu görülmektedir. Mesleği hekim ve teknisyen olan katılımcıların diğer meslek guruplarına göre bilgi teknolojilerini daha etkin kullanmak zorunda olmaları, karşılaşılan risk ve güvenlik açıklarından daha fazla haberdar olmalarını gerektirdiği için bu sonucun oluşması anlamlı bulunmuştur.

Sonuç olarak katımcıların “Kişisel verilerin korunması düzeyi yüksek, saldırı ve tehditlere yönelik farkındalık düzeyi orta, bilgi güvenliği farkındalığı genel düzeyi orta’’ olarak saptanmıştır.

Araştırmadan elde edilen sonuçlardan şu öneriler çıkarılabilir;

Sağlık kurumlarında bilgi güvenliğini sağlamak dinamik bir süreçtir. Sadece teknoloji yöntemlerini kullanarak bilgi güvenliğinin sağlanması düşüncesinden uzaklaşıp insan faktörü sisteme dahil edilmeli, en üst yöneticiden başlayarak tüm personelin katılması sağlanmalıdır. Bilgi güvenliği süreci değişimlere ve iyileştirmelere ihtiyaç duymaktadır, güncelliğini koruma adına gerekirse bağımsız kurumlarca belli aralıklarla denetlenmeli, risk ve tehditler tanımlanmalı ve önlem alınmalıdır. Kurumda bilgi güvenliği farkındalığı oluşturmak için; çalışanların, görev ve yetkileri dikkate alınarak, ihtiyaç ve beklentilerine uygun eğitimler düzenlenmeli ve belirli aralıklarla tekrar edilmelidir. Kuruma yeni başlayan personel için oryantasyon programına bilgi güvenliği eğitimi mutlaka dahil edilmelidir. Bilgi güvenliği farkındalığı çalışmaları belirli zamanda başlayan ve biten bir süreç olmamalı ve kurum kültürü haline getirilmelidir.

KAYNAKÇA

1. Barutçugil İ. *Bilgi Yönetimi*, Kariyer Yayıncılık, İstanbul, 2002, 58-59.

2. Atılgan D. "Bilgi Yönetimi Kavramı ve Gelişimi", *Türk Kütüphaneciliği*, 2009, 23(1): 201-212.

3. Uçak NÖ. "Bilgi: Çok Yüzlü Bir Kavram", *Türk Kütüphaneciliği*, 2010, 24(4): 705-722.

4. Yılmaz M. "Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi", *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, 2009, 49(1): 95-118.

5. Yılmaz M. "Bilgi Yönetimi Ve Örgütsel Öğrenme İlişkisi: Kavramsal Bir Yaklaşım", *A.Ü. Türkiyat Araştırmaları Enstitüsü Dergisi [TAED]*, 2011, (46):313-332.

6. Selvi Ö. "Bilgi Toplumu, Bilgi Yönetimi ve Halkla İlişkiler", *Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi*, 2012, (3): 191-214.

7. Yumuşak İG, Aydın M. ''Bilgi Kamusal Bir Mal mıdır?", *Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 2005, (10): 104-122.

8. Keser H, Güldüren C. "Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması", *K. Ü. Kastamonu Eğitim Dergisi*, 2015, 23(3): 1167-1184.

9. Demir B. "Muhasebe Bilgi Sistemlerinde Bilgi Güvenliği", *Muhasebe ve Finansman Dergisi*, 2005, (26): 147-156.

10. Yılmaz E, Şahin YL, Akbulut Y. "Öğretmenlerin Dijital Veri Güvenliği Farkındalığı", *SAÜ Eğitim Bilimleri Enstitüsü*, 2016, 6(2): 26-45.

11. Vural Y, Sağıroğlu Ş. "Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme", *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 2008, 23(2):507-522.

12. Yılmaz H. "TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi", *Denetişim*, 2014, (15): 45-59.

13. Çetinkaya M. *Bilgi Güvenliği Yönetim Sistemi Altyapısının Değerlendirilmesi İçin Bir Test Aracı Geliştirilmesi* (Tez). İstanbul Kültür Üniversitesi Fen Bilimleri Enstitüsü Yayınlanmamış Yüksek Lisans Tezi; İstanbul, 2008, 511.

14. Henkoğlu T, Yılmaz B. "Avrupa Birliği (AB) Bilgi Güvenliği Politikaları", *Türk Kütüphaneciliği*, 2013, 27(3): 451-471.

15. Güngör M. *Ulusal Bilgi Güvenliği: Strateji Ve Kurumsal Yapılanma* (Tez). Türkiye Cumhuriyeti Kalkınma Bakanlığı Uzmanlık Tezi; Ankara, 2015.

16. Whitman ME, Mattord HJ. "Principles of Information Security", *Cengage Learning*, Boston, 2017, 3.

17. Gülmüş M. *Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği* (Tez), Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Yayınlanmış Yüksek Lisans Tezi; İstanbul, 2010, 17-30.

18. Canbek G, Sağıroğlu Ş. "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", *Gazi Üniversitesi Politeknik Dergisi*, 2006, 9(3): 165-174.

19. Al U. "Internet'te Veri Güvenliği", *Oluşum*, 2010, 10(38): 37-50.

20. Prislan K. "Efficiency of Corporate Security Systems in Managing Information Threats: An Overview of the Current Situation". *Journal of Criminal Justiceand Security*, 2014, 16(2): 128–147.

21. Erol SE, Ceyhan EB, Sağıroğlu Ş. "Kişisel, Kurumsal ve Ulusal Bilgi Güvenliği Farkındalığı Üzerine Bir İnceleme", 8. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara, 2015, 144-153.

22. Güldüren C, Çetinkaya L, Keser H. "Ortaöğretim Öğrencilerine Yönelik Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme Çalışması", *İlköğretim Online*, 2015, 15(2): 682-695.

23. İzgi C. “Mahremiyet Kavramı Bağlamında Kişisel Sağlık Verileri”, *Türkiye Biyoetik Dergisi*, 2014, 1(1): 25-37.

24. Henkoğlu T, Uçak NÖ. “Üniversite Kütüphanelerinde Kişisel Verilerin Korunması”, *Bilgi Dünyası*, 2015 16(1): 45-74.

25. Doğantimur F. *ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği* (Tez). Uzman Yeterlilik Tezi; T.C. Maliye Bakanlığı Strateji Geliştirme Başkanlığı, Ankara, 2009, 9.

