T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

Sağlık Yönetimi Anabilim Dalı
Sağlık Yönetimi

Yüksek Lisans Tezi

ISO/IEC 27001 KAPSAMINDA BİLGİ GÜVENLİĞİ YÖNETİM FARKINDALIĞININ DEĞERLENDİRİLMESİ: ANKARA İLİ SAĞLIK KURUMLARI BİLGİ İŞLEM BİRİMİ ÇALIŞANLARI ÖRNEĞİ

Hadis SOYSAL
0009-0008-8656-0215

Danışman
Doç. Dr. Yusuf Yalçın İLERİ
0000-0002-3911-1192

Konya – 2023

TEŞEKKÜR

Yüksek lisans eğitimim ve tez çalışmam süresince bilgi ve tecrübelerinden istifade ettiğim ve bu çalışmanın ortaya çıkmasına vesile olan danışman hocam Doç. Dr. Yusuf Yalçın İLERİ' ye, Doç. Dr. Ayhan ULUDAĞ ve Dr. Öğr. Üyesi Emel FİLİZ ile yüksek lisans eğitimim süresince bana çok şey öğreten, ilgi ve desteklerini esirgemeyen değerli hocalarım Doç. Dr. Şerife Didem KAYA ve Doç. Dr. Aydan YÜCELER' e,

Araştırmamın her aşamasında fikirleri, uygulamaları ve analizleri ile desteğini esirgemeyen, kendisiyle gurur duyduğum canım ablam Dr. Öğr. Üyesi Sümeyra SOYSAL'a

Süreçte bana olan güvenlerini hiç kaybetmeyen ve zamanından aldığım değerli ailem, kıymetli eşim Aysel SOYSAL ve Nisan 2022 de hayatımızı her yönüyle değiştiren Kerem SOYSAL bebeğimize, sonsuz özlemle aradığım Annem Miyase SOYSAL, Döne SOYSAL'a ve Hasan AKÇA'ya

Çalışmamın uygulama aşamasında her türlü desteği sağlayan Ankara İl Sağlık Müdürlüğü Destek Hizmetleri Başkanı Dr. Zübeyir DEDEOĞLU, Uzman Emre Çağatay DOĞAN ve Uzman Mustafa Atilla IŞIK,

Her koşulda yanımda olarak beni daima destekleyen Sağlık Bakan Danışmanı Dr. Arif Burak AKTAŞ ve Daire Başkanı Fahrettin ERGÜN'e, bilgeliği ve tecrübeleri ile bana yol gösteren her anlamda desteğini koşulsuz sunan Arif Satılmış AKÇA' ya,

Araştırmaya katılan Ankara İl Sağlık Müdürlüğü ve Bağlı Sağlık Tesisleri çalışanlarına,

Bu araştırmanın var olmasına katkıları olan herkese sonsuz teşekkürlerimi sunarım.

Hadis SOYSAL

Haziran 2023

İÇİNDEKİLER

TEZ ONAY SAYFASI

Necmettin Erbakan Üniversitesi Sağlık Bilimleri Enstitüsü Sağlık Yönetimi Anabilim Dalı Yüksek Lisans Öğrencisi Hadis SOYSAL'ın "**ISO/IEC 27001 Kapsamında Bilgi Güvenliği Yönetim Farkındalığının Değerlendirilmesi: Ankara İli Sağlık Kurumları Bilgi İşlem Birimi Çalışanları Örneği**" başlıklı tezi tarafımızdan incelenmiş; amaç, kapsam ve kalite yönünden Yüksek Lisans Tezi olarak kabul edilmiştir.

Konya / 02/06/2023

Tez Danışmanı Doç. Dr. Yusuf Yalçın İLERİ
Necmettin Erbakan Üniversitesi

Jüri Üyesi Doç.Dr. Ayhan ULUDAĞ
Necmettin Erbakan Üniversitesi

Jüri Üyesi Dr. Öğr. Üyesi Emel FİLİZ
Selçuk Üniversitesi

Yukarıdaki tez, Necmettin Erbakan Üniversitesi Sağlık Bilimleri Enstitüsü Yönetim Kurulunun 07/06/2023 tarih ve 13/14 sayılı kararı ile onaylanmıştır.

Prof. Dr. Hasibe VURAL

Enstitü Müdürü

TEZ ÇALIŞMASI ORİJİNALLİK RAPORU

ISO/IEC 27001 Kapsamında Bilgi Güvenliği Yönetim Farkındalığının Değerlendirilmesi: Ankara İli Sağlık Kurumları Bilgi İşlem Birimi Çalışanları Örneği başlıklı tez çalışmamın toplam **94** sayfalık kısmına ilişkin, 15.05.2023 tarihinde tez danışmanım tarafından **Turnitin** adlı intihal tespit programından aşağıda belirtilen filtrelemeler uygulanarak alınmış olan orijinallik raporuna göre, tezimin benzerlik oranı **%16** olarak belirlenmiştir.

Uygulanan filtrelemeler:

1. Tez kabul sayfası hariç
2. Tez çalışması orijinallik raporu sayfası hariç
3. Bilimsel etik beyannamesi sayfası hariç
4. Önsöz hariç
5. İçindekiler hariç
6. Simgeler ve kısaltmalar hariç
7. Materyal ve metot hariç
8. Kaynaklar hariç
9. Alıntılar dâhil
10. 7 kelimeden daha az örtüşme içeren metin kısımları hariç

Necmettin Erbakan Üniversitesi Tez Çalışması Orijinallik Raporu Uygulama Esaslarını inceledim ve tez çalışmamın, bu uygulama esaslarında belirtilen azami benzerlik oranının (%30) altında olduğunu ve intihal içermediğini; aksinin tespit edileceği muhtemel durumda doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi ve yukarıda vermiş olduğum bilgilerin doğru olduğunu beyan ederim.

15.05.2023

Hadis SOYSAL

Danışman Doç. Dr. Yusuf Yalçın İLERİ

BİLİMSEL ETİK BEYANNAMESİ

Bu tezin tamamının kendi çalışmam olduğunu, planlanmasından yazımına kadar tüm aşamalarında bilimsel etiğe ve akademik kurallara özenle riayet edildiğini, tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez hazırlama kurallarına uygun olarak hazırlanan bu çalışmada başkalarının eserlerinden yararlanılması durumunda bilimsel kurallara uygun olarak atıf yapıldığını ve bu kaynakların kaynaklar listesine eklendiğini beyan ederim.

15/05/2023

Hadis SOYSAL

KISALTMALAR VE SİMGELER LİSTESİ

ABD: Amerika Birleşik Devletleri

AB: Avrupa Birliği

IBM: International Business Machines

WHO: Dünya Sağlık Örgütü

GDPR: AB Genel Veri Koruma Yönetmeliği'nin

HIPAA: ABD Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası

CDC: Amerika Birleşik Devletleri Sağlık ve Sosyal Hizmetler Bakanlığı'na bağlı Hastalık Kontrol ve Korunma Merkezi

AHIMA: Amerikan Sağlık Bilgi Yönetimi Derneği

OAIC: Avustralya Bilgi Komiserliği Ofisi

DPA: İngiltere Veri İşleme Sözleşmesi

SB: Sağlık Bakanlığı

TÜİK: Türkiye İstatistik Kurumu

KVVK: Kişisel Verilerin Korunması Kanunu

BT: Bilgi Teknojileri

HBS: Hastane Bilgi Sistemleri

EHS: Elektronik Sağlık Kayıtları

RFID: Radyo Frekansı ile Tanımlama teknolojisi,

n: Örneklem Sayısı

p: Anlamlılık Düzeyi

SPSS: Statistical Package for the Social Sciences

SS: Standart Sapma

x^2: Pearson Ki-Kare

$: Dolar

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Necmettin Erbakan Üniversitesi, Sağlık Bilimleri Enstitüsü
Sağlık Yönetimi Anabilim Dalı
Sağlık Yönetimi
Yüksek Lisans Tezi

ISO/IEC 27001 KAPSAMINDA BİLGİ GÜVENLİĞİ YÖNETİM FARKINDALIĞININ DEĞERLENDİRİLMESİ: ANKARA İLİ SAĞLIK KURUMLARI BİLGİ İŞLEM BİRİMİ ÇALIŞANLARI ÖRNEĞİ

Hadis SOYSAL

Konya-2023

Sağlık kurumları hastaların kişisel bilgilerinin yanı sıra tıbbi ve idari verilerin yoğun bir şekilde kullanıldığı ve bu bilgilerin tanımlaması, değerlendirilmesi, uygulanması, saklanması ve veri paylaşılmasına olanak sağlayan bilgi ve iletişim teknolojilerin yoğun ve etkin kullanıldığı bir sektör olarak yer almaktadır. Sağlık sektörü diğer sektörlere göre elde edilen verilerin önemi gereği daha büyük siber risklerle karşı karşıya kalmakta, karşılaşılabilecek veri ihlallerin kontrolü için de bilgi güvenliği politikalarının uygulanlması zorunlu bir süreç haline gelmektedir. Bilgi güvenliği yalnızca sağlık tesislerinin bilgi sistemlerinin güvenliğini ile ilgili olmadığı, bilgi güvenliği sürecinde insan faktörü, cihazların durumu, personel çeşitliliği, erişim yetkisi, mahremiyet, maliyet, etik, eğitim ve görev düzeyi ile ilgili birçok faktörün etki ettiği karmaşık bir süreç olarak karşımıza çıkmaktadır.Bu araştırmanın amacı, sağlık tesislerin bilgi işlem altyapısı anlamında her türlü operasyonel faaliyetlerin süreçlerinden sorumlu bilgi işlem personelinin Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi kapsamındaki uygulamaların; ISO/IEC 27001 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler dokümanı EK-A' da yer alan Referans Kontrol Amaçları ve Kontroller paralelinde (Kılıç 2019) tarafından hazırlanan ankete göre kavramsal farkındalık düzeyleri ile cinsiyete, deneyime, eğitim düzeyine, unvana, çalıştığı birime, çalıştığı kurumun türüne ve çalıştığı kurumun kapasitesine göre bilgi güvenliği yönetim farkındalığı arasındaki ilişkiyi ortaya koymaktır.

Ankara İl Sağlık Müdürlüğü ve bağlı tüm sağlık tesislerinde (Merkez Müdürlük, Hastaneler, İlçe Hastaneleri, İlçe Sağlık Müdürlükleri, Entegre Hastaneler) bilgi işlem biriminde çalışan yönetici, mühendis, tekniker ve diğer kamu personeli çalışanlar ile hizmet alım yöntemi ile sağlık tesislerinde istihdam edilen bilgi işlem personelinden gönüllü olarak katılan 268 sağlık çalışanın veri toplama aracına verdiği cevaplar üzerinden çalışmanın amacına yönelik veriler elde edilmiş olup kayıp ve uç değerlere ilişkin ön analizi sonucunda 260 çalışana ait anket verileri SPSS 21 istatistik programı ile incelenmiştir. Çalışmada tanımlayıcı istatistikler ile birlikte bölüm puanları normal dağılmadığı için Mann_Whitney U testi ve grup ortalamalarının karşılaştırılmasında parametrik olmayan yöntemlerden Kruskall-Wallis H testi kullanılmıştır. Her bir araştırma problemi için alt amaç soru gruplarına ait Cronbach Alfa değerleri incelendiğinde sonuçların 0,88 ile 0,98 arasında olduğu görülmüş ve analizlerde kullanılan ölçeklerin güvenilir oldukları gözlenmiştir. Ankete katılan 260 sağlık çalışanın %66,2'si 2.ve 3.basamak sağlık tesisinde çalışmaktadır. Katılımcıların %35'i lisans eğitime sahip olup, %37,7'si 34-41 yaş grubunda olup %72,7'si erkek, ve %80,00'i evlidir. Katılımcıların %25'i 6-10 yıl hizmet süresine sahiptir. Katılımcılardan 163 kişi %62,7'si kamu alımları ile yerleşen tekniker, teknisyen veya hizmet alım yöntemi ile çalışan bilgi işlem/HBYS personelini ve personelin %66,2'sı bilgi işlem biriminde doğrudan çalışırken, %17,3'ü sağlık tesislerinde yönetici unvanında çalışmaktadır. Sağlık çalışanlarının bilgi güvenliği yönetim farkındalığını değerlendirme formunda yer alan her soruya verdikleri evet, kısmen ve hayır cevaplarına karşılık olarak bölümlere verdikleri cevapların en az %95,77'si evet yanıtı verdiği, çalışanların; eğitim durumu, unvan, çalıştığı kurum türü, çalıştığı kurum kapasitesi ile bilgi güvenliği yönetimi politikaları kavramsal farkındalık düzeyi arasında anlamlı ve pozitif yönlü bir ilişki olduğu tespit edilmiştir.

Anahtar Kelimeler: Bilgi, Bilgi Güvenliği, Iso 27001, Siber Güvenlik, Veri İhlali

ABSTRACT

Necmettin Erbakan University, Graduate School of Health Sciences
Health Management Department
Health Management
Master Thesis

EVALUATION OF INFORMATION SECURITY MANAGEMENT AWARENESS WİTHİN THE SCOPE OF ISO/IEC 27001: THE CASE OF ANKARA PROVINCE HEALTH INSTİTUTİONS INFORMATİON PROCESSING UNIT EMPLOYEES

Hadis SOYSAL

Konya-2023

Health institutions are a sector where medical and administrative data are used intensively as well as personal information of patients and information and communication technologies that enable the definition, evaluation, application, storage and data sharing of this information are used intensively and effectively. The health sector is faced with greater cyber risks due to the importance of the data obtained compared to other sectors, and the implementation of information security policies for the control of data breaches that may be encountered becomes a mandatory process. Information security emerges as a complex process that is not only related to the security of information systems of health facilities, but also affected by many factors related to the human factor, condition of devices, personnel diversity, access authorization, privacy, cost, ethics, education and duty level in the information security process.The purpose of this research is to analyze the applications of the IT personnel responsible for the processes of all kinds of operational activities in terms of the IT infrastructure of health facilities within the scope of the Information Security Policy Directive of the Ministry of Health; According to the survey prepared by ISO/IEC 27001 Information Technology - Security Techniques - Information Security Management Systems - Requirements document in parallel with Reference Control Objectives and Controls (Kılıç 2019) in Annex-A, conceptual awareness levels and gender, experience, education level, title The aim is to reveal the relationship between information security management awareness according to the unit, the type of institution and the capacity of the institution.

Managers, engineers, technicians and other public personnel working in the IT unit of Ankara Provincial Health Directorate and all affiliated health facilities (Central Directorate, Hospitals, District Hospitals, District Health Directorates, Integrated Hospitals) and data processing personnel employed in health facilities by service procurement method. Data for the purpose of the study were obtained through the answers given to the data collection tool by 268 health workers who voluntarily participated in the study. In the study, Mann_Whitney U test and Kruskall-Wallis H test, which is one of the non-parametric methods, were used to compare the group averages, since the descriptive statistics and department scores were not normally distributed. When the Cronbach Alpha values of the sub-objective question groups for each research problem were examined, it was observed that the results were between .88 and .98, and it was observed that the scales used in the analyzes were reliable. 66.2% of the 260 health workers who participated in the survey work in the second and third level health facilities. 35% of the participants have undergraduate education, 37.7% are in the 34-41 age group, 72.7% are male and 80.00% are married. 25% of the participants have 6-10 years of service. Of the participants, 163 (62.7%) were technicians, technicians or IT personnel working with the service procurement method, who settled with public procurement, and 66.2% of the personnel worked directly in the information processing unit, 17.3% of them He works as a manager at the facility. In response to the yes, partially and no answers given to each question in the information security management awareness evaluation form of healthcare professionals, at least 95.77% of the answers given to the departments gave a yes answer; It has been determined that there is a significant and positive relationship between educational status, title, type of institution, capacity of the institution and the level of conceptual awareness of information security management policies. In response to the yes, partially and no answers given by the healthcare professionals to each question in the information security management awareness evaluation form, at least 95.77% of the answers given to the departments gave a yes answer; It has been determined that there is a significant and positive relationship between educational status, title, type of institution, the capacity of the institution, and the level of conceptual awareness of information security management policies.

Keywords: Cyber Security, Data Breach, Information, Information Security, Iso 27001,

1. GİRİŞ VE AMAÇ

Kuruluşlar günümüzde, teknoloji ve gelişimin dinamik ortamları nedeniyle dramatik bir değişim sürecinden geçmektedir. Kuruluşların, insanların, süreçlerin, yeteneklerin ve performansın sürekli iyileştirilmesi yoluyla kendi alanlarında rekabetçi olmaya odaklanmakta (Aras, 2018) ve rekabet avantajlarını sürdürmek için tüm kaynaklarını, özellikle entelektüel kaynaklarını kullanması gerekmektedir.

Dijital teknolojiler, ara bağlantı ve cihazlardaki son gelişmeler, iletişimin artan hızı, işletme maliyetlerinin düşmesi, sistem erişilebilirliğinin iyileştirilmesi ve bunun verimlilik ve üretkenlik üzerindeki etkisi açısından kuruluşlara çeşitli faydalar sağlamıştır (Rohan ve ark., 2023). Günümüzde bilginin elde edilmesi ve elde edilen bilginin yoğun bir şekilde kullanıldığı sağlık hizmeti işletmelerinde, bilgi; işletmenin merkezi olan "yüksek değerli bir bilgi işleme ve değerlendirme, saklama süreci" olarak kabul edilmektedir (Sveiby, 1997; Daveport, 1998).

Son yıllarda ekonomik ve demografik koşullar küresel ve ulusal sağlık sektörünün dijitalleşmesinde önemli ve hızlı bir artışa sebep olmuştur (Haux, 2006). Geçmiş yıllarda analog teknolojiye ve manuel bakıma bağlı olan endüstri, şimdi optimize edilmiş ve verimli tekniklerin ve daha az insan hatasının ana akım haline geldiği bir çağa girmiştir. Sağlık sektörünün dijitalleşmesi hem sağlık çalışanları hem de hastalara yardımcı olmak ve sağlık hizmetlerinin sunumunu iyileştirmek için kullanılan bilgi teknolojileri, hassas bilgilerin ve hasta kayıtlarının toplanması, depolanması ve bunların erişimi ile ilgili sorunların temelini bir yandan azaltırken, diğer taraftan yeni teknoloji ve gelişmelerden kaynaklı çeşitli güvenlik tehditlerine, saldırılara, güvenlik açıklarına, siber suçlara ve siber tehditlere maruz kalmasına da neden olmaktadır (Mehraeen ve ark., 2013).

Sağlık hizmeti verilerinin hassas doğası göz önüne alındığında, sağlık hizmeti sağlayıcılarının güvenilir bir bilgi güvenliği hizmetine sahip olması hayati önem taşımaktadır. Stratejiler sağlık hizmeti verilerine tepki vermeli aynı zamanda siber suçlular tarafından başlatılan saldırıları da öngörmeli, önlemeli ve korumalıdır. Son yıllarda siber suçlular elektronik tıbbi kayıtlarla ilgilenmekte olup bilgilerin karaborsa değeri kredi kartı numaralarından veya banka hesap şifrelerinden çok daha yüksek öneme sahiptir (Pick, 2021). Çünkü elektronik tıbbi kayıtlardaki verileri; hastaların isimleri, doğum tarihleri, adresleri, telefon numaraları, çalışma yerleri ve pozisyonları, kimlikleri, kart numaraları, sigorta, hastalık bilgileri, fiziksel kayıtlar, tıbbi test sonuçları vb. kişisel bilgileri toplu olarak içermektedir.

Bir işletmede toplanan bilginin önemi, en önemli varlıklarından biridir. Bu nedenle kapsamlı araştırmalar, bilgi ve bilgi sistemlerinin stratejik değerini vurgulamaktadır (Glazer, 1993; McFadzean ve ark., 2006; Nadiminti ve ark., 1996; Vanwegen ve DeHoog, 1996). Günümüzde bilgisayarlar günlük hayatımızın önemli bir parçası haline geldiğinden, veri güvenliğinin de kurumlar açsından öncelikler daha önemli hale gelmektedir. Esas olarak, düşüncelerin genellikle birinin hayatını kurtarmaya odaklandığı sağlık sektöründe, ancak tıbbi kayıtlar gibi özel verileri depolayan arayüzlere ve bilgisayar sistemlerine erişimi güvence altına almak, bilgi sızıntısı, bilgi ihlali, iç ve dış saldırılara karşı dikkate alınması gereken önemli bir durum olarak karşımıza çıkmaktadır. (Sağıroğlu ve Alkan, 2018). Güvenlik politikaları ve davranış kuralları, yöneticiler tarafından çalışanların güvenlik davranışlarını yönlendirmek ve kontrol etmek için sıklıkla kullanılan ana veya tek araçtır. Bir kuruluşun güvenlik politikaları ve prosedürleri, bilgi güvenliğinin nasıl yönetileceğine ilişkin temel varsayımları ve inançları içermektedir (Vroom ve Solms, 2004).

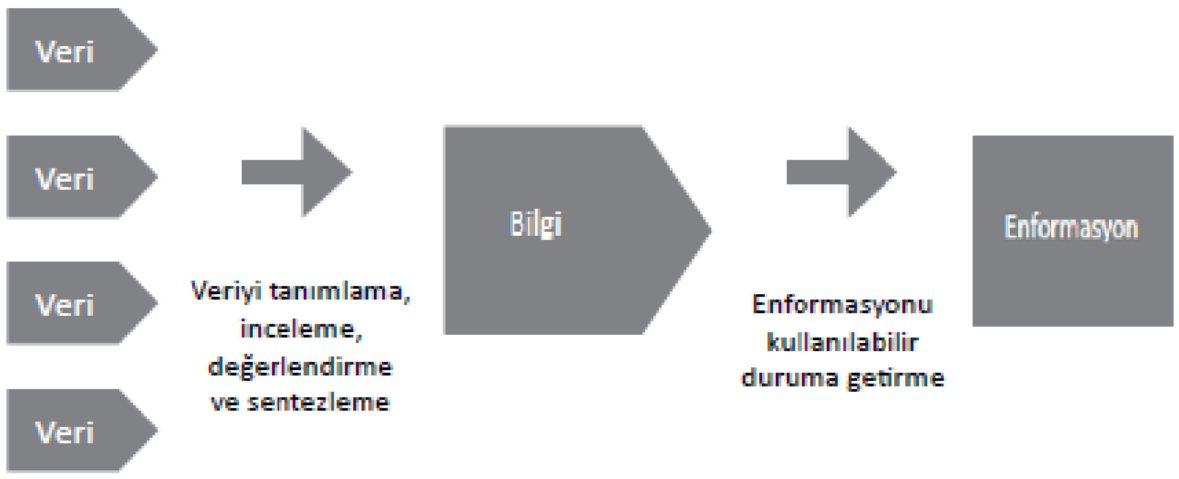
Bu çalışma, ISO27001 politikaları ve Sağlık Bakanlığı Bilgi Güvenliği Yönetmeliği hükümlerine göre zorunlu yasal politikalar ile prosedür uygulamalarının sağlık tesislerindeki bilgi işlem biriminde çalışanların farkındalığını ve uygulama süreçlerindeki bilgi güvenliği düzeylerini ölçmeyi amaçlamaktadır. Çalışmanın birinci bölümünde bilgi güvenliği kavramından ve bilgi güvenliği standardından bahsedilmiştir. İkinci bölümde ise sağlık kurumlarında bilgi, bilgi güvenliği ve bilgi teknolojileri tanımlamaları yapılarak bilgi güvenliği ve ihlal durumunda kurumların karşılaşabilecekleri maliyetler açısından incelemeler yapılmıştır. Üçüncü bölüm ise araştırmanın yapıldığı bölümdür. Çalışmanın amacı, yöntemi ve araştırma soruları bu bölümde açıklanmıştır. Anketlerin analizi yapılmıştır ve elde edilen bulgular bu bölüme eklenmiştir. Elde edilen bulgular tartışılmış ve sonuçlar ortaya konulmuştur.

2. GENEL BİLGİLER

2.1. Bilgi Güvenliği Kavramı

Yirmibirinci yüzyıl bilginin önemli bir stratejik kaynak haline geldiği bilgi çağıdır. Bilgi edinme, işleme ve güvenlik garantisi yeteneği, kapsamlı ulusal güçte kritik roller oynamaktadır ve bilgi güvenliği, ulusal güvenlik ve sosyal istikrar ile ilgili olarak yer almaktadır (Shen ve ark., 2007). Latince "datum" kelimesinin çoğul hali olan "veri", "verilmiş olan şeyler" anlamına gelmektedir. Kullanım için bir şekilde işlenmiş bilgi, genellikle bir bilgisayarda saklanan kayıtları ifade etmektedir (Buckland, 1991).

İşletmenin doğasındaki hızlı değişim ve gelişim nedeniyle, bir bilgi parçası başarının önemli bir faktörü olarak kabul edilmektedir (Qader ve ark., 2022). Bilgi, varlık ve teknolojinin önemi, modern organizasyonlar için temel farklılaştırıcı olarak giderek daha fazla kabul görmektedir (Stoll ve ark., 2013). Bilgi, sağlık hizmet uygulamalarında riskleri yönetmek için ek zorunluluklar ve sorumluluklar sunan günümüzün yüksek bağlantılı internet ve teknolojiye bağımlı ortamında sağlık hizmeti kuruluşlarının sürdürülebilirliği için kritik bir faktör olarak görülmektedir (Hammoda ve Durst, 2022).



Şekil 2.1. Verilerin Bilgiye Dönüşmesi (Yılmaz, 2014)

2.2. Bilgi Güvenliği Yönetim Sistemi (BGYS)

Bilgi yönetimi bir uygulamadır ve sadece bir teknoloji veya bir dizi metodoloji değildir. Bilgi yönetiminin üç ana bileşeni insan, süreç ve teknolojidir. Herhangi bir sağlık sektörünün 21. yüzyılda iyi bir uygulamaya sahip olması için, bu üç bileşenin yerinde olduğundan ve en iyi uygulamayı elde etmek için düzgün çalıştığından emin olmalıdır (Acharyulu, 2011).

İletişim medyasının giderek yaygınlaşması, elektronik depolama ve bilgi iletimi ile teknolojilerinin büyüme hızlarının katlanarak artmasından dolayı günlük hayatta olduğu kadar işletmelerde de elektronik uygulamaların artması, ağ sistemleri üzerinde bilgi paylaşımının yapılması, bilginin birçok noktadan erişilebilirliği hem kişisel hem de kurumsal kullanım için bilgi güvenilirliğine duyulan ihtiyaçı yıllar içinde artırmıştır (Yıldırım ve ark., 2011).

Dijital hasta kayıt süreçlerinin yoğun bir şekilde kullanılması, artan yasal düzenleme ve uygulamalar, hastalar, hizmet sağlayıcılar, sigorta ve sağlık primleri ödeme yapan sistemler arasında artan bilgi alışverişi, daha iyi ve güvenli bir bilgi güvenliği yönetimi ihtiyacına işaret etmektedir. Kuruluşlar, günümüzün yüksek ağ bağlantılı sistemler ortamında, ilgili her bir kişinin, kuruluşun, güvenlik vizyonunu paylaşmasını, rollerini ve sorumluluklarını anlamasını ve gerçekleştirmek için yeterince eğitilmesini sağlamadan bilgilerin güvenilirliğini, gizliliğini ve kullanılabilirliğini koruyamaz (ISO/IEC TR 13335-1, 2004, s. 14).

Bilgi yönetimi, bir organizasyonun entelektüel kaynaklarını yaratmak, depolamak, bunlara erişmek ve yaymaktır (Antunes ve Pinheiro, 2020). Bilgi güvenliği, kuruluşların bilgi kaynaklarının farkına varmak, faaliyetlerini tehlikeye atan riskleri en aza indirmek ve risk analizi yaparak bilgilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak için idari ve teknik önlemleri alma ve süreçleri düzenleyerek yönetme işlevidir (Silva ve ark., 2014; İleri, 2016).

Von (2001), bilgi güvenliğinin çok boyutlu karakteri yapısının bütüncül ve kapsamlı bir şekilde, tüm boyutları dikkate alınarak ele alınması gerekmekte olduğunu ve bilgi güvenliği boyutlarını;

•Stratejik/Kurumsal Yönetim Boyutu;

•Yönetişim/Örgütsel Boyutu;

•Politika Boyutu;

•En İyi Uygulama Boyutu;

•Etik Boyutu;

•Sertifikasyon Boyutu;

•Hukuki Boyutu;

•Sigorta Boyutu;

•Personel/İnsan Boyutu;

•Farkındalık Boyutu;

•Teknik Boyutu;

•Ölçüm/Metrikler (Uyumluluk Gözlem/Gerçek zamanlı BT denetimi) Boyutu;

•Denetim boyutu ’dur.