26. Von Solms B. “Information Security”, *The Fourth Wave. Computers & Security*, 2006, (25): 165-168.

27. Ohki E. “Information Security Governance Framework. Information Security Governance Framework”, *WISG '09 Proceedings of the First ACM Workshop on Information Security Governance*, Chicago 2009, 1-6.

28. Marşap A, Akalp G, Yeniman E. “Sağlık İşletmelerinde İnsan Kaynağının Kurumsal Bilgi Güvenliği Kültürü Gelişimi”, *Bilişim Teknolojileri Dergisi*, 2010, 3(1): 31-40.

29. Can Ö, Akbaş MF. “Kurumsal Ağ ve Sistem Güvenliği Politikalarının Önemi ve Bir Durum Çalışması”, *TÜBAV Bilim Dergisi*, 2014, 7(2): 16-31.

30. Von Solms R, Von Solms SH. “Information Security Governance” *Due Care. Computers & Security*, 2006, 25, 494-497.

31. Hekim H, Başıbüyük O. “Siber Suçlar Ve Türkiye’nin Siber Güvenlik Politikaları”, *Uluslararası Güvenlik ve Terörizm Dergisi*, 2013, 4(2): 135-158.

32. Eminağaoğlu M, Gökşen Y. “Bilgi Güvenliği Nedir, Ne Değildir, Türkiye’ de Bilgi Güvenliği Sorunları ve Çözüm Önerileri”, *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 2014, 11(4): 1-15.

33. Acılar A, Baştuğ A. “Socia Engineering: An Information Security Threat In Enterprises”, *Global Business Research Congress (GBRC)* 2016, 289-297.

34. Samy GN, Ahmad R. “Threatsto Health Information Security”, Fifth International Conference on Information Assuranceand Security Xi'an, China, 2009, 540-543.

35. Appari A, Johnson ME. “Int. J. Internet and Enterprise Management”, 2010, 6(4): 279-314.

36. Zhang R, Liu L. *Security Models and Requirements for Healthcare Application Clouds*, CLOUD '10 Proceedings of the IEEE, 3rd International Conference on Cloud Computing, Washington, 2010: 268-275.

37. Hiller J. “Prıvacy and Security In The Implementation Of Health Information Technology (Electronic Health Records): U.S. And EU Compared. Privacyand Security in the Implementation of Health Information Technology (Electronic Health Records): US and EU Compared”, BUJ Sci&Tech L, 2011, (17), 1–39.

38. Meingast M, Roosta T, Sastry S. “Security and Privacy Issues with Health Care Information Technology”, Conf Proc IEEE Eng Med Biol Soc. (1), 2006, 5453-5458.

39. Cooper T, Collman J. “Managing Information Security and Privacy in Healthcare Data Mining”, In Medical Informatics: Knowledge Management and Data Mining in Biomedicine Hsinchun Chen et. al (Eds) Berlin: Springer Science & Business Media, 2006, 100-103

40. Öğütçü G, Gürel N, Cula S. “Elektronik Sağlık Kayıtlarının İçeriği, Hassasiyeti ve Erişim Kontrollerine Yönelik Farkındalık ve Beklentilerin Değerlendirilmesi”, VIII. Ulusal Tıp Bilişimi Kongresi, Antalya, 2011, 88-96.

41. Karaaslan E. “Elektronik Sağlık Kayıtlarının Gizlilik ve Mahremiyeti”, İnet-Tr’15, XX. Türkiye'de İnternet Konferansı, İstanbul Üniversitesi, 2015, 215-220.

42. Ay E. “Elektronik Hasta Kayıtları ve Etik Sorunlar”, *İş Ahlakı Dergisi*, 2009, 2(3): 67-74.

43. Özata M, Özer K. “Hastanelerde Hasta Mahremiyetine Yönelik Uygulamalarının Sağlıkta Kalite Standartları Bağlamında Değerlendirilmesi: Konya Örneği”, *International Journal of Social Science*, 2009, (45): 11-33.

44. Fuller SR, Miller DW. “Information Security and Confidentiality: Comingto a Health Care Organization Near You”, *Hospital Physician*, 2000, 21-26.

45. Andriole KP. “Security of Electronic Medical Information and Patient Privacy: What You Need to Know”, *Journal of the American College of Radiology*, 2011, 11(12): 1212-1216.

46. Omotosho A, Emuoyibofarhe J. “A Criticism of the Current Security, Privacy and Accountability Issues in Electronic Health Records”, *International Journal of Applied Information Systems*, 2014, (8): 11-18.

47. Hembroff GC, Wang X, Muftic S. “Providing an Additional Factor for Patient Identification Based on Digital Fingerprint”, *Health Sec '11 20th USENIX Security Symposium (USENIX Security '11) San Francisco*, 2011, Retrievedfromhttps://www.usenix.org/legacy/event/healthsec11/tech/final_files/hembroff-healthsec11.pdf Access: 29 August 2017.

48. Laurinda BH. State Of The Art And Scıence, *American Medical Association Journal of Ethics*, 2012, 14 (9): 712-719.

49. Mc Clanahan K. “Balancing Good Intentions: Protecting the Privacy of Electronic Health Information”, *Bulletin of Science, Technology&Society*, 2008, 28(1): 69-79.

50. Kişisel Sağlık Verilerinin İşlenmesi Ve Mahremiyetinin Sağlanması Hakkında Yönetmelik, http://www.resmigazete.gov.tr/eskiler/2016/10/20161020-1.htm Erişim tarihi. 19.09.2017.

51. Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi,Ankara,2014,https://bilgiguvenligi.saglik.gov.tr/files/BilgiGüvenliğiPolitikalarıYönergesi.pdf Erişim Tarihi.16.06.2017

52. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü, Bilgi Güvenliği Politikalar Kılavuzu,Ankara, 2014.

53. PersonelGizlilikSözleşmesi,01.10.2013 https://bilgiguvenligi.saglik.gov.tr/Dokumantasyon, Erişim Tarihi:01.06.2017

54. SağlıkBakanlığıKurumsalGizlilikTaahütnamesi,01.10.2013

https://bilgiguvenligi.saglik.gov.tr/ Dokumantasyon,Erişim Tarihi.01.06.2017

55. Köksal A, Esatoğlu AE. "Ankara ilindeki Üniversite ve Özel Hastanelerde Kullanılan Elektronik Hastane Bilgi Sisteminin Analizi", *Ankara Üniversitesi Dikimevi Sağlık Hizmetleri MYO Dergisi*, 2005, 7(1): 53-65.