Bir bilgi güvenliği ekosistemi, insanları, süreçleri ve teknolojiyi destekleyen mantıksal, fiziksel ve ekonomik bileşenlere sahip olabilen belirli bir altyapı tarafından desteklenen sınırlı sayıda etkileşimli aracıdan oluşmaktadır (Ioannidis ve ark., 2016). Temel olarak, insanları, süreçleri ve bilgi teknolojisi sistemlerini içeren bilgi güvenliği yönetim sistemi; bir işletmenin bilgi güvenliğini bir risk değerlendirmesi yoluyla koruduğu kapsamlı bir yöntemdir (Bokhari ve Manzoor, 2022).

Bilgi güvenliği yönetim sistemi, bir işletmenin varlıklarının güvenliğini ve güvenilirliğini artırmak için sistematik olarak prosedürlerin oluşturulması, belgelendirilmesi ve sürekli yönetilmesi ve gerçekleştirilmesi için bir dizi süreç içerir. Bilgi güvenliğinin hedefleri olan bilgi gizliliği, bütünlüğü ve kullanılabilirliği ile bilgi güvenliğinin sürekli iyileştirilmesini içermektedir (Park ve ark., 2010). Bilgi güvenliği, altyapı varlıklarına ilişkin bilgilerin kayıp, kötüye kullanım, ifşa veya hasar risklerine karşı korunması ile ilgili faaliyetleri tanımlamaktadır. Yeterli bir güvenlik düzeyine ulaşılmasını, kaynakların verimli bir şekilde kullanılmasını ve en iyi güvenlik uygulamalarının benimsenmesini sağlamaya yardımcı olmak için bir dizi kıyaslama veya standarda ihtiyaç vardır (Sheikhpour ve Modiri, 2012; Von Solms,1999).

Bilgi teknolojisinin dinamikleri ve bilgi sistemlerinin artan karmaşıklığı, bilgi güvenliği yönetimine de yansımaktadır. Bilgi güvenliği standartları, kendilerini çeşitli görevler için genel çözümler olarak belirlemiştir (Milicevic ve Goeken, 2010). Bu bağlamda, Securityscorecard’a göre en çok kullanılan standart çerçeveler;

- Bilgi Teknolojisi için Kontrol Hedefleri (COBIT)
- Uluslararası Standardizasyon Ofisi (ISO) 27001
- Avrupa Birliği Siber Güvenlik Ajansı (ENISA) Ulusal Yetenek Değerlendirme Çerçevesi
- Bilgi Riski (FAIR) Siber Risk Çerçevesi

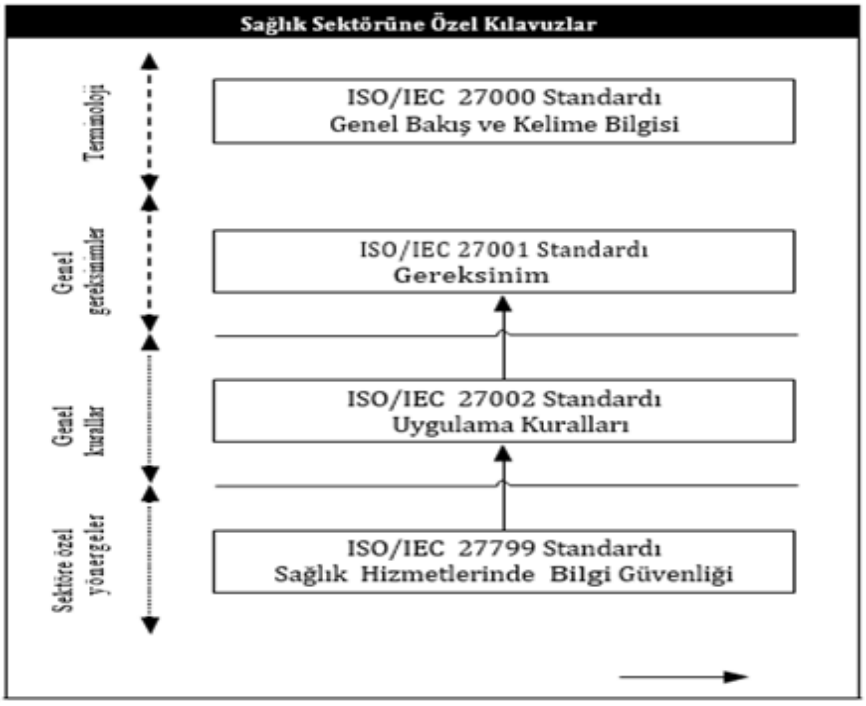
- Uluslararası Otomasyon Topluluğu (ISA/IEC 62443)
- Nesnelerin İnterneti (IoT) Siber Güvenlik Birliği (IOTCA)
- Ulusal Teknolojiler Enstitüsü (NIST)
- İnternet Güvenliği Merkezi (CIS)

Son yıllarda, bilgi güvenliği hedeflerine sistematik olarak uymaya yönelik genel olarak daha fazla ihtiyaç bulunduğu tüm sektörler tarafından fark edilmiş olup, sektör yöneticilerinin bilgi güvenliği risk yönetimi alanlarını desteklemek için çok sayıda araç ve yöntemin artırılması gerektiğini belirtmişlerdir (Brunner ve ark., 2020).

2.3. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi

ISO27001, bir bilgi güvenliği yönetim standardı olarak organizasyon yapılarını planlamayı, politika, süreçler, kaynaklar ve sertifikasyon programını içeren bir dizi uygulama ve kontrol sürecidir (Freeman, 2007; http://www.enisa.europa.eu). ISO27001, müşterilere, çalışanlara ve tedarikçilere, bilgi güvenliğinin anlaşma yaptıkları kuruluşlar için ciddi bir endişe kaynağı olduğu konusunda bilgilendirirken, bilgi güvenliği tehditleri ve sorunlarıyla başa çıkmak için önceden tanımlanmış süreçler de kuruluşun yönetim sisteminin ve iş kültürünün ayrılmaz bir parçasıdır.

Bilgi güvenliği yönetim sistemi (ISO 27001, 2005), sistem organizasyon yapılarını, planlamayı, politikayı, süreçleri ve kaynakları içeren; bir kuruluşta gizlilik, bütünlük ve kullanılabilirliği korumaya yönelik organize bir yaklaşım olan, Uluslararası Elektroteknik Komisyonu (IEC) ile ortaklaşa Uluslararası Standardizasyon Örgütü (ISO) tarafından yayınlanan, bilgi güvenliğine odaklanmış ve günümüzde en çok kabul edilen ISO/IEC tarafından yayınlanan uluslararası standarttır (Narayana ve ark., 2010). ISO / IEC 27002 geniş ve karmaşık bir standart olup, sağlık kuruluşlarına ve kişisel sağlık bilgilerinin diğer sorumlularına, bilgilerin gizliliğinin, bütünlüğünün ve kullanılabilirliğinin en iyi nasıl korunacağı konusunda rehberlik sağlamaktadır (www.iso.org). Ancak ISO 27799, ISO/IEC 27002'nin genel gereksinimleri tutarlı bir şekilde sağlık sektörü için uygun yönergeleri belirlemiştir.



Şekil 2. Sağlık Sektörüne Özel Kılavuzlar (Hamıdovıc ve Kabıl, 2011)

Bu standart hem ticari hem de devlet kuruluşları tarafından, kuruluşun politikasının yönetimi ve bilgi güvenliğinin uygulanması için temel olarak dünya çapında kullanılmaktadır (Sheikhpour ve Modiri, 2012). ISO 27001 sertifikasına sahip olmak, açık yönergelerin karşılanmasıyla birlikte bilgi güvenliğini yönetim kontrolü altına alır. Bilgi teknolojileri güvenliğini artırmak için oluşturulan yönergelerden bazıları, güvenlik olaylarına yanıt verme, çalışan işe alma, mobil cihaz yönetimi, ofis güvenliği, güvenli yazılım geliştirme, fidye yazılımı ve kötü amaçlı yazılım stratejileri ve daha fazlası içindir (Mcy, 2019).

ISO 27001 belgesi; kuruluşa rekabet avantajı sağlamakta ve bilgi güvenliği yönetim sisteminde dünya çapında kabul görmüş standartlara uyum sağlayabilmek için kuruluşun itibarını arttırmayı sağlamaktadır (Gillies, 2011). Bir bilgi güvenliği yönetim sistemi (BGYS), tüm politikaları, prosedürleri, belgeleri, kayıtları, planları, yönergeleri, anlaşmaları, sözleşmeleri, süreçleri, uygulamaları, yöntemleri, faaliyetleri, rolleri, sorumlulukları, ilişkileri, araçları, teknikleri, teknolojileri, kaynakları, kuruluşların bilgileri korumak, muhafaza etmek, bilgi güvenliği risklerini yönetmek, kontrol etmek ve iş hedeflerine ulaşmak için kullandıkları yapılardır (RM Studio).

ISO 27001 süreç yaklaşımı, çeşitli yasal gerekliliklere uyan tüm unsurları içerir, ancak bunları biraz farklı bir şekilde düzenlerken aşağıda yer alan adımlara göre yönlendirmektedir (Çubukçu, 2018).

1. Bilgi varlıklarını ve bunlarla ilişkili güvenlik gereksinimlerini tanımlayın.

2. Bilgi güvenliği risklerini değerlendirin.

3. Kabul edilemez riskleri yönetmek için ilgili kontrolleri seçin ve uygulayın.

4. Kuruluşun bilgi varlıklarıyla ilişkili güvenlik denetimlerinin etkinliğini izleyin, sürdürün ve artırın.

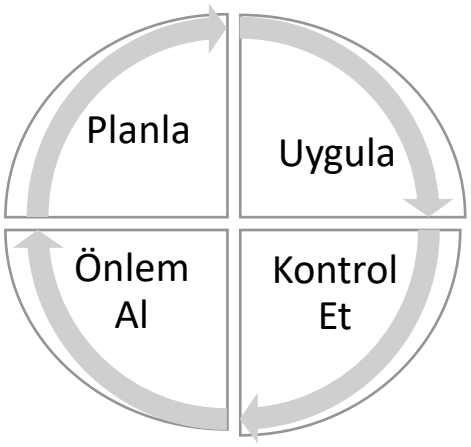
BGYS'nin kuruluşun bilgi varlıklarını sürekli olarak etkin bir şekilde korumasını sağlamak, risklerdeki veya kuruluşun stratejilerindeki veya iş hedeflerindeki değişiklikleri için bu adımların sürekli olarak tekrarlanması gerekmektedir (Humphreys, 2008).

ISO 27001 BGYS; bilgi varlıklarını korumaya yönelik spesifikasyonlar ve kontroller sağlamak, müşterilerin ilgili kuruluş üzerindeki bütünlüğünü ve güvenini artırmak için kuruluşta uygulanan bir bilgi güvenliği uyumluluk standartlarıdır. Kritik bilgileri koruma ve güvence altına alma bilinci için gereksinimleri ve sürecin yürütülmesine yönelik birçok organizasyonun BGYS'yi benimsemesine yol açmıştır (Maarop ve ark., 2016;Proença ve Borbinha, 2018; Von Solms, 1999).

2.3.1. ISO/IEC 27001 puko yaklaşımı

Küresel bilgi teknolojisi (BT) endüstrisi, BT ürünleri ve hizmetleri için güvenliğin kalitesini ve tutarlılığını artırmak ve iç ve dış saldırılardan korumak için bilgi güvenliği kültürünün gelişimini vurgulayan standartlara duyulan ihtiyacı kabul etmektedir (Özbilgin ve Özlü). Bu nedenle, Uluslararası Standardizasyon Örgütü / Uluslararası Elektroteknik Komisyon (ISO/IEC) 27000 serisi, bir kuruluşun bilgi güvenliği yönetim sistemi için gereksinimlere, güvenlik kontrollerine ve uygulama kılavuzu ile riskler için bir yönetim sistemedir (Carcary ve ark., 2016).Tanınan risklerle uğraşırken, risk kararı (kaçınmak, azaltmak, aktarmak, kabul etmek) parasal kriterlere göre belirlemek ve finansal durumlara yeniden kaynaklar gerektiren uygun önlemlere göre kurumlar için planlama yapmaktadır (Blakley ve ark., 2001).

ISO / IEC 27001, tüm işletmelerin "can damarı" olan organizasyonların bilgi varlıklarını korumak için geliştirilmiştir (Humphreys, 2005). ISO/IEC 27001, bir kuruluşun BGYS'sini kurmayı, uygulamayı, izlemeyi ve etkinliğini artırmayı amaçlayan (Şen ve Yerlikaya, 2013) ve ülkemizde PUKO döngüsü olarak tanımlanan ISO 27001, Şekil 3'te gösterildiği gibi BGYS'nin uygulanmasında "Planla – Uygula –Kontrol et – Önlem al" modeli kullanılmaktadır (Marttin ve Pehlivan, 2010)



Şekil 3. PUKÖ Döngüsü Modeli (Anonim)

1. **Plan (Plan):** BGYS'yi geliştirmek için planlama oluşturmak bir adımdır. Riski yönetmek ve bilgi güvenliğini artırmak için güvenlik politikası, itirazlar, süreçler ve prosedürler oluşur.
2. **Uygula (Do):** Güvenlik politikasını oluşturmak, kontrollerini, süreçlerini ve prosedürlerini uygulanması ve denetimlerin gerçekleştirilmesi
3. **Kontrol Et (Check):** Güvenlik politikası, hedefleri ve BGYS uygulamasının etkinliğini kontrol etmek ve gözden geçirmek için bir adımdır. (Etkinlik ve Verimlilik notkası)
4. **Önlem (Act):** BGYS'nin döngüsünü sağlamak için yönetim tarafından yapılan incelemelere göre sürecin sürdürülmesi ve iyileştirilmesi, sistemin bakımı, detaylandırılması ve değiştirilmesi noktasıdır.

ISO27001 BGYS yaşam döngüsü birkaç aşamadan oluşmaktadır (Pavlov ve Karakaneva (2011). Bunlardan ana sekizi aşağıda tanımlanmıştır:

1.Risk tedavisinin planı, süreçlerin, prosedürlerin ve kontrollerin dokümantasyonu.

2.Planın uygulanması.

3.Kontrollerin uygulanması.