56. Akgün S, Assaf AF. "Sağlık Kuruluşlarında Hasta Güvenliği Kültürünü Nasıl Oluşturabiliriz?" *Hastane Yönetimi*, 2007, (11): 1-8.

57. Ceylan F. Hastane Bilgi Yönetim Sistemleri, Uludağ Üniversitesi Sağlık HizmetleriMeslekYüksekokulu, http://www.uludag.edu.tr/dosyalar/shmyo/ders_notlari/kaynak/HBYS-2015.pdf,ErişimTarihi.15.07.2017

58. Sağlık Bakanlığı Bilgi Güvenliği Farkındalık Bildirgesi, 2015, https://bilgiguvenligi.saglik.gov.tr/files/Gizlilik_Sozlesmeleri,pdf. Erişim Tarihi.05.07.2017

59. Kavuncubaşı Ş. "Hastane ve Sağlık Kurumları Yönetimi", Ankara, 2000.

60. Kaya S. "Sağlık Kurumlarında Kalite Yönetimi", *Anadolu Üniversitesi Açıköğretim Fakültesi Yayınları*, 2013, (1821).

61. Bilgi Güvenliği Yönetim Politikası, 2015.

62. Karaca ŞB. *Sağlık Hizmetlerinde Kalite Yönetimi Ve Hasta Beklentileri Konusunda Bir Uygulama* (Tez). Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü, Yayınlanmamış Yüksek Lisans Tezi; 2014.

63. Öztürk A. "Kalite Yönetimi ve Planlaması", *Ekin Yayınevi*, Bursa, 2009, 35-52.

64. Ersoy EV. "ISO/IEC 27001 Bilgi Güvenliği Standardı", *ODTÜ Yayıncılık*, Ankara, 2012, 14,15.

65. Yılmaz H. "Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması Ve Bilgi Güvenliği Risk", *Denetişim Dergisi*, 2015, 15(51):52,55.

66. Türk Standartları Enstitüsü, “Bilgi Teknolojisi-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemleri-Gereksinimler”, TS ISO/IEC 27001:2005, 2006.

67. Şahinaslan E, Kandemir R, Şahinaslan Ö. “Bilgi Güvenliği Farkındalık Eğitimi Örneği”. Akademik Bilişim ‹09 - XI. Akademik Bilişim Konferansı Bildirileri, Urfa, 2009, 189-194.

68. Karasar N. “Bilimsel Araştırma Yöntemi”, 2. Baskı, Nobel Yayınları, Ankara, 2009: 77.

69. Sümbüloğlu K. “*Biyoistatistik*”, Özdemir Yayıncılık, Ankara, 1993.

70. Yılmaz E, Şahin YL, Akbulut Y. “Öğretmenlerin Dijital Veri Güvenliği Farkındalığı”, *Sakarya University Journal of Education*, 2016, 6(2), 26-45.

71. Ramachandran S, Rao VS, Goles T, Dhillon G. “Variations in Information Security Culture Across Professions: A Qualitative Study”, *The University of Texas, College of Business*, Working Paper, Texas, 2016, 22(7): 34-38.

72. Gerçeker B. *Sağlık Kuruluşlarında Örgüt iklimi ve Bilgi Güvenliğinin ilişkisi* (Tez). İzmir Dokuz Eylül Üniversitesi, Sağlıkta Kalite Geliştirme ve Akreditasyon Anabilim Dalı Yüksek Lisans Tezi; 2012.

73. Karadağ M, Abuhanoğlu H. “Sosyo-Kültürel Özelliklerin Bilgi Güvenliği Farkındalığı Üzerine Etkisi: Gülhane Askeri Tıp Fakültesi Eğitim Hastanesinde Bir Çalışma”, *The Journal of Academic Social Science Studies*, 36: 379-386 Doi number: http://dx.doi.org/10.9761/JASSS2884 Summer II 2015 Erişim: 02.08. 2017

EKLER

EK-1: Anket Formu

I.BÖLÜM
(KİŞİSEL BİLGİLER)

1.Cinsiyetiniz?

( ) Erkek ( ) Kadın

2.Yasınız.

( ) 20 den az ( ) 20-30 ( ) 31-40 ( ) 41-50 ( )51 ve üzeri

3. Eğitim Durumunuz.

( ) Lise ( ) Ön lisans ( ) Lisans ( ) Lisans Üstü

4.Göreviniz.

( ) Hekim ( ) Hemşire ( )Ebe ( ) Teknisyen ( ) Diğer

5.Çalıştığınız hastane türü.

( )Eğitim Araştırma ( )Hizmet Hastanesi ( )Dal Hastanesi

6.Toplam Is Tecrübeniz.

( ) 1 yıldan az ( ) 1-5 yıl arasında ( ) 6-10 yıl arasında ( ) 10 yıldan fazla

7.Mevcut Is Yerinde Çalışma Süreniz.

( ) 1 yıldan az ( ) 1-5 yıl arasında ( ) 6-10 yıl arasında ( )10 yıldan fazla

8.Kaç yıldır bilgisayar kullanıyorsunuz?

( ) 1-5 Yıl ( ) 11-15 Yıl ( ) 21-25 Yıl ( ) 31-35 Yıl ( ) 41 Yıl ve üzeri

( ) 6-10 Yıl ( ) 16-20 Yıl ( ) 26-30 Yıl ( ) 36-40 Yıl

9.Kaç yıldır internet kullanıyorsunuz?

( ) 1-5 Yıl ( ) 11-15 Yıl ( ) 21-25 Yıl ( ) 31-35 Yıl ( ) 41 Yıl ve üzeri

( ) 6-10 Yıl ( ) 16-20 Yıl ( ) 26-30 Yıl ( ) 36-40 Yıl

II. BÖLÜM

(BİLGİ GÜVENLİĞİ FARKINDALIK DÜZEYİ BELİRLEME ÖLÇEĞİ)

Aşağıda bilgi güvenliği farkındalığına yönelik görüşlerinizi tanımlayan 34 madde bulunmaktadır. Aşağıdaki ifadelere ne derece katılıp-katılmadığınızı seçeneğin yanındaki kutuya (X) işareti koyarak belirtiniz. Lütfen her soruyu dikkatli okuyunuz ve boş madde bırakmayınız.

	Maddeler	Hiç Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Tamamen Katılıyorum
1	Bilgisayarıma kötü niyetli kod (malicious code) bulaşıp bulaşmadığını anlayabilirim.					
2	Kötü niyetli yazılımlara (malware) karşı alınması gereken güvenlik tedbirlerini biliyorum.					
3	Aldatmaca (hoax) nedir biliyorum.					
4	Zincir e-postalara (chain e-mail) karşı nasıl hareket etmem gerektiğini biliyorum.					
5	Bilgisayarımda casus yazılım (spyware) olup olmadığını anlayabilirim.					
6	Bilgisayarıma casus yazılım yüklenmesini engelleme yöntemlerini biliyorum.					
7	Kimlik hırsızlığı (identity theft) nedir biliyorum.					
8	Kimlik hırsızlığına karşı alınması gereken güvenlik tedbirlerini biliyorum.					
9	Sahte virüs koruma yazılımının ne olduğunu biliyorum.					
10	Hizmet aksatma (Denial of Service - DoS) saldırısı nedir biliyorum.					
11	Kimlik avı (phishing) saldırısı nedir biliyorum.					
12	Sosyal mühendislik (social engineering) saldırısı nedir biliyorum.					
13	Sosyal mühendislik saldırısına uğramamak için nasıl hareket etmem gerektiğini biliyorum.					
14	Siber zorbalık (cyberbullying) nedir biliyorum.					
15	Siber zorbalığa karşı kendimi nasıl koruyacağımı biliyorum.					

	Maddeler	Hiç Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Tamamen Katılıyorum
16	Siber zorbalığa karşı çocuklarımı nasıl koruyacağımı biliyorum.					
17	Bilgi güvenliğinin ne anlama geldiğini biliyorum.					
18	Bilgi güvenliği ile ilgili sorumluluklarımın ne olduğunu biliyorum.					
19	Kullandığım bilgi sistemlerinde tanımlanmış olan kuralları nasıl uygulayacağımı biliyorum.					
20	Bilgi sistemlerinde kullanılan virüs koruma yazılımını nasıl kullanacağını biliyorum.					
21	Bilgisayarımdaki virüs koruma yazılımının gerçek zamanlı koruma (realtime protection) özelliğini kullanmaktayım.					
22	Bilgisayarımdaki virüs koruma yazılımının otomatik güncelleştirme yapmasını sağlayabilirim.					
23	Dijital imza (digital signature) nedir biliyorum.					
24	Şüpheli veya bilinmeyen kaynaklardan gelen özellikle eklentisi olan e-postaları açmanın taşıdığı riski biliyorum.					
25	E-posta gönderirken "Gizli" (BCC) alanının sağladığı avantajları biliyorum.					
26	İstenmeyen elektronik posta (spam) nedir biliyorum.					
27	İstenmeyen elektronik posta miktarını azaltmak için gerekli bilgiye sahibim.					
28	Sosyal ağ sitelerini (social networking sites) güvenli olarak nasıl kullanacağını biliyorum.					
29	USB sürücülerini (USB drives) kullanırken dikkat edilmesi gereken hususları biliyorum.					
30	Taşınabilir cihazlara (portable devices) yönelik fiziksel güvenliği sağlamak ile ilgili dikkat edilmesi gereken konuları biliyorum.					
31	Taşınabilir cihazlara yönelik veri güvenliği ile ilgili dikkat edilmesi gereken konuları biliyorum.					
32	Kişisel mahremiyet nedir biliyorum.					
33	Çevrimiçi güvenli alışveriş yapmak için gerekli olan güvenlik tedbirlerini biliyorum.					
34	Mavidiş (Bluetooth) teknolojisi ile veri aktarımı konusunda bilgi sahibiyim.					

Teşekkürler...

EK-2: Etik Kurul Onayı

Sağlık Bakanlığı

Sağlık Bilimleri Üniversitesi
Kartal Koşuyolu Yüksek İhtisas Eğitim ve Araştırma Hastanesi
Girişimsel Olmayan Klinik Araştırmalar Etik Kurulu

Etik Kurul 2016

SAYI:2016.5/2-13
KONU: Etik kurul kararı

Sayın ÇİĞDEM ÇELİKÇÖP
Sorumlu Araştırmacı

Kartal Koşuyolu Yüksek İhtisas Eğitim ve Araştırma Hastanesi Girişimsel Olmayan Klinik Araştırmalar Etik Kurulu'na sunmuş olduğunuz 09.11.2016 tarihli**"Kalite yönetim direktörlerinin bilgi güvenliği farkındalığı:İstanbul ili örneği"** konulu çalışmanız 02.12.2016 tarihli etik kurul toplantısında görüşülmüş, başvuru dosyası ile ilgili belgeler araştırmanın/çalışmanın gerekçe, amaç, yaklaşım ve yöntemleri dikkate alınarak incelenmiş ve uygun bulunmuş olup araştırmanın/çalışmanın başvuru dosyasında belirtilen merkezlerde gerçekleştirilmesinde etik ve bilimsel sakınca bulunmadığına toplantıya katılan üyelerin oy birliği ile karar verilmiştir.

Ayrıca çalışmanın yapılacağı kamu hastaneler birliği genel sekreterliklerinden ayrı ayrı izinlerin alınması gerekmektedir.