4.Planlanan kontrol etkinliğinin değerlendirilmesi için metodolojinin uygulanması.

5.BGYS ile çalışan çalışanların eğitimi.

6.Sistemin konuşlandırılması.

7.İşleyiş kontrollerinin test edilmesi ve sistemin denetimi.

8.Güvenlik olaylarına karşı tepki için prosedürlerin ve kontrollerin tanıtılması.

ISO 27001 süreci olarak adlandırılan "Plan-Yap-Kontrol Et-Harekete Geç" modeline göre (Beckers ve ark., 2012) *Planlama* aşamasında bir BGYS kurulur, *Uygula* aşamasında BGYS'ler uygulanır ve işletilir, *Kontrol et* aşamasında BGYS'ler izlenir ve gözden geçirilir ve *Önlem al* aşamasında BGYS'ler korunur ve geliştirilir. Kısaca ISO 27001'de *Plan* aşamasında, BGYS'nin, ilgili taraflarının, çevrenin, varlıkların ve ilgili tüm teknolojinin kapsamı risk değerlendirmeleri ve sınırları tanımlanır.

CISCO' ya göre; bilgi güvenliği yönetim sistemi, bir veri ihlali senaryosunda kuruluşlara yardımcı olmak için oluşturulmuş bir dizi yönerge ve süreçtir. İşletmeler, resmi bir dizi yönergeye sahip olarak riski en aza indirebilir ve personel değişikliği durumunda iş sürekliliğini devam ettirebilir. ISO 27001, bir şirketin BGYS'si için iyi bilinen bir özellik olarak tanımlamaktadır.

2.3.2. ISO/IEC 27001 Bgys ana maddeler ve kontroller

ISO 27001:2013 Ek A, 14 kontrol kategorisinde gruplandırılmış 114 kontrol içerir. 14 kategorinin her biri ve o kategorinin birincil amacı veya hedefleri hakkında net bir açıklama sunarken sürecin sadece bilgi teknoloji güvenliği alanında olmadığı sürecin bir bütün olarak tüm yönleri ile değerlendirilmesi gerektiği belirler (Adsivera, 2022; Shojaie ve ark., 2014).

Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi, 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 40 ıncı maddesinin birinci fıkrasına dayanılarak hazırlanmıştır. Sağlık Bakanlığı'nın merkez ve taşra teşkilatı ile bağlı kuruluşlarda görev yapan tüm personelin; bilginin işlenmesi süreçlerinde bilgi güvenliğinin sağlanmasına yönelik tedbir almak; bilginin gizlilik, bütünlük ve erişilebilirlik kapsamında değerlendirilerek içeriden veya dışarıdan kasıtlı ya da kazayla oluşabilecek tüm tehditlerden korunmasını sağlama amaçlamaktadır. Yürütülen faaliyetlerin etkin, doğru, hızlı ve güvenli olarak gerçekleştirilmesinde bilgi güvenliği faaliyetleri kapsamında uyulması gereken usul ve esaslarını herhangi bir nedenle Bakanlık bilgi ve bilgi işleme tesislerine erişim yetkisi verilenleri, bilgi sistemlerini, insan kaynaklarını, fiziksel ve çevresel güvenlik sistemlerini, hizmet sağlayıcılarını, sistem, veri ve bilgi kullanıcılarını ve kurallarının usul ve esasları tanımlamayı kapsamaktadır.

Bakanlık Makamının 02/05/2018 tarihli ve 98813779.719.54 sayılı onayı ile yayımlanan Bilgi Güvenliği Politikaları Yönergesinin eki olarak Bilgi Güvenliği Politikaları Kılavuzu yayımlanmıştır. Kılavuz hazırlanırken kişisel verilerin ve özellikle kişisel sağlık verilerinin kullanımı ve korunmasına ilişkin hususlara ilişkin mevzuat da dikkate alınmış ve ISO 27001 standardı başlıkları altında işlenebilecek hususlar, önemli ölçüde kılavuza aktarılmış olup (Bilgi Güvenliği Politikaları Kılavuzu, 2018) Tablo 2.3.2. de ISO 27001 Ek-A Kontrol Maddeleri Açıklamaları ve Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu İle karşılaştırma Tablo 2.3.2.1 kısaca ve özetle temelde aşağıdaki konu başlıklarını içermektedir.

Tablo 2.3.2.1. ISO 27001 Ek-A Kontrol Maddeleri Açıklamaları ve Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu İle Karşılaştırma Tablosu

ISO 27001 Ek-A Kontrol Maddeleri ve Açıklamaları		**Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu Maddeleri**
Bilgi Güvenliği Politikaları (Madde A.5)	Kuruluşun bilgi güvenliği uygulamalarıyla birlikte giden politikalar ele alınır. Kurumun gereksinimleri ile birlikte yasalar çerçevesinde düzenlemeler yapılır	A.1.1. Temel Prensipler A.1.2. Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu A.1.3. Kurumsal BGYS Politikalarının Oluşturulması ve Uygulanması
Bilgi Güvenliği Organizasyonu (Madde A.6)	Çalışanların kuruluş içerisinde hangi görevlerden sorumlu olması gerektiğine göre kuruluş içindeki bilgi güvenliği uygulamalarının yönetimini ve işletilmesini ele alır.	A.2.1. Bakanlık Bilgi Güvenliği Yönetim Komisyonu A.2.2. Sağlık Bakanlığı Sektörel SOME A.2.3. Bilgi Güvenliği Alt Komisyonları A.2.4. Bilgi Güvenliği Yetkilisi A.2.5. Kurumsal SOME Ekip Lideri ve Kurumsal SOME'ler A.2.6. Üst Yönetimlerin Sorumluluğu
İnsan Kaynakları Güvenliği (Madde A.7)	İşe alım ve fesih işlemlerine yönelik sürecini güvenlik çerçevesi içerisinde ele alır.	A.3.1. İşe Alma Öncesinde Yapılacak Kontroller A.3.2. Çalışma Esnasında Uygulanacak Kontroller A.3.3. Bilgi Güvenliği Teknik ve Farkındalık Eğitimleri A.3.4. Görev Değişikliği veya İşten Ayrılma İçin Uygulanacak Kontroller A.3.5. Kullanıcıların Bilgi Güvenliği Sorumlulukları A.3.6. Elektronik Posta Güvenliği A.3.7. Sosyal Mühendislik ve Sosyal Medya Güvenliği
Varlık Yönetimi (Madde A.8)	Her türlü bilgi güvenliği varlıklarının kullanıcı sorumlulukların belirlenmesini ve korunmasına yönelik süreçleri belirler	A.4.1. BGYS Bakış Açısıyla Varlıklar A.4.2. Varlık Envanterinin Tespiti A.4.3. Bilgi Sınıflandırma/Gizlilik Derecelerinin Verilmesi A.4.4. Taşınabilir Ortam Yönetimi A.4.5. Ortamın Yok Edilmesi

Tablo 2.3.2.1. ISO 27001 Ek-A Kontrol Maddeleri Açıklamaları ve Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu İle Karşılaştırma Tablosu Devamı

Erişim Kontrolü (Madde A.9)	Çalışanların erişim sorumluklarına yönelik süreçleri belirler	A.6.1. Erişim Kontrol Politikası A.6.2. Kullanıcı Erişimlerinin Yönetimi A.6.3. Parola Güvenliği A.6.4. Sağlık Bakanlığı Uygulamalarına OGN A.6.5. Merkezi Aktif Dizin ve E-Posta Sistemine Erişim A.6.6. Veri Merkezi ve Sunucu Barındırma Hizmetlerine Erişim A.6.7. Merkezi Veri Tabanı Yönetim Sistemi A.6.8. Elektronik Belge Yönetim Sistemi A.6.9. Kimlik Paylaşım Sistemine Erişim Bilgi Güvenliği Politikaları Kılavuzu 2 A.6.10. e-Nabız, USS Bilgi Yönetim Sistemi ve KDS Raporlarına Erişim A.6.11. Halk Sağlığı Yönetim Sistemine Erişim A.6.12. Merkezi Web İçerik Yönetim Sistemi A.6.13. Sağlık Bilişim Ağına Erişim A.6.14. Uzaktan Çalışma ve Erişim
Kriptoloji (Madde A.10)	Veri şifrelemesi ile ilgili süreçleri belirler	A.7.1. Kriptografik Politikalar A.7.2. Kriptografik Araç ve Yöntemler
Fiziksel ve Çevresel Güvenlik (Madde A.11)	Fiziksel alanlara erişim ile tesis güvenliğine yönelik süreçleri belirler.	A.8.1. Genel Hususlar A.8.2. Güvenli Alanlar A.8.3. Ekipman Güvenliği
İşletim güvenliği (Madde A.12)	Verilerin toplanması, saklanması ve iletilmesine yönelik prosedür ve işlemleri belirler	A.9.1. Yazılı İşletim Prosedürleri A.9.2. Değişiklik Yönetimi A.9.3. Kapasite Yönetimi A.9.4. Geliştirme, Test ve İşletim Ortamlarının Ayrılması A.9.5. Etki Alanı Kurulum ve Yönetimi A.9.6. Sunucu ve Sistem Güvenliği A.9.7. Ağ İşletim Güvenliği A.9.8. Veri Tabanı Güvenliği A.9.9. Yazılım Güvenliği A.9.10. Sunucu/Sistem Odası Güvenliği A.9.11. Tıbbi Cihaz Güvenliği A.9.12. İz Kayıtları (Log) Yönetimi A.9.13. Yedekleme Yönetimi A.9.14. Teknik Açıklık Yönetimi A.9.15. Sistem Güvenlik Testleri
Haberleşme güvenliği (Madde A.13)	Her türlü iletişim noktasından iletilen bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini korumakla ilgili süreçlerini belirler	A.10.1. Ağ Güvenliği A.10.2. Uç Nokta (Yerel Alan Ağı) Ağ Güvenliği A.10.3. Kablosuz Ağ Güvenliği A.10.4. Veri Aktarımı Güvenliği A.10.5. Gizlilik Sözleşmeleri A.10.6. Veri Aktarım Anlaşmalar
Sistem Temini Geliştirme ve Bakımı (Madde A.14)	Bu bölümdeki kontroller, yeni bilgi sistemleri satın alırken veya mevcut olanları yükseltirken bilgi güvenliğinin dikkate alınmasını sağlar.	Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzunda bu bölüme ilişkin bilgi bulunmamaktadır
Tedarikçi ilişkileri (Madde A.15)	Kuruluşlar ve üçüncü taraflar arasındaki etkileşimler ile ilgili hizmet düzeyini bilgi güvenliğini belirler.	A.11.1. Mal ve Hizmet Alımları Güvenliği A.11.2. SBYS Firmaları ile İlişkilerde Dikkat Edilecek Hususlar

Tablo 2.3.2.1. ISO 27001 Ek-A Kontrol Maddeleri Açıklamaları ve Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu İle Karşılaştırma Tablosu Devamı

Bilgi güvenliği ihlal olayı yönetimi (Madde A.16)	Bilgi güvenliği olay müdahalesinin yönetim sürecini belirler	A.12.1. İhlal Bildirimi ve Olay Yönetimi A.12.2. Kanıt Toplama
İş Sürekliliği Yönetiminin Bilgi Güvenliği Yönü (Madde A.17)	Kesinti durumunda bilgi güvenliği iş süreçlerinin sürdürülmesini yönelik süreçleri belirler	A.13.1. İş Sürekliliği Genel Yaklaşımı Bilgi Güvenliği Politikaları Kılavuzu A.13.2. İş Sürekliliği Adımları A.13.3. İş Sürekliliği Stratejisi Belirleme A.13.4. İş Sürekliliği Planı Oluşturma A.13.5. İş Sürekliliği Planlarını Tatbikatlar ile Test Etme
Uyum (Madde A.18)	Yasal süreçlere uyumluluk noktasındaki süreçleri belirler	A.14.1. Yasal Gereksinimlere Uyum A.14.2. Lisanslama ve Fikri Mülkiyet Hakları A.14.3. Kişisel Verilerin Korunması Mevzuatı A.14.4. 5651 Sayılı Kanun ile Uyum A.14.5. Bilgi Güvenliği Denetimler

2.4. Sağlık Kurumlarında Bilgi

Çoğu kuruluşla yaptığımız hemen hemen her işlem ve etkileşim, adımız, adresimiz ve doğum tarihimiz gibi kişisel verileri paylaşmamızı içermektedir. Bir web sitesini her ziyaret edildiğinde, internette bir şey aranıldığında veya satın alındığında, sosyal medyayı kullanımı veya bir e-posta gönderildiğinde veriler çevrimiçi olarak da paylaşılmaktadır (ICO, 2022).

02.05.2018 tarihli ve 98813779.719.54 sayılı oluru ile onaylanmış ve yürürlüğe giren Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi'n de; bilgi: kurum için değeri olan, uygun bir şekilde korunması gereken, yazılı veya sistemler üzerinde işlenen tüm kaynakları olarak tanımlanmaktadır. Sağlık bilgisi insan bilgisidir (Omri ve ark., 2021). Sağlık bilgileri yönetimi, kaliteli hasta bakımı sağlamak için hayati önem taşıyan dijital ve geleneksel tıbbi bilgileri edinme, analiz etme ve koruma uygulamasıdır. İşletme, bilim ve bilgi teknolojisinin birleşimidir (Ahıma, 2022). Sağlık endüstrisi, gelişmiş bilgi ve formasyon kaynakları tarafından desteklenen bir işletmeden genişletilmiş bir işletmeye dönüşmüştür. Günümüzün bilgi-teorik sağlık işletmelerinde, bilgi 'yüksek değerli bir bilgi biçimi' olarak kabul edilmektedir (Davenport ve ark., 1998).

Bilgisayar sistemlerinin ortaya çıkışı ve potansiyeli ile birlikte, sağlık sistemlerindeki tüm klinik muayenelerin ve tıbbi kayıtların dijitalleştirilmesi günümüzde standart ve yaygın olarak benimsenen bir uygulama haline gelmiştir. 2003 yılında, Tıp Enstitüsü olarak bilinen Ulusal Bilim, Mühendislik ve Tıp Akademileri'nin bir bölümü, sağlık sektörünü hastaların ve klinisyenlerin yararına geliştirmek için tutulan kayıtları temsil etmek üzere "elektronik sağlık

kayıtları" terimini oluşturdu (Reisman, 2017; Dash ve ark., 2019). Tüm sağlık sistemi sektörlerinde elektronik sağlık bilgileri oluşturulur, kullanılır, serbest bırakılır ve yeniden kullanılır (Schmit ve ark., 2017).

Amerika Birleşik Devletleri Sağlık ve Sosyal Hizmetler Bakanlığı'na bağlı Hastalık Kontrol ve Korunma Merkezi (CDC) Elektronik sağlık kayıtları, sağlık bilgi alışverişi, yaşamsal kayıtlar, bağışıklama bilgi sistemleri, sendromik sürveyans sistemleri ve diğer halk sağlığı veri tabanları gibi sağlık bilgi kaynakları, belirli popülasyon sağlık ihtiyaçları ve halka hitap etmekten sorumlu uygulayıcılara etkili müdahaleler hakkında kritik öneme sahip veriler sağlamaktadır. Sağlık sektörü doktorların ve hastaların sağlık geçmişinin manuel kayıtlarını tuttuğu, zaman geçtikçe bu manuel kayıtların yerini elektronik kayıtların aldığı ve artık günümüzde hasta kayıtlarının elektronik olarak internetin kullanıldığı her yerden erişilebilen veri tabanı deposunda saklamak için kullanılan bir sistemin uygulama sürecindeyiz (Jigna ve ark., 2019).

Dünya Sağlık Örgütü'ne (2016) göre dijital sağlık, sağlık hizmetlerinin kalitesini ve etkinliğini artırmada, sağlık sisteminin hastalar için maliyetini düşürmede ve klinik araştırmalarda önemli bir etkiye sahip, hızla genişleyen bir tıp alanı olmaktadır. Dijital sağlık, hastaların izlenmesi, teşhis, yönetim, önleme, rehabilitasyon ve uzun vadeli bakım sunumunun etkinliğini artırmayı amaçlayan multidisipliner bir alan olarak tanımlamaktadır. Bu nedenle sağlık sektöründe dijital teknolojilerin uygulamaları çeşitlilik göstermektedir (Greaves ve ark., 2018).

Teknolojik gelişmeler, son yıllarda toplumların ve iş ortamının endüstriyel bir ekonomiden bilgi ekonomisine dönüşümünü sağlamıştır (Vial, 2019). Bilgi yoğun faaliyetlerin, yenilikçi eylemlerin ve teknolojik ilerlemenin bir kombinasyonu, dijital merkezli stratejilerle desteklenen yenilikçi ürün ve hizmetlerle sonuçlanmıştır (Garcia-Perez ve ark., 2022). Özellikle küresel sağlık hizmetleri ekosisteminin paydaşları ve "değerli, yeni ve öngörülemeyen yetenekler üretebilen" parçalar arasında yeni bilgi üretmek için sürekli karmaşık bir ortamda etkileşim halindedir (Secundo ve ark., 2019).

Amerikan Sağlık Bilgi Yönetimi Derneği (AHIMA), sağlık bilgileri, semptomlar, teşhisler, prosedürler ve sonuçlar dahil olmak üzere bir kişinin tıbbi geçmişiyle ilgili verilerdir. Bir sağlık kaydı, bir hastanın geçmişi, laboratuvar sonuçları, röntgenler, klinik bilgiler, demografik bilgiler ve notlar gibi bilgileri içerir. Bir hastanın sağlık bilgileri, hastanın

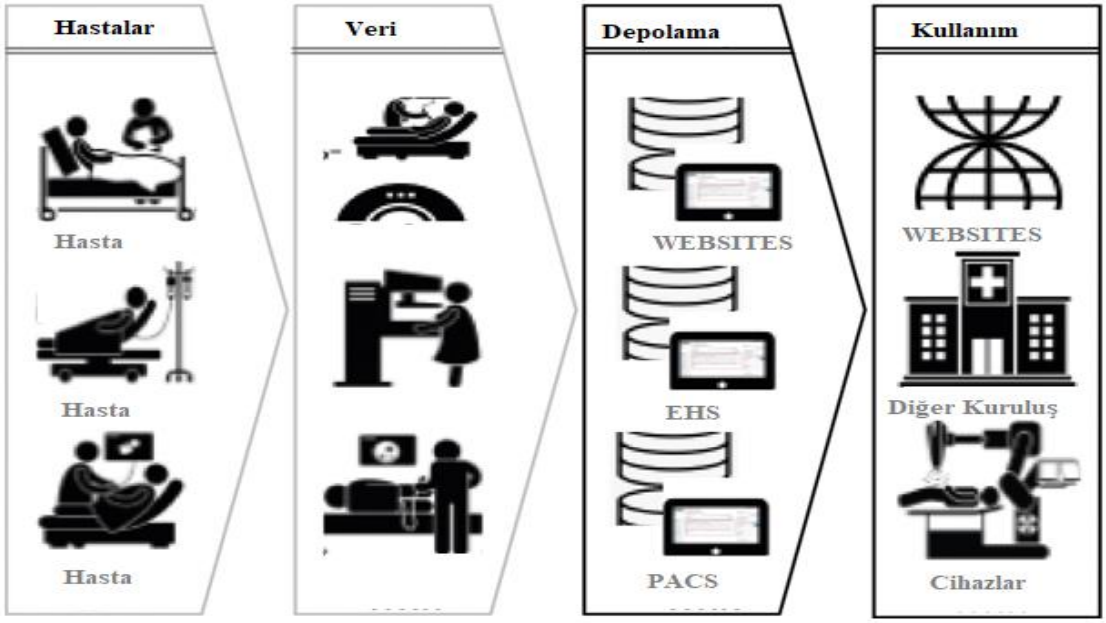
sağlığının nasıl değiştiğini görmek için ayrı ayrı görüntülenebilir; bir popülasyonun sağlığının nasıl değiştiğini ve tıbbi müdahalelerin sağlık sonuçlarını nasıl değiştirebileceğini anlamak için daha büyük bir veri setinin parçası olarak da görmektedir.

Avustralya Bilgi Komiserliği Ofisi (OAIC) tarafından sağlık bilgileri, sağlığınız veya engelliliğiniz hakkında herhangi bir kişisel bilgi olarak tanımlarken hastalık, yaralanma veya sakatlık hakkında bilgi veya görüş içermekte olarak tanımlamaktadır. Ayrıca bazı sağlık bilgileri örnekleri şunları içerir:

- Belirtilerin veya teşhis notları,
- Aldığınız veya alacağınız bir sağlık hizmeti hakkında bilgi,
- Uzman raporları ve test sonuçları,
- Reçeteler ve diğer ilaç alımları,
- Diş kayıtları,
- Genetik bilgileri,
- Gelecekteki sağlık hizmetleri ile ilgili durumlar,
- Olası organ bağışı ile ilgili detaylar,
- Randevu ve fatura detayları,
- Bir sağlık hizmeti sağlayıcısın sizinle ilgili diğer kişisel bilgiler,

Sağlık sektöründeki tipik bir bilgi akışı; hasta sağlık kayıtları, tanı ve tedavi sunumu dışında bir dizi amaca hizmet eder (Larson ve ark., 2020). Örneğin, bilgi, sağlık sistemi içindeki verimliliği artırmak, kamu politikası geliştirme ve yönetimi yönlendirmek ve tıbbi araştırmaların yürütülmesinde kullanılabilmektedir (Eichler ve ark.,2019; Oner, 2014) Bir hastanın tıbbi kayıtları, verilen hizmetlerin ödenmesini yapmak için ödeme yapan kuruluşlarla (örneğin, özel sigorta veya Sosyal Güvenlik Kurumları) da paylaşılır. Sağlık hizmeti sağlayıcıları, operasyonlarını yönetmek ve hizmet kalitesini artırmak için elde edilen kayıtları da kullanmaktadır. Ayrıca, sağlayıcılar sağlık bilgilerini bakım hizmetlerini kolaylaştırmak için diğer sağlık paydaşları aracılığıyla paylaşabilmektedir.

Sağlık sektörü bilgi paylaşımı, idari maliyetlerin düşürülmesi ve bakım kalitesinin iyileştirilmesi için hastaneler, klinikler, eczaneler ve müşterilerle bağlantılı olan bilgi tabanlı bir topluluk haline gelmektedir. Bu nedenle, sağlık hizmetlerinin başarısı kritik olarak klinik, faturalama ve kullanım bilgilerinin veya bilgisinin kurumsal sınırlar içinde ve ötesinde toplanmasına, analizine ve sorunsuz değiş tokuşundan dolayı profesyonel bilgiye güvenmektedir (Bose, 2003).



Şekil 4. Tıbbi alandaki veri akışının bir modeli (Razaque, 2019)

Sağlık işletmeleri; elektronik tıbbi kayıtlar, klinik araştırma verileri, hastane kayıtları, idari raporlar gibi büyük miktarda veri ürettikleri için bilgi ve bilgi yönetimi teknolojilerinin bir araya getirilmesinden dolayı 'veri zengini' olarak kabul edilmektedir (Abidi, 2001). İnternet teknolojisinin hızla gelişmesiyle birlikte, büyük veri analizinin giderek tıp endüstrisine nüfuz etmesi elektronik kayıtlar, hastane bilgi yönetim sistemleri, radyolojik görüntüleme sistemleri ile tıbbi bilgini dijitalleşmesi süreciyle birlikte veriler ortaya çıkmaktadır. İlgili alanlardaki uzmanlar, tıp alanındaki verilerin yıllar içinde kat ve kat artacağını belirtmektedir (Stankovic, 2016).

2.5. Sağlık Kurumlarında Bilgi Güvenliği

Veri ihlalleri, ihlal oluşumları ve ihlal riski alanları ile ilgili olaylara ve faktörlere odaklanan risk yönetimi ve sağlık hizmeti güvenliği sağlamak için birçok önemli sağlık yasasının, güvenlik çerçevesinin ve ulusal bilgi işlem girişimlerinin odak noktası olmuştur (McLeod ve Dolezel, 2018). Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesi'n de; Bilgi güvenliği: Bilgi ve bilgi işleme tesislerinin emniyetli ve güvenilir olarak kullanılabilmesi, bütünlüğünün ve gizliliğinin muhafazası ve yetkisiz şahısların bilgiye ulaşmaları halinde tespit edilmelerine yönelik tedbirlerin tümünü ifade ederken; Bilgi güvenliği yönetim sistemi: Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak üzere sistemli, kuralları koyulmuş, planlı, yönetilebilir, sürdürülebilir, yazılı hale getirilmiş, kurumun yönetimince

kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütününü olarak tanımlanmaktadır.

İşletmelerin bilgisayar tabanlı sistemlere ve ağlara artan bağımlılığı göz önüne alındığında, sistemlerin güvenlik açıkları çok fazladır (Choobineh ve ark 2007). Bilgi güvenliğinin temel amacı, farklı kurumsal güvenlikle ilgili tehditlerin ve kurumsal güvenlik açıklarının neden olabileceği durumları yok etmek veya zararın etkilerimi en aza indirmek için uygun kontrol önlemlerini uygulamaktır (Enisa, 2014).

Bilgi güvenliği, bir kuruluşun bilgi teknolojisine bağımlılığıyla orantılı olarak önemlidir (Blakley ve ark., 2001). Sağlık bilgi sistemleri çok çeşitli dijital teknolojileri kapsamaktadır ve hasta kaydı, veri izleme, laboratuvar testleri ve radyoloji gibi hemen hemen tüm süreçlerde sağlık tesisi için olmazsa olmaz bir uygulama durumundadır (Luna ve ark., 2016). Hastalık teşhis ve tedavileri büyük ölçüde tıbbi ekipman ve alanlara bağlı olduğundan, sağlık tesislerinin hastalara daha güvenli ve kesintisiz hizmet sunmasını sağlaması gerekmektedir (Demirdöğen ve ark., 2021). Küresel ve ulusal sağlık hizmetleri ekonomik, demografik ve teknolojik koşullara bağlı olarak büyük değişiklikler halindedir. Günümüz teknolojilerinde sürekli olarak sağlık hizmetleri için yeni tıbbi teknoloji biçimleri ve uygulamaları eklenmektedir. Eklenen her yeni teknolojik uygulama sayesinde bilgisayarlı ya da bilgisayarsız bir sistem tarafından farklı biçimlerdeki bilgi elde edilmekte olup, sağlık hizmetleri için elde edilen her bilgiyi yönetmek açık bir zorunluluk haline gelmiştir. Kuruluşlar bilgisayar ağlarını internete veya iş ortaklarının BT ağlarına bağladıkça, BT sistemleri ve kullanıcıları üzerindeki merkezi kontrol ve dolayısıyla bilgi güvenliği büyük ölçüde kaybolabilmektedir (Solmas, 1999). Artık bu bilgiler elektronik ve çok sayıda ağda mevcut olduğundan, bir mahremiyet ihlali milyonlarca insanı etkileme potansiyeline sahiptir (Abouelmehdi ve ark., 2017)

Bilgi güvenliği, saldırılar karşısında bilginin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak için araçlar ve mekanizmalar sağlamayı amaçlamaktadır. İlk bakışta, bilgi güvenliği, korunması gerekenler ile çevresi arasındaki ayrıma dayanıyor gibi görünmektedir. Gizli bilgiler "dışarı" çıkmamalı ve yetkisiz bilgiler "içeri" girmemelidir (Pieters, 2011). Sağlık hizmeti teknolojisinin sürekli gelişmesine rağmen, bir hasta sağlık kayıt sisteminin uygulanması ve sistemlerin hassasiyeti nedeniyle hala önemli bir zorluk teşkil etmektedir. Hasta verilerinin çeşitli sağlık tesislerinde saklanması ve paylaşılmasının yanı sıra, sistem verilerinin çeşitli sağlayıcılar arasında zorunlu dağılma eğilimi de vardır. Çoğu hasta elektronik sağlık kayıt sistemi, hasta bilgilerini depolamak ve iletmek için merkezi bir yönetim

yapısı kullanırken hassas bilgileri bir başka sağlık tesisine mahrem bilgileri aktardığı için endişeleri mevcut olmaktadır (Kumar ve ark., 2022).