Bilgilerinizi ve gereğini rica ederim.**02.12.2016**

Prof.Dr.Hasan Sunar

Kartal Koşuyolu Yüksek İhtisas Eğitim ve Araştırma Hastanesi Girişimsel Olmayan Etik Kurul Başkanı

Etik Kurul
Tel:(0216)5001500(1666) Fax:(0216)5001537
Adres: Cevizli Mah., Denizer Cad. Cevizli Kavşağı, Kartal/İstanbul No:1
Elektronik Ağ Adresi: www.kosuyolu.gov.tr

EK-3: İstanbul İli Anadolu Kuzey Kamu Hastaneler Birliği Genel Sekreterliği Araştırma İzni

Evrak Tarih ve Sayısı: 10.02.2017-5016

T.C.
SAĞLIK BAKANLIĞI
TÜRKİYE KAMU HASTANELERİ KURUMU
İstanbul İli Anadolu Kuzey Kamu Hastaneleri Birliği Genel Sekreterliği

Sayı : 77517973-770-
Konu : Anket İzni

SAYIN ÇİĞDEM ÇELİKÇÖP
Cevizli Mahallesi Toros Cad. Yıldız Konutları A Blok D:14 Maltepe/İstanbul

İlgi : 30/12/2016 tarih ve bila sayılı başvurunuz

İlgi sayılı dilekçe ile tarafımıza başvuruda bulunduğunuz "Kalite Yönetim Direktörlerinin Bilgi Güvenliği Farkındalığı: İstanbul İli Örneği/başlıklı Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ)" konulu veri toplamaya yönelik çalışmanızı Genel Sekreterliğimize bağlı sağlık tesislerimizden ekte uygunluğu bulunan hastanelerde yürütme talebiniz ilgili kurumların görüşleri doğrultusunda Genel Sekreterliğimizce uygun görülmüştür.

Bilgilerinizi ve gereğini rica ederim.

Yrd.Doç.Dr. Yavuz BAŞTUĞ
Genel Sekreter a.
İdari Hizmetler Başkanı

EKLER :
Yazı Örneği (12 Sayfa)

E-5 Karayolu Üzeri 34752 / Ataşehir / İstanbul
Telefon: 2165787878 - 7767 Faks: 0216 578 78 21
e-Posta: idarihiz.egitim@iakb.gov.tr
Ayrıntılı bilgi için irtibat: Gülsemin FİLİZ

EK-4: İstanbul İli Beyoğlu Kamu Hastaneler Birliği Genel Sekreterliği Araştırma İzni

Evrak Tarih ve Sayısı: 30.12.2016-66472

T.C.
SAĞLIK BAKANLIĞI
TÜRKİYE KAMU HASTANELERİ KURUMU
İstanbul İli Beyoğlu Kamu Hastaneleri Birliği Genel Sekreterliği

APS

Sayı : 97175836-770-
Konu : Araştırma İzni (Çiğdem ÇELİKÇÖP)

OKAN ÜNİVERSİTESİ REKTÖRLÜĞÜ
(Sağlık Bilimleri Enstitüsü Müdürlüğü)
Avni Dilligil Sok., No:18, Mecidiyeköy/İstanbul

İlgi : 93919723-770 sayılı yazınız.

İlgi sayılı yazınıza istinaden; Enstitünüz Sağlıkta Kalite Yönetimi Yüksek Lisans Programı öğrencisi Çiğdem ÇELİKÇÖP'ün, Yrd.Doç.Dr. Onur YARAR danışmanlığında "Kalite Yönetimi Direktörlerinin Bilgi Güvenliği Farkındalığı: İstanbul İli Örneği" konulu tez çalışmasını Genel Sekreterliğimize bağlı sağlık tesislerinde yapabilmesi uygun görülmüş olup Üniversiteniz Rektörlüğü ile Genel Sekreterliğimiz arasında imzalanan Araştırma İzinleri İşbirliği Protokolünün (i) maddesinde ve Araştırma İzin Taahhütnamesinde belirtildiği üzere araştırmanın bitiminin ardından çalışmanın bir örneğinin Genel Sekreterliğimize teslim edilmesi hususunda;

Gereğini bilgilerinize arz ederim.

Dr. Aşkın AYVAZ
Genel Sekreter a.
İdari Hizmetler Başkanı

Fulya Mah. Mehmetçik Cad. No:63 Şişli/İstanbul
Telefon:0 212 386 13 30 / 2047 Faks:0212 386 13 31
e-Posta: cemilesavci@beyoglubirlik.gov.tr
Ayrıntılı bilgi için irtibat: Cemile SAVCI
Eğitim, Araştırma ve Geliştirme

EK-5: İstanbul İli Çekmece Bölgesi Kamu Hastaneler Birliği Genel Sekreterliği Araştırma İzni

İSTANBUL İLİ ÇEKMECE BÖLGESİ KAMU HASTANELERİ BİRLİĞİ GENEL SEKRETERLİĞİ - İSTANBUL İLİ ÇEKMECE BÖLGESİ KHBGS İDARİ HİZMETLER BAŞKANLIĞI
31/03/2017 10:15 - 40580992 - 663.08 - E.6504
00042348179

T.C.
SAĞLIK BAKANLIĞI
TÜRKİYE KAMU HASTANELERİ KURUMU
İstanbul İli Çekmece Bölgesi Kamu Hastaneleri Birliği Genel Sekreterliği

Sayı : 40580992-663.08
Konu : Çiğdem ÇELİKÇÖP'ün Araştırma İzni Hk.

DAĞITIM YERLERİNE

İlgi: Okan Üniversitesinin 09/01/2017 tarihli ve 35570620-770 sayılı yazısı.

Okan Üniversitesi Sağlık Bilimleri Enstitüsü Sağlıkta Kalite Yönetimi yüksek lisans programı öğrencisi Çiğdem ÇELİKÇÖP'ün **"Kalite Yönetim Direktörlerinin Bilgi Güvenliği Farkındalığı: İstanbul İli Örneği"** konulu yüksek lisans tezi kapsamında; Genel Sekreterliğimize bağlı sağlık tesislerimizde çalışma yapma talebi ile ilgili yapmış olduğu başvuru değerlendirilmiş olup, Küçükçekmece Ağız ve Diş Sağlığı Merkezi ve Avcılar Ağız ve Diş Sağlığı Merkezi dışındaki sağlık tesislerimizde söz konusu araştırma konusundaki çalışmaların hizmeti aksatmayacak şekilde, gönüllülük esası, kişisel veriler ve özel hayatın korunması ile yapılacak çalışmanın kurumumuz bilgisi dışında ilan edilmemesi ilkelerine dikkat edilmesi kaydıyla yapılması uygun görülmüştür.

Adı geçen çalışmacının araştırma onay yazısı ile birlikte söz konusu sağlık tesislerinin Eğitim ve Ar-Ge Birimine başvurarak çalışmasını başlatabileceği hususunda;

Gereğini arz/rica ederim.