Tüm dünyada sağlık hizmetleri yöneticileri, sınırlı bütçeler kullanarak hizmet kalitesini artırmanın yollarını aramaktadır. Mobil uygulamaların ve tele sağlık cihazlarının kullanımı, veri toplama, veri paylaşımı ve iş birliği dahil olmak üzere sağlık hizmetlerinin çeşitli yönlerini geliştirmenin yolları olarak görülmektedir. İnternet üzerinden birden çok taraf arasında ve birden çok kanal aracılığıyla artan miktarda veri paylaşımı, siber güvenliği optimize etmenin yeni yollarını gerektirken farkındalıklarda artmaya devam etmektedir (Petersilge, 2020). Elektronik sağlık kayıtlarına ve birbirine bağlı cihazlara hızlı geçiş, siber güvenliğe geçmişten gelen ve sürekli yatırım yapılmaması ve sağlık personelinin güvenlik geçici çözüm davranışlarının anlaşılmaması, sağlık sektörünü saldırılara karşı savunmasız bırakmıştır (Coventry ve Branley, 2018).

Ancak günümüz dünyasında hasta verileri ile çalışanlarının mahremiyeti korunması, saklanan verilerin güvenliği konusunda endişeli olmakla birlikte bu verileri korumak için asgari standartları sürdürmeleri gerekmektedir (Vora ve ark., 2019). Bilgi, sağlık kuruluşlarının varlıklarını devam ettirebilmeleri için hayati önem taşır ve bilgi güvenliği yönetimi süreci yoluyla güvence altına alınması zorunludur (Peltier, 2016).

Sağlık hizmetlerinde büyük veri analitiği birçok fayda taşır, vaat eder ve sağlık hizmetlerini dönüştürmek için büyük bir potansiyel sunar, ancak çok yönlü engeller ve zorluklar ortaya çıkarmaktadır. Sağlık hizmetleri veri güvenliği ve ayrıcalığı konusundaki endişeler yıldan yıla artmaktadır. Ek olarak, sağlık kuruluşları reaktif bir güvenlik ve gizlilik gereksinimlerinin belirlenmesinde aşağıdan yukarıya, teknoloji merkezli yaklaşım, kuruluşu ve hastalarını korumak için yeterli değildir (White Paper, 2011).

2.6. Sağlık Kurumlarında Bilgi Teknolojileri

Tüm kuruluşlar, sadece hayatta kalmak için değil, aynı zamanda günümüzün son derece rekabetçi küresel pazarlarındaki büyümeleri ve genişlemeleri için de bilgi teknolojisi kaynaklarına bağımlıdır (Eloff ve Solms, 2000). Sağlık hizmetleri bilgi teknolojisi, dünya çapında verilerin elektronik olarak saniyeler içinde depolanmasına ve dağıtılmasına izin vermektedir (Altameem ve ark., 2022). Çok çeşitli sağlık hizmeti veri teknolojilerinin sorunsuz entegrasyonu, yalnızca klinik ve organizasyonel süreçler hakkında daha derin içgörüler elde etmemizi sağlamakla kalmaz, aynı zamanda hastaların daha hızlı ve daha güvenli bir şekilde

hizmet almasını kolaylaştırırken, güvenliğini, bakım kalitesini ve genel hasta deneyimini iyileştirmeye yardımcı olmaktadır (Abouelmehdi ve ark., 2018).

Sağlık bilgi teknolojisi, basit çizelgelemeden daha gelişmiş karar desteğine ve tıbbi teknolojiyle entegrasyona kadar uzanan çeşitli teknolojileri içermektedir. Sağlık bilgi teknolojisi, elektronik doktor reçeteleri, klinik karar desteği sistemleri, e-reçete yazma, elektronik oturum kapatma ve devretme araçları, barkodlu ilaç yönetimi, akıllı pompalar, otomatik ilaç dağıtım dolapları, elektronik ilaç yönetimi, hasta veri yönetim sistemleri, malzemeler için RFID sistemler, hasta elektronik portalları, teletıp, elektronik olay raporlama ve elektronik tıbbi kayıt gibi uygulamalar sağlık hizmetlerini iyileştirmek ve dönüştürmek için sayısız fırsat sunarken; insan hatalarını azaltmak, klinik sonuçları iyileştirmek, bakım koordinasyonunu kolaylaştırmak, uygulama verimliliklerini artırmak ve zaman içinde elde edilen verileri izlemek için onlarca sistemi sağlık hizmetlerinde kullanmak için sunmaktadır (Alotaibi ve Federico, 2017).

Günümüzde sağlık hizmetlerinin yüksek kalitede performans, verimli, eşit ilkeler, karşılanabilir ve erişilebilir hedeflere ulaşmada sağlık sistemleri altyapısının etkisi büyük olmasına rağmen bu hedeflere ulaşmada sağlık sistemlerinin performansını etkileyen sağlık hizmetlerinde durmaksızın devam eden dijitalleşme süreci ile birlikte gerçekleşen teknolojik değişimlerdir (Ricciardi, 2019). Son on yılda bilgi teknolojilerinin inanılmaz şekilde büyümesi ile beraber, bu teknolojilerin hızlı bir şekilde sağlık hizmetlerine entegrasyonu sayesinde ve sağlık hizmeti maliyetlerinin düşürülmesi, sağlık hizmeti kalitesinin iyileştirilmesi, hasta güvenliğinin sağlanması ve tıbbi hataların azaltılmasına yönelik artan baskılar sonucu sağlık bilgi sistemlerinin kullanımının artmasına neden olmuştur (Meier ve ark., 2013; Agarwal ve ark., 2011).

Dünya Sağlık Örgütüne göre sağlık bilgi sistemleri, sağlık sisteminin her seviyesindeki karar vericilerin sorunları ve ihtiyaçları belirlemelerini, sağlıkla ilgili kanıta dayalı kararlar vermelerini sağlamak için bilgi üretimi olarak özetlenebilecek çok sayıda kullanıcıya ve çok çeşitli amaçlara hizmet etmektedir şeklinde tanımlanmaktadır (WHO, 2022). Sağlık teknolojileri yaşamları uzatma, kurtarma ve iyileştirme potansiyeline sahiptir (Dimitrov, 2016). Sağlık sektöründeki hızlı değişim ve gelişim, tıbbi teknoloji ve tedavi yöntemlerindeki karmaşıklık, ileri uzmanlığa sahip çok sayıda sağlık çalışanlarının bir arada çalışması, hastaların sağlık hizmetlerinden bekledikleri kalite seviyesindeki artış, sağlık sektöründe harcamaların giderek artması ve ekonomik darboğazalar gibi etkenler, sağlık hizmetlerinin en

düşük maliyetle en yüksek kalitede sunabilmek amacıyla teknolojik değişim ve ilerlemeyi zorunlu kılmaktadır (İleri, 2018).

Büyük ve orta ölçekli sağlık kuruluşlarının bilgi teknolojisi gereksinimleri, yalnızca büyük veri kümeleri veya çok sayıda kullanıcı nedeniyle değil, aynı zamanda sürekli gelişen hastane bilgi sistemleri (HBS) nedeniyle karmaşık olmaktadır. Hem şirket içi hem de uzak dahili kullanıcılar ve hastalar için birçok faktörlerin yanı sıra, artan ağ hızları ve bant genişlikleri ve tıbbi cihazların geliştirilmesine yönelik uluslararası standartların varlığı, bu cihazların diğer tıbbi cihazlar ve sistemler ile hem aynı kuruluş içinde hem de farklı kuruluşlarda yüksek düzeyde birlikte çalışabilirlik ve bağlanabilirlik sağlamak durumunda kalmıştır. Bilgi sistemlerinin bu geniş kapsamı ve karmaşıklığı, bu sistemlerin güvenlik gereksinimlerine doğrudan yansır (Sönmez ve ark., 2022)

Bilgi teknolojileri alanında cihazlar ve yazılımlar gelişmeye devam ettikçe sağlık hizmetlerinde dokümantasyon, bilgi toplama ve karar vermeyi süreçlerini iyileştirme, kolaylaştırmakta ve kullanıcılar açısından daha verimli çalışma rutinleri ve bilgi yönetimi sağlayarak sağlık hizmetlerinin kalitesini ve verimliliği artırmaya devam edecektir. Sağlık hizmetlerinin iyileştirilmesi ve dönüştürülmesi için insan hatalarının azaltılması, klinik sonuçların iyileştirilmesi, bakım koordinasyonunun kolaylaştırılması, uygulama verimliliğinin artırılması ve zaman içinde verilerin izlenmesi dahil olmak üzere çok sayıda fırsat sunmaktadır. Sağlık hizmetleri teknolojileri, basit çizelgelemeden daha gelişmiş karar desteğine ve tıbbi teknolojiyle entegrasyona kadar değişen çeşitli teknolojileri içerir (Askari-Majdabadi ve ark., 2019)

Sağlık hizmetlerinin dijital dönüşümü yıkıcı olabilmektedir; ancak nesnelerin interneti, sanal bakım, uzaktan izleme, yapay zekâ, büyük veri analitiği, blok zinciri, akıllı giyilebilir cihazlar, platformlar, veri alışverişi ve depolaması sağlayan araçlar ve uzaktan veri yakalama ve veri alışverişi ve paylaşımını sağlayan araçlar gibi teknolojiler sağlık ekosistemi genelinde bir bakım sürekliliği oluşturan ilgili bilgiler, tıbbi teşhis, veriye dayalı tedavi kararları, dijital terapötikler, klinik denemeler, bakımın kendi kendine yönetimi ve kişi merkezli bakımın yanı sıra daha fazlasını oluşturarak sağlık sonuçlarını iyileştirme potansiyeline de sahiptir (WHO 2021b).

Günümüzdeki teknolojiler sayesinde cihazların birbirine bağlanabilirliği artmakta, geleneksel olarak bağımsız olarak çalışan sistemler artık sağlık tesisi ağına entegre olarak

kullanıcılarına hizmet vermektedir. Tıbbi cihazların birlikte çalışabilirliği ve birbirine bağlanabilirliği, sağlık sektöründe daha önce bilinmeyen siber güvenlik sorunları yaratır (Jara ve ark., 2013). Geçmişte, tıbbi cihazlar genellikle hastane ağına bağlı olmayan bağımsız cihazlardı. Ağ dışı faktörlerden kaynaklanan durumlara karşı hala hassas olmalarına rağmen, bu cihazların siber güvenlik riskleri muhtemelen günümüzün ağa bağlı cihazlarıyla karşılaştırıldığında daha azdı. Hastane ağına daha fazla tıbbi cihaz bağlandıkça, daha önce eski cihazlarda görülmeyen sorunlara maruz kalmaktadırlar. Hazır yazılımlara, özellikle ticari işletim sistemlerine (örn. Microsoft Windows sürümleri) dayanan cihazlar, kötü amaçlı yazılımlar ve virüsler gibi çok çeşitli tehdide karşı da savunmasızdır (Coronado ve Wong, 2014).

Sağlık yöneticileri, kurumlarında bilgiyi daha hızlı ve doğru şekilde toplayabilmek, bu bilgiyi sistematik süreçlerle depolamak, bilgiye gereksinim duyan ve erişim yetkisi olan taraflara zaman ve konum sınırı olmadan iletebilmek böylelikle elektronik bilgi iletişim sistemlerinin getirdiği verimlilik, etkinlik, hız ve rekabetçilik unsurlarından en üst seviyede yararlanabilmek için giderek daha fazla sağlık bilişim sistemlerine yatırım yapmaktadırlar (Kara, 2022).

BT, sosyal ve teknolojik değişikliklerden kaynaklanan gelişen paradigma değişimi, küresel sağlık sistemi taleplerini etkili bir şekilde karşılayabilecek ve aynı zamanda gelecekteki eğilimlere hitap edebilecek yenilikçi bir bilgi tabanlı sağlık sistemi geliştirme ihtiyacı yaratmıştır. Hastane bilgi yönetim sistemi, hastane bilgilerinin sadece sınır içinde değil, aynı zamanda tele-tıp veya e-sağlık hizmetleri gibi hastane sınırlarının ötesinde de işlenmesi ve yönetilmesinde geliştirilmiştir. Sağlık hizmetleri, hasta refahı konusundaki ezici endişe nedeniyle bilgi yönetimine diğer endüstrilerden daha fazla bağlı olabilir (Acharyulu, 2011).

Endüstri 4.0 uygulamalarındaki kapsamlı teknolojik gelişmelerle birlikte, hassas sağlık bilgileri yetkisiz kullanıcılar tarafından erişilmeye, kopyalanmaya ve/veya manipüle edilmeye karşı giderek daha savunmasız hale gelmektedir. Sağlık hizmetlerinde insanların artık giyilebilir cihazlar anlayışı, geleneksel internet üzerinden insandan nesneye, nesneden nesneye veya nesneden nesneye iletişim sağlayan veya tedarik eden herhangi bir hizmeti sağlayan bir anlayıştır. Bu aktörler arasındaki bağlantılar ve iletişim nedeniyle, bir endişe kaynağı haline gelen bilgi veya şeylerin güvenliğine ve mahremiyetine yönelik birçok potansiyel tehdit ve saldırı altındadır (Hughes-Lartey ve ark., 2021).

2.7. Dünya'da Bilgi Güvenliği Politikaları

Bilgi güvenliği konusunda uluslararası alan da uygulanan politikalar incelenmiş, sırasıyla Türkiye, Avrupa Birliği, İngiltere, Kanada ve ABD gibi ülkelerin bilgi güvenliği politikalarının yönelik genel bilgiler bu bölümde verilmiştir**.**

Türkiye'de veri korumayı kapsayan ana mevzuat, 7 Nisan 2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu'dur (KVKK). Kanun, öncelikle AB Direktifi 95/46/EC'ye dayanmaktadır. Bu Kanunun amacı, kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemektir. Kanun hükümleri, kişisel verileri işlenen gerçek kişiler ile bu verileri tamamen veya kısmen otomatik olan ya da herhangi bir veri kayıt sisteminin parçası olmak kaydıyla otomatik olmayan yollarla işleyen gerçek ve tüzel kişiler hakkında uygulanmaktadır (Mevzuat KVKK, 2016)

Avrupa Veri Koruma Yönetmeliği (GDPR, 2022), Avrupa çapında veri gizliliği yasalarını uyumlu hale getirmek için tüm üye devletlerde 25 Mayıs 2018 tarihinden itibaren geçerli olmak üzere bir Avrupa Birliği yasadır. AB üye devletlerindeki yaşayan bireylerin kurum ve kuruluşlar tarafından kişisel verilerin korunmasını gerektiğini ve AB vatandaşlarının verilerini işleyen herhangi bir kuruluşun uyması gereken usul ve esasları belirlemektedir.

GDPR'ye göre sağlıkla ilgili kişisel veriler, ilgili kişinin geçmiş, şimdiki veya gelecekteki fiziksel veya zihinsel sağlık durumuna ilişkin bilgileri ortaya koyan, ilgili kişinin sağlık durumuna ilişkin tüm verileri içermektedir. GDPR şirketlerin şunları yapmasını zorunlu kılmaktadır:

- Veri ihlali bildirimleri sağlamak,
- Bir veri koruma görevlisi atamak,
- Veri işleme için kullanıcının onayını sağlamak,
- Gizlilik için verileri anonimleştirmek,

İngiltere de Veri İşleme Sözleşmesi (DPA) 01 Ocak 2021'de Avrupa Birliği (Çekilme) Yasası 2018 kapsamındaki düzenlemelerle yürürlüğe giren bir Birleşik Krallık yasasıdır. Kolluk kuvvetleri ve istihbarat teşkilatları hariç, Birleşik Krallık'ta kişisel verilerin işlenmesine yönelik temel ilkeleri, hakları ve yükümlülükleri belirler. Birleşik Krallık veri koruma çerçevesi ile Avrupa Birliği ayrılma süreci öncesi ve sonraki çerçevesini belirlemektedir. Yasa kapsamında genel bir veri işleme rejimi, kolluk kuvvetleri ve istihbarat teşkilatları için ayrı bir

veri koruma rejimi ve yedi bölümden oluşacak şekilde kişisel verilerin işlenmesine ilişkin hükümler düzenlemiştir (Data Protection Act, 2018).

Kanada da Kişisel Bilgileri Koruma ve Elektronik Belgeler Yasası (PIPEDA), özel sektör kuruluşları için federal gizlilik yasasıdır. PIPEDA kapsamında, kişisel bilgiler, kimliği belirlenebilir bir kişi hakkında kaydedilmiş olsun ya da olmasın, gerçeklere dayalı veya öznel bilgileri içerir. Bu, aşağıdakiler gibi herhangi bir biçimdeki bilgileri içerir:

- Yaş, isim, kimlik numaraları, gelir, etnik köken veya kan grubu;
- Görüşler, değerlendirmeler, yorumlar, sosyal statü veya disiplin cezaları;
- Çalışan dosyaları, kredi kayıtları, kredi kayıtları, tıbbi kayıtlar, bir tüketici ile bir tüccar arasında bir anlaşmazlığın varlığı, niyetler (örneğin, mal veya hizmet satın alma veya iş değiştirme).
- PIPEDA, ticari bir faaliyet sırasında kişisel bilgileri toplayan, kullanan veya ifşa eden Kanada genelindeki özel sektör kuruluşları için geçerlidir.

Bir kişinin sağlık veya sağlıkla ilgili bilgilerini yöneten kuruluşlar, bunu ancak o kuruluş amaçlarını ayrıntılı bir şekilde açıkladıktan sonra o kişinin rızasıyla yapabilir. PIPEDA uyumluluğu arayan kuruluşlar, yasanın "on adil bilgi ilkesini" karşılamakla yükümlüdür (RSI Security, 2020).

Amerika Birleşik Devletleri Sağlık ve İnsan Hizmetleri Bakanlığı (HIPAA) tarafından, " Gizlilik Kuralı " olarak da anılan 1996 yılında Sağlık Sigortası Taşınabilirlik ve Hesap Verebilirlik Yasası olarak kabul edilen kanun, tıbbi bilgi yönetimini sigorta ve sağlık faturalarıyla ilgili amaçlar için standartlaştırmıştır. Gizlilik, bireylerin sağlık bilgilerinin uygun şekilde korunmasını sağlarken, yüksek kaliteli sağlık hizmeti sağlamak ve teşvik etmek ve halkın sağlığını ve refahını korumak için gereken sağlık bilgilerinin akışına izin verme hedefine sahiptir. Korunan sağlık bilgileri, şekli ne olursa olsun bir hasta veya çalışanın tıbbi kayıtlarıyla ilgili herhangi bir bilgi olarak tanımlanırken, tamamen dijitalleştirilmiş kuruluşlar, tıpkı kâğıt dosyaları yönetirken yaptıkları gibi yasal düzenlemelere uymak zorundadır. HIPAA'ya göre bir bireyin tıbbi kayıtları, tedavileri, ödemeleri ve sağlık koşullarını (geçmiş, şimdiki ve gelecekteki) içerdiğinden dolayı sağlık bilgileri oldukça hassas bilgiler olarak tanımlarken elektronik sağlık kayıtlarının nasıl işleneceğine ilişkin bir protokol ile sağlık kuruluşlarının veri ve bilgilerin güvence altına alır (Sidhu 2018). Bu nedenle, sağlık bilgileri ile ilgili ayrıcalıklı şirketler, katı gizlilik ve siber güvenlik standartlarını karşılamalıdır. Yasa ayrıca bazı

kuruluşların hastalardan ve çalışanlardan gerekenden daha fazla sağlıkla ilgili bilgi toplamasını da engellemekte olup sağlık sigortası şirketleri, sağlık bakım kuruluşları, sağlık hizmeti sağlayıcıları ve herhangi bir işletmeye dış kaynaklı hizmet sağlayan iş ortakları ve bağlı kuruluşların politikalarına ve prosedürlerine uyması gereken kuruluşlardır. (HIPAA, 2022; CDC,2022)

2.8. Sağlık Alanında Bilgi Güvenliği İhlal Örnekleri Ve İhlal Maliyeti

Sağlık kuruluşları, bilgi güvenliği sorununun ölçeğini ve etkisini anlamaya başlamaktadır. Sağlık kurumları karar vericileri, verilerinin ve sistemlerinin güvenliğini sağlamayla ilgili çok sayıda teknik ve ekonomik sorunla karşı karşıya kalmaktadır (Derrick ve ark., 2014).

Sağlık sektörünün dijital dönüşümü, toplumların bilgi teknolojileri alanındaki radikal yeniliklerle dayalı bir ekonomiye geçerken sağlık ve bakım ekosistemindeki en son teknolojilerin ve uygulamalarının benimsemektedir. Ancak sağlık hizmetlerinde siber güvenlik zorluklarına dayanıklı ve sürdürülebilir bir dijital dönüşüme yönelik stratejik vizyonu tanımlaması gereken temel kavramlara ilişkin hâlâ sınırlı bir anlayış bulunmaktadır (Garcia-Perez ve ark., 2022). Tüm kuruluşlar, hassas bilgilerini hedef alabilecek çeşitli bilgi güvenliği saldırılarına maruz kalabilir (Ionescu ve ark., 2018). Sağlık tesislerinin yukarıda açıklanan riskleri azaltmanın önemini anlaması gerekir. Siber güvenlikle ilgili cihaz arızası nedeniyle tesislerin geçici olarak kapatıldığı olaylar yaşanmıştır (Coronado ve ark., 2014).

Bir bireyle ilgili en hassas veri, sağlık verileridir. Sağlık verilerini sağlamak için birçok uyum standardı, kuralı ve tutarlılık gerekliliği olmasına rağmen, koruma ve güvenlik kesintileri, elektronik tıbbi hizmetler çerçeveleri için önemli endişeler olmaya devam etmektedir (Vaishnav ve ark., 2022). Sağlık sektöründeki siber güvenlik tehditleri, hassas sağlık bilgilerinin artan değeri ve dijitalleştirilmiş sağlık sistemlerinde mevcut olan hasta verileri ve sağlık hizmetlerinin zayıf siber güvenlik savunması ve kurum yöneticilerinin bu alandaki farkındalığı sağlık hizmetlerine yönelik siber saldırılar nedeniyle günümüzde sağlık verilerinin korunmasının önemi ve zorunluluğu artmaktadır (Offner ve ark., 2020). Sağlık kurumları, herhangi bir siber güvenlik ihlalinin kişisel olarak tanımlanabilir tıbbi bilgilerin ifşa edilmesine neden olabileceği, acil durum veya hayat kurtarıcı bakım da dahil olmak üzere klinik hizmetleri ciddi şekilde kesintiye uğratabileceği veya can kaybına neden olabilecektir. Güvenlik ihlalleri sonucunda kısa ve uzun vadeli ekonomik ve yasal etkileri olmaktadır (Bhuyan ve ark., 2020)

2.8.1. Bilgi güvenliği ihlal örnekleri

Günümüzde bilgi teknolojileri alanında gerçekleşen gelişmelere paralel olarak (Tonta, 1999) hem sağlık kuruluşun bilgileri hem de hasta bilgilerinin korunması (Esatoğlu ve Köksal, 2010) ya da kolay erişim sağlanabilmesi adına çevrimiçi olarak veya mobil cihazlarla erişim sağlamak adına sağlık sektörü içerisinde bilgilerinin güvende tutulmasına yardımcı olmak için bilgi teknolojileri güvenliği etrafında birçok zorunlu yasal politika ve prosedür düzenlemesi oluşturulmuştur (Kayrak, 2012).

Teknolojideki hızlı değişimler ve kuruluşların operasyonlarının dijitalleşmesi, işletmelerin işlerini sürdürmede yeni zorluklarla karşı karşıya bıraktı. Bu zorunlu ve hızlı değişiklikler, kuruluş yönetiminin bilgilerini ve varlıklarını korumaya daha fazla dikkat etmesini gerektirirken diğer yandan işletme bilgilerini ve varlıklarını güvenceye almak, amaçlarına ve hedeflerine ulaşmak için bilgi güvenliğine daha fazla yatırım yapılmasını gerektiğini tespit etmiş ya da deneyimlemişlerdir (Posey ve ark., 2015).

Kişisel veriler gibi hassas verilerin güvenlik ihlali, son yıllarda düzenli olarak meydana gelen bir olgu haline gelmektedir. Bu güvenlik ihlalleri, kuruluşların bilgi sistemlerine sızmak için farklı yollarla saldıran kötü niyetli siber aktörler tarafından gerçekleştirilmektedir (Floyd ve ark., 2016). Veri ihlalleri bireylere ve kuruluşlara çeşitli şekillerde zarar verebilir. Veri hırsızlığı durumlarında kuruluşların uğraşmak zorunda kaldığı büyük finansal gerilemenin yanı sıra, bu tür durumlar aynı zamanda kuruluşların imajını zedeleyerek itibarlarını ve marka değerlerini zedelemektedir. Veri ihlalleri genellikle dahili ve harici olmak üzere iki ana kategoriye ayrılmaktadır (Seh ve ark., 2020);

- **Dahili veri ihlalleri**, sistem içerinde çalışan personelin yardımıyla meydana gelen olaylardan oluşmaktadır. Örneğin; ayrıcalığın kötüye kullanılması, yetkisiz erişim/ifşa etme, gereksiz ama hassas verilerin uygunsuz şekilde elden çıkarılması, kayıp veya hırsızlık veya gizli verilerin yetkisiz bir tarafla kasıtsız olarak paylaşılması vb.

- **Harici veri ihlalleri** ise herhangi bir harici varlık veya kaynağın neden olduğu olaylar olarak tanımlanmaktadır. Örnek olarak, kötü amaçlı yazılım saldırısı, fidye yazılımı saldırısı, kimlik avı, casus yazılım gibi herhangi bir bilgisayar korsanlığı/BT olayları vb.

Seh ve ark., (2020)'nın yapmış oldukları çalışmaya göre kişi ve kuruluşların veri varlıklarının risk altında olduğunu özellikle sağlık sektörü veri mahremiyeti ve gizliliği açısından saldırganlar tarafından hedef alınan en savunmasız sektör olarak görülmektedir. Sağlık hizmeti verileri, diğer veri türlerinden daha hassastır, çünkü herhangi bir veri tahrifatı hatalı tedaviye, hastalarda ölümcül ve geri dönüşü olmayan kayıplara neden olabilmektedir. Bu nedenle, sağlık hizmeti verilerinin gelişmiş güvenliğe ve ihlallere karşı korumalı olmaya ihtiyacı vardır.

Bir insan hatası genellikle kullanıcıların ve çalışanların yanlış bilgilendirilmesinden kaynaklanır. İnsanlar farkındalık eksikliği nedeniyle şirketlerini ve kişisel verilerini tehlikeye atabilir. İnsan hatası, siber güvenlik ihlallerinin önde gelen nedeni olarak görülmektedir. 2021 yılı "IBM Siber Güvenlik İstihbarat Endeksi Raporu"na göre bu ihlallerin %95'inden çalışanların sorumlu olduğu bilinmektedir (IBM, 2021). Bilgi güvenliği yönetimindeki en önemli zorluklardan biri, organizasyonel, bireysel ve teknik faktörlerin birlikte bir organizasyonda bilgi güvenliğinin sonuçlarını nasıl etkilediğini anlamaktır. Ancak günümüzde medyada bilgisayar korsanları ve suçlular sıklıkla manşetlere konu olsa da kanıtlar daha fazla bilgi güvenliği olayının dahili çalışan eylemlerinin bir sonucu olarak ortaya çıktığını göstermektedir (Hu ve ark., 2012).

Seh ve ark., (2020) Sağlık Hizmetleri Veri İhlalleri: İçgörüler ve Etkileri adlı çalışmasında sağlık hizmeti veri ihlallerini ve bunların nedenlerini ile sonuçlarını incelemiştir. Araştırma kapsamında küresel olarak kabul görmüş kuruluşların Ponemon Enstitüsü'nün veri ihlali maliyetleri hakkındaki raporları ve Verizon (2022) şirketinin veri ihlalleri hakkındaki çalışmaları ele alınarak hazırlanmış rapora göre;

Tablo 2.8.1.1. 2005-2019 Yılları Veri İhlali Sektörel Dağılımı

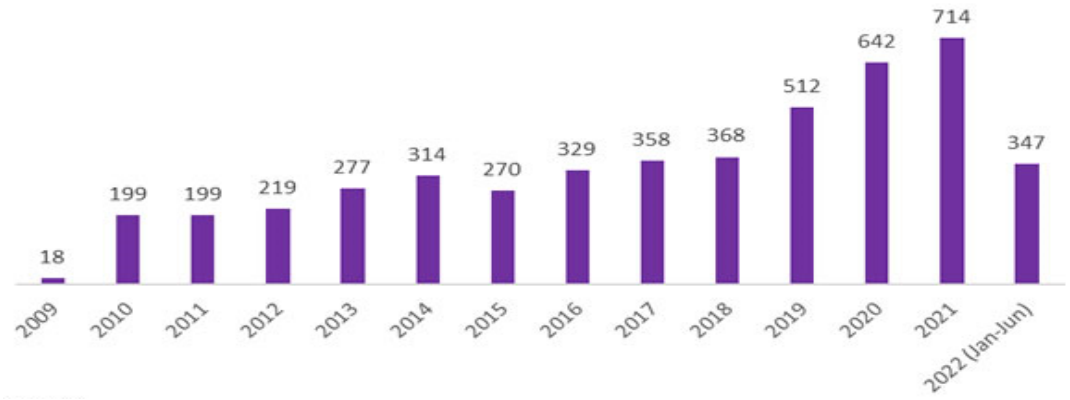
Sektör	Son 15 Yıl Veri İhlali (2005-2019)	Son 5Yıl Veri İhlali (2015-2019)
	İhlal Sayısı(n)	İhlal Sayısı(n)
Eğitim	671	64
Finans	410	194
İşletmeler	426	113
Sağlık/Hizmet Sağlayıcılar	3912	1587
Online Firmalar	561	45
Devlet Kurumları	75	7
Sivil Toplum Kuruluşları	300	62
Toplam	**6355**	**2072**

Kaynak: (Ponemon ve Verizon, 2022)

- 15 yıllık zaman diliminin kapsamlı bir analizinde, sağlık sektörünün hem (2005'ten 2019'a) hem de (2015'ten 2019'a)kadar olan zaman dilimlerinde veri ihlallerinde en yüksek seviyeyle karşı karşıya kaldığını göstermektedir. 2005-2019 yılları arasında bildirilen 6355 ihlal olayından 3912'si yalnızca sağlık sektöründe kaydedilirken toplam ihlal oranının %62'sini oluşturmaktadır.