Doç. Dr. Mehmet Emin KALKAN
Genel Sekreter

DAĞITIM:
İstanbul Avcılar Murat Kölük Devlet Hastanesi
İstanbul Başakşehir Devlet Hastanesi
İstanbul Beylikdüzü Ağız Ve Diş Sağlığı Merkezi
İstanbul Beylikdüzü Devlet Hastanesi
İstanbul Çatalca İlyas Çokay Devlet Hastanesi
İstanbul Esenyurt Devlet Hastanesi
İstanbul Silivri Devlet Hastanesi
İstanbul Silivri Ceza İnfaz Kurumu Devlet Hastanesi
İstanbul S.B.Ü. Kanuni Sultan Süleyman Eğitim Ve Araştırma Hastanesi
İstanbul S.B.Ü. Mehmet Akif Ersoy Göğüs Kalp Ve Damar Cerrahisi Eğitim Ve Araştırma Hastanesi
Okan Üniversitesi Rektörlüğü (Avni Dilligil Sok. No:18 Mecidiyeköy-Şişli İstanbul)

İstanbul ili Çekmece Kamu Hastaneleri Birliği Genel Sekreterliği Eğitim ve Ar-Ge Birimi Zafer Mah.Çınar Sok. Adapark Plaza No:1 Yenibosna/İSTANBUL
Faks No:
e-Posta:bilal.alegoz@saglik.gov.tr İnt.Adresi: Biyolog Bilal ALEGÖZ İletişim: 0212 454 61 00 - 6410 Fax: 0212 454 61 61
Bilgi için:Bilal ALEGÖZ
Unvan:BİYOLOG
Telefon No:

EK-6: İstanbul İli Fatih Bölgesi Kamu Hastaneler Birliği Genel Sekreterliği Araştırma İzni

İSTANBUL İLİ FATİH BÖLGESİ KAMU HASTANELERİ BİRLİĞİ GENEL SEKRETERLİĞİ - İSTANBUL İLİ FATİH BÖLGESİ KHBGS İDARİ HİZMETLER BAŞKANLIĞI
21/02/2017 18:10 - 70794255 - 663.08 - E.2544
00039874627

T.C.
SAĞLIK BAKANLIĞI
Türkiye Kamu Hastaneleri Kurumu
İstanbul İli Fatih Bölgesi Kamu Hastaneleri Birliği Genel Sekreterliği

Sayı : 70794255-663.08
Konu : Araştırma İzni (Çiğdem ÇELİKÇÖP)

İSTANBUL OKAN ÜNİVERSİTESİ REKTÖRLÜĞÜ
Avni Dilligil Sk. No:18 Mecidiyeköy / İSTANBUL

İlgi : 29/12/2016 tarihli ve 70764255-770 sayılı yazınız.

İlgi sayılı yazınız ile Üniversiteniz Sağlıkta Kalite Yönetimi Yüksek lisans program öğrencisi Çiğdem ÇELİKÇÖP'ün, Yrd.Doç.Dr.Onur YARAR danışmanlığında yapacağı **"Kalite Yönetimi Direktörlerinin Bilgi Güvenliği Farkındalığı: İstanbul İli Örneği"** konulu yüksek lisans tez çalışmasını Genel Sekreterliğimize bağlı tüm Hastanelerde yapabilme talebi tarafımıza bildirilmişti.

Söz konusu araştırma çalışmasının Üniversiteniz ile Genel Sekreterliğimiz arasında imzalanan protokol doğrultusunda birliğimize bağlı "S.B.Ü Haseki Eğitim ve Araştırma Hastanesi", "S.B.Ü. Süleymaniye Kadın Doğum ve Çocuk Hastalıkları Eğitim ve Araştırma Hastanesi", "S.B.Ü. İstanbul Yedikule Göğüs Hastalıkları ve Göğüs Cerrahisi Eğitim ve Araştırma Hastanesi", "Bayrampaşa Devlet Hastanesi", "Lütfiye Nuri Burat Devlet Hastanesinde" yapılması Genel Sekreterliğimiz Bilimsel Kurulu tarafından bilgi güvenliği ve bilimsel çalışmanın etikliği açısından uygun görülmüştür.

Gereğini arz ederim.

Ph. Dr. Hanifi AKTAŞ
Genel Sekreter a.
İdari Hizmetler Başkan V.

Seyitnizam Mh. Mevlana Cd. No:85 Zeytinburnu / İstanbul
Faks No:0(212)5229811
e-Posta:sureyya.gok@saglik.gov.tr İnt.Adresi: Eğitim ve Arge Birimi
Bilgi için:Süreyya GÖK
Unvan:FİRMA
Telefon No:0(212)5308311/1136

EK-7: İstanbul İli Anadolu Güney Kamu Hastaneler Birliği Genel Sekreterliği Araştırma İzni

İSTANBUL İLİ ANADOLU GÜNEY KAMU HASTANELERİ BİRLİĞİ GENEL SEKRETERLİĞİ - İSTANBUL İLİ ANADOLU GÜNEY KHBGS İDARİ HİZMETLER BAŞKANLIĞI
01/02/2017 14:41 - 35778018 - 774.99 - E.2012

T.C.
SAĞLIK BAKANLIĞI
Türkiye Kamu Hastaneleri Kurumu
İstanbul İli Anadolu Güney Kamu Hastaneleri Birliği Genel Sekreterliği

Sayı : 35778018-774.99
Konu : Araştırma İzinleri

SAYIN ÇİĞDEM ÇELİKÇÖP
Cevizli Mah. Toros Cad. Yıldız Konutları A Blok Daire: 14 Maltepe / İstanbul

"Kalite Yönetim Direktörlerinin Bilgi Güvenliği Farkındalığı; İstanbul İli Örneği" başlıklı çalışmanızda kullanacağınız anketi Genel Sekreterliğimize bağlı Sağlık Tesislerinde uygulama talebiniz Bilimsel Araştırma ve Değerlendirme Komisyonumuzca incelenmiş olup, 30/01/2017 tarihli Komisyon toplantısında alınan kararla uygun görülmüştür. Söz konusu çalışmanın onay tarihinden itibaren 10 (on) ayda tamamlanması ve çalışmanın bitiminde bir nüshasının tarafımıza gönderilmesi hususunda;

Bilgilerinizi ve gereğini rica ederim.

Kadir IŞIK
Genel Sekreter a.
İdari Hizmetler Başkanı V.

Başıbüyük Mah. Atatürk Cad. No.1 Maltepe / İstanbul
Faks No:02164210005
e-Posta:emine.denizegilli@saglik.gov.tr İnt.Adresi: www.iagb.gov.tr
Bilgi için:Emine DENİZ EĞİLLİ
Unvan:HEMŞİRE
Telefon No:(0216) 4212626-(1321)

EK-8: İstanbul İli Bakırköy Bölgesi Kamu Hastaneler Birliği Genel Sekreterliği Araştırma İzni

İSTANBUL İLİ BAKIRKÖY BÖLGESİ KAMU HASTANELERİ BİRLİĞİ GENEL SEKRETERLİĞİ - BAKIRKÖY İDARİ HİZMETLER BAŞKANLIĞI
29/03/2017 14:07 - 95273397 - 604.02 - E.6269
00042308023

T.C.
SAĞLIK BAKANLIĞI
TÜRKİYE KAMU HASTANELERİ KURUMU
İstanbul İli Bakırköy Bölgesi Kamu Hastaneleri Birliği Genel Sekreterliği

Sayı : 95273397-604.02
Konu : Araştırma İzni Hk. (Çiğdem ÇELİKÇÖP)

DAĞITIM YERLERİNE

Okan Üniversitesi Sağlık Bilimleri Enstitüsü Sağlıkta Kalite Yönetimi yüksek lisans öğrencisi Çiğdem ÇELİKÇÖP'ün, **"Kalite Yönetimi Direktörlerinin Bilgi Güvenliği Farkındalığı; İstanbul İli Örneği"** konulu çalışmasını kurumunuzda yapma talebi Genel Sekreterliğimizce uygun görülmüştür.

Söz konusu araştırmanın yürütülmesi esnasında adı geçene gerekli kolaylığın gösterilmesi ve çalışmanın başlangıç tarihi, başlamaması, iptali veya sonlandırılması gibi durumların Genel Sekreterliğimize bildirilmesini rica ederim.

Dr. Abdulvahit SÖZÜER
Genel Sekreter a.
İdari Hizmetler Başkanı

Dağıtım:
S.B.Ü. İstanbul Fizik Tedavi Ve Rehabilitasyon E.A.H.
S.B.Ü. İstanbul Bakırköy Prof. Dr. Mazhar Osman Ruh Sağlığı Ve Sinir Hast. E.A.H.
S.B.Ü. İstanbul Bakırköy Dr.Sadi Konuk E.A.H.
S.B.Ü. İstanbul Bağcılar Eğitim Ve Araştırma Hastanesi
İstanbul Esenler Kadın Doğum Ve Çocuk Hastalıkları Hastanesi
İstanbul Bahçelievler Devlet Hastanesi

Zuhuratbaba Mah.Dr Tevfik Sağlam Cad. 25/2 34147 Bakırköy İSTANBUL
Ayrıntılı bilgi için: İstanbul İli Bakırköy Bölgesi Kamu Hastaneleri Birliği Genel Sekreterliği Eğitim ve Ar-Ge Birimi nilufer.savas@saglik.gov.tr

EK-8: İstanbul İli Bakırköy Bölgesi Kamu Hastaneler Birliği Genel Sekreterliği Araştırma İzni

İSTANBUL İLİ BAKIRKÖY BÖLGESİ KAMU HASTANELERİ BİRLİĞİ GENEL SEKRETERLİĞİ - BAKIRKÖY İDARİ HİZMETLER BAŞKANLIĞI
29/03/2017 14:07 - 95273397 - 604.02 - E.6270
00042307867

T.C.
SAĞLIK BAKANLIĞI
TÜRKİYE KAMU HASTANELERİ KURUMU
İstanbul İli Bakırköy Bölgesi Kamu Hastaneleri Birliği Genel Sekreterliği

Sayı : 95273397-604.02
Konu : Araştırma İzni Hk. (Çiğdem ÇELİKÇÖP)

OKAN ÜNİVERSİTESİ REKTÖRLÜĞÜNE
(Avni Dilligil Sok. No:18 34394 Mecidiyeköy / İstanbul)

İlgi : 93919723-770 sayılı yazınız.

İlgide kayıtlı yazınız ile Üniversiteniz Sağlık Bilimleri Enstitüsü Sağlıkta Kalite Yönetimi yüksek lisans öğrencisi Çiğdem ÇELİKÇÖP'ün, **"Kalite Yönetimi Direktörlerinin Bilgi Güvenliği Farkındalığı; İstanbul İli Örneği"** başlıklı çalışmasını, Genel Sekreterliğimize bağlı İstanbul Lepra Deri ve Zührevi Hastalıkları Hastanesi, İstanbul Bahçelievler Devlet Hastanesi, Sağlık Bilimleri Üniversitesi Bakırköy Prof. Dr. Mazhar Osman Ruh Sağlığı ve Sinir Hastalıkları Eğitim ve Araştırma Hastanesi, Sağlık Bilimleri Üniversitesi Bağcılar Eğitim ve Araştırma Hastanesi, İstanbul Fizik Tedavi ve Rehabilitasyon Eğitim ve Araştırma Hastanesi, Bağcılar Ağız ve Diş Sağlığı Merkezi, Bahçelievler Ağız ve Diş Sağlığı Merkezi, Güngören Ağız ve Diş Sağlığı Merkezi, Esenler Kadın Doğum ve Çocuk Hastalıkları Hastanesi ve Sağlık Bilimleri Üniversitesi Bakırköy Dr. Sadi Konuk Eğitim ve Araştırma Hastanesi'nde uygulama talebi, başvuru dosyası ve ilgili belgeleri, 28.03.2017 tarihinde gerçekleştirilen 2017/2 sayılı Bilimsel Araştırmalar Komisyonu Toplantısında araştırmanın; amaç, gerekçe, yaklaşım ve yöntemleri, yürürlükte bulunan "İyi Klinik Uygulama Kılavuzu" dikkate alınarak incelenmiş olup araştırmanın yürütülmesinde sakınca olmadığına karar verilmiştir.

İş bu konuda adı geçenin yapacağı çalışmasının bitiminde bir nüshasının Genel Sekreterliğimize teslim edilmesi hususunda;

Gereğini arz ederim.

Dr. Abdulvahit SÖZÜER
Genel Sekreter a.
İdari Hizmetler Başkanı

Zuhuratbaba Mah.Dr Tevfik Sağlam Cad. 25/2 34147 Bakırköy İSTANBUL
Ayrıntılı bilgi için: İstanbul İli Bakırköy Bölgesi Kamu Hastaneleri Birliği Genel Sekreterliği Eğitim ve Ar-Ge Birimi nilufer.savas@saglik.gov.tr

EK-9: Araştırma İzni Veren Hastaneler

1. Avcılar Murat Kölük Devlet Hastanesi,
2. Bayrampaşa Devlet Hastanesi,
3. Başakşehir Devlet Hastanesi,
4. Bahçelievler Ağız ve Diş Sağlığı Merkezi,
5. Bahçelievler Devlet Hastanesi,
6. Bağcılar Ağız ve Diş Sağlığı Merkezi,
7. Beykoz Devlet Hastanesi,
8. Beykoz Ağız ve Diş Sağlığı Merkezi,
9. Beylikdüzü Ağız ve Diş Sağlığı Merkezi,
10. Beylikdüzü Devlet Hastanesi,
11. Beşiktaş Sait Çiftçi Devlet Hastanesi,
12. Çatalca İlyas Çokay Devlet Hastanesi,
13. Çekmeköy Ağız ve Diş Sağlığı Hastanesi,
14. Esenler Kadın Doğum ve Çocuk Hastalıkları Hastanesi,
15. Erenköy Fizik Tedavi ve Rehabilitasyon Hastanesi,
16. Esenyurt Devlet Hastanesi,
17. Eyüp Devlet Hastanesi,
18. Göztepe Ağız ve Diş Sağlığı Merkezi,
19. Güngören Ağız ve Diş Sağlığı Merkezi,

20. İstanbul Sağlık Bakanlığı Marmara Üniversitesi Pendik Eğitim ve Araştırma Hastanesi,
21. İstanbul Lepra Deri ve Zührevi Hastalıkları Hastanesi,
22. İstanbul Fizik Tedavi ve Rehabilitasyon Eğitim ve Araştırma Hastanesi,
23. İstanbul Meslek Hastalıkları Hastanesi,
24. İstanbul Tacirler Eğitim Vakfı Sultanbeyli Devlet Hastanesi,
25. İstanbul Medeniyet Üniversitesi Göztepe Eğitim ve Araştırma Hastanesi,
26. İstanbul Avcılar Ağız ve Diş Sağlığı Merkezi,
27. Kartal Ağız ve Diş Sağlığı Merkezi,
28. Kartal Yavuz Selim Devlet Hastanesi,
29. Kağıthane Devlet Hastanesi,
30. Lütfiye Nuri Burat Devlet Hastanesi,
31. Maltepe Devlet Hastanesi,
32. Okmeydanı Ağız Diş Sağlığı Hastanesi,
33. Pendik Devlet Hastanesi,
34. Sancaktepe Ağız ve Diş Sağlığı Hastanesi,
35. Sarıyer İsmail Akgün Devlet Hastanesi,
36. Sarıyer İstinye Devlet Hastanesi,
37. Sarıyer Ağız Diş Sağlığı Hastanesi,
38. Silivri Devlet Hastanesi,
39. Silivri Ceza İnfaz Kurumu Devlet Hastanesi,

40. Sultanbeyli Ağız ve Diş Sağlığı Merkezi,
41. S.B.Ü Metin Sabancı Baltalimanı Kemik Hastalıkları Eğitim ve Araştırma Hastanesi,
42. S.B.Ü Prof. Dr. N. Reşat Belger Beyoğlu Göz Eğitim ve Araştırma Hastanesi,
43. S.B.Ü İstanbul Dr. Siyami Ersek Göğüs Kalp ve Damar Cerrahisi Eğitim ve Araştırma Hastanesi,
44. S.B.Ü İstanbul Ümraniye Eğitim ve Araştırma Hastanesi,
45. S.B.Ü Sultan Abdülhamit Han Eğitim ve Araştırma Hastanesi,
46. S.B.Ü Bakırköy Prof. Dr. Mazhar Osman Ruh Sağlığı ve Sinir Hastalıkları Eğitim ve Araştırma Hastanesi,
47. S.B.Ü Bağcılar Eğitim ve Araştırma Hastanesi,
48. S.B.Ü Bakırköy Dr. Sadi Konuk Eğitim ve Araştırma Hastanesi,
49. S.B.Ü Süleymaniye Kadın Doğum ve Çocuk Hastalıkları Eğitim ve Araştırma Hastanesi,
50. S.B.Ü Haseki Eğitim ve Araştırma Hastanesi,
51. S.B.Ü Şişli Hamidiye Etfal Eğitim ve Araştırma Hastanesi,
52. S.B.Ü Okmeydanı Eğitim ve Araştırma Hastanesi,
53. S.B.Ü Kartal Koşuyolu Yüksek İhtisas Eğitim ve Araştırma Hastanesi,
54. S.B.Ü Kartal Dr. Lütfi Kırdar Eğitim ve Araştırma Hastanesi,
55. S.B.Ü Zeynep Kamil Kadın ve Çocuk Hastalıkları Eğitim ve Araştırma Hastanesi,
56. S.B.Ü Süreyyapaşa Göğüs Hastalıkları ve Göğüs Cerrahisi Eğitim ve Araştırma Hastanesi,

57. S.B.Ü Kanuni Sultan Süleyman Eğitim ve Araştırma Hastanesi,
58. S.B.Ü Mehmet Akif Ersoy Göğüs Kalp ve Damar Cerrahisi Eğitim ve Araştırma Hastanesi,
59. S.B.Ü. İstanbul Yedikule Göğüs Hastalıkları ve Göğüs Cerrahisi Eğitim ve Araştırma Hastanesi,
60. S.B.Ü Gaziosmanpaşa Taksim Eğitim ve Araştırma Hastanesi,
61. S.B.Ü Erenköy Ruh ve Sinir Hastalıkları Eğitim ve Araştırma Hastanesi,
62. S.B.Ü. Fatih Sultan Mehmet Eğitim ve araştırma Hastanesi,
63. Şile Devlet Hastanesi,
64. Tuzla Devlet Hastanesi,
65. Üsküdar Ahmet Yüksel Özemre Ağız ve Diş Sağlığı Merkezi,
66. Üsküdar Devlet Hastanesi,
67. Yakacık Doğum ve Çocuk Hastalıkları Hastanesi,