- Sağlık sektörünü, sırasıyla eğitim ve diğer kamu kurumları izlemektedir. Sağlık sektörünün karşılaştığı 3912 veri ihlal olayından 1587'si son beş yılda (2015-2019) gerçekleşirken bu da son tespit edilen sağlık hizmeti veri ihlallerinin %41'ini oluşturmaktadır.

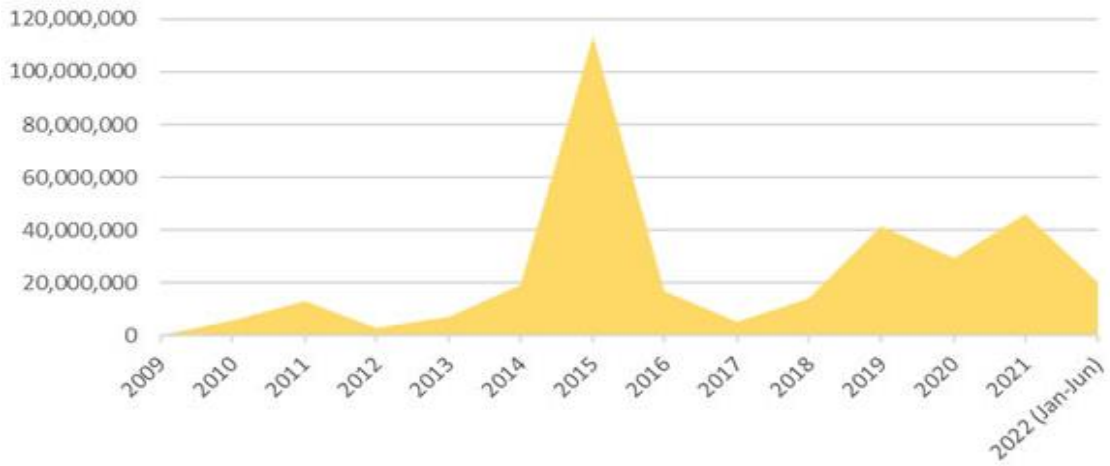
Siber saldırılar, hassas hastane operasyonlarının gecikmesine ve kesintiye uğramasına neden olur ve hastaların hayatlarını riske atar (Argaw ve ark. 2020). Mayıs 2017'deki küresel WannaCry saldırısının ölçeği benzeri görülmemiş bir büyüklükte olup WannaCry, dünya çapında 300.000'den fazla bilgisayara bulaşarak kullanıcıların bitcoin fidyeleri ödemesini talep etti. İngiltere'deki 50 hastane, MRI tarayıcıları ve kan depolama buzdolapları gibi bağlı cihazlarda sistem çapında arızalar, hasta bakımında gecikmeler ve sistemlerde işlev kaybı yaşanmıştır. Bu saldırı spesifik olarak sağlık kuruluşlarına yönelik olmamasına karşın saldırının yaygınlığından dolayı etkilenmiştir. Ancak diğer fidye yazılımları özellikle sağlık sektörünü hedef almıştır (Scott ve Wingfield, 2017).



Şekil 5. Amerika 2009-2021 arasında Yıllara Göre Veri İhlal Dağılımı(Hipaajournal, 2022)

ABD 'de 2009 ile 2021 arasında, 500 veya daha fazla sağlık kaydı içeren toplam 4.419 sağlık hizmeti veri ihlali gerçekleşmiştir. Bu ihlaller, 314.063.186 sağlık hizmeti kaydının kaybolması, çalınması, ifşa edilmesi veya izin verilmeyen şekilde ifşa edilmesiyle sonuçlanmıştır. ABD'nin 2021 nüfusunun %95'ine denk gelen bu oran 2018 yılına kıyasla

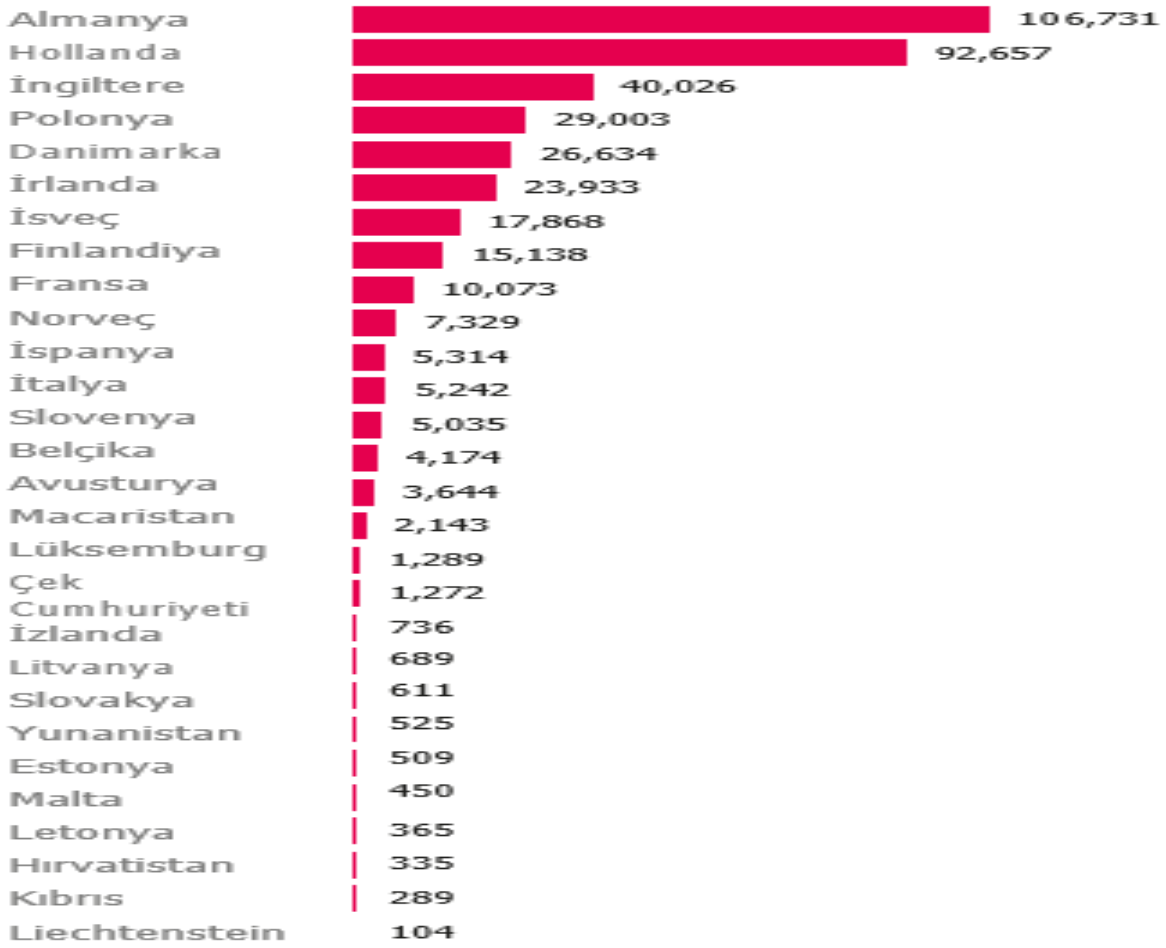
günde yaklaşık 1 oranında 500 veya daha fazla kaydın sağlık hizmeti veri ihlali rapor ediliyorken bu oran 2021'de 1,95 sağlık hizmeti veri ihlali rapor edilmektedir (HIPPA).



Şekil 6. ABD 2009-2021 arasında Veri İhlali Etkilenen Kişi Sayısı (Hipaajournal)

Her yıl ifşa edilen kayıt sayısında genel bir artış eğilimi olmuştur. 2015 yılı içerisinde, ifşa edilen, çalınan veya izin verilmeyen 113 milyondan fazla kaydın ihlal edilmesi ile yaklaşık 78 milyon kişinin verileri ihlal edilmiş olup ABD tarihindeki en büyük ihlal olarak kayıtlara geçmiştir (Fortune, 2015).

ABD tıbbi fatura ve borç tahsildarı American Medical Collection Agency (AMCA), bir veri ihlalinin ardından iflas koruması için başvuruda bulundu. AMCA, 1 Ağustos 2018 ile 30 Mart 2019 arasında olduğu tahmin edilen bir zaman diliminde hacklendi ve bunun sonucunda birçok kurumsal müşterilerin bilgilerin çalındığını, en az 20 milyon ABD vatandaşının, ad/soyadı, sosyal güvenlik numaraları, adresleri, doğum tarihleri ve ödeme kartı bilgileri dahil olmak üzere kullanıcı ihlalden dolayı etkilendiği bildirilmiştir (Osborne, 2019).



Şekil 7. Veri İhlal Bildirimi (GDPR, Mayıs 2018-Ocak 2022)

25 Mayıs 2018'de AB Genel Veri Koruma Yönetmeliği'nin (GDPR) uygulanmasından bu yana dördüncü yıllık DLA Piper para cezaları ve veri ihlali anketi çalışma kapsamında ki dönemler içerisinde Almanya ve Hollanda toplam ihlal bildirimi sıralaması içerisinde en başta yer almaktadır. Raporun devamında her 100 bin nüfus ortalamasına göre 150 vaka sayısı ile Hollanda ilk sırada yer almaktadır.

ABD Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA), hassas hasta sağlık bilgilerinin hastanın izni veya bilgisi olmadan ifşa edilmesinden korumak için ulusal standartların oluşturulmasını gerektiren federal bir yasa olarak tanımlanmaktadır. Aynı zamanda Ekonomik ve Klinik Sağlık Yasası için Sağlık Bilgi Teknolojisi Yasası (HITECH)'e göre ABD Sağlık ve İnsan Hizmetleri Dairesi'nin Sivil Haklar Bürosu'nu kendi web sitesinde sağlık hizmeti veri ihlali rakamlarını yayınlamaya çağırmasından bu yana 2020'de diğer yıllara göre daha büyük sağlık hizmeti veri ihlalleri bildirildi. Çalışmaya göre temel sonuçlar; (Alder, 2020) şu şekildedir:

- Sağlık hizmeti veri ihlallerinde yıldan yıla % 25 artışmıştır.
- Sağlık hizmeti veri ihlalleri 2014'ten bu yana iki katına çıkmıştır.
- 2020'de 500 veya daha fazla kayıttan 642 sağlık hizmeti veri ihlali bildirilmiştir.
- 2020'de her gün 500 veya daha fazla sağlık bakımı kaydının 1.76 veri ihlali rapor edilmiştir.
- 2020'de 29 milyondan fazla sağlık hizmeti kaydı ihlal edilmiştir.
- Bir ihlal 10 milyondan fazla kaydı içeriyordu ve 63'ü 100.000'den fazla kaydın ihlal edildiğini görülmüştür.
- Bilgisayar korsanlığı / BT olayları, veri ihlallerinin% 67'sini ve ihlal edilen kayıtların% 92'sini oluşturulmuştur.
- Ekim 2009'dan bu yana 500 veya daha fazla kayıttan 3.705 veri ihlali rapor edilmiştir.
- Ekim 2009'dan bu yana 78 milyon sağlık hizmeti kaydı ihlal edilmiştir.

HIPAA'a göre, bilgisayar korsanlığı ve diğer BT olayları, 2020'de sağlık hizmeti veri ihlali raporlarına hâkim oldu. 2020'de 429 bilgisayar korsanlığı / BT ile ilgili veri ihlali rapor edildi ve bu, rapor edilen tüm ihlallerin% 66.82'sini ve ihlal edilen tüm kayıtların %91.99'unu oluşturuyor. Bu olaylar, güvenlik açıklarının ve kimlik avı, kötü amaçlı yazılım ve fidye yazılımı saldırılarının istismarını içerir ve son aylarda son aylarda önemli ölçüde artmıştır (Alder, 2020).

Tablo 2.8.1.2 2020 Sağlık Hizmeti Veri İhlallerinin Başlıca Nedenleri

İhlal Türü	İhlal sayısı	Kayıtlar ihlal edildi	İhlal Edilen Ortalama Kayıtlar
Bilgisayar Korsanlığı / BT Olayı	429	26.949.956	62.820
Yetkisiz Erişim / İfşa	143	787.015	5.504
Çalınması	39	806.552	20.681
Yanlış İmha	16	584.980	36.561
Zarar	15	169.509	11.301

Kaynak: (HIPAA, 2020)

HIPAA'a göre; veri depolamak için şifreleme ve bulut hizmetlerinin artan kullanımı, önceden bildirilen ihlallerin çoğunu oluşturan kayıp / hırsızlık olaylarının sayısını azaltmaya yardımcı oldu. Kimlik avı saldırıları, sağlık hizmetlerinde veri ihlallerinin hala önde gelen nedenlerinden biridir ve genellikle kötü amaçlı yazılım veya fidye yazılımının konuşlandırıldığı

çok aşamalı bir saldırının ilk adımıdır. E-posta hesabı ihlalleri 2020 yılında iki günde birden fazla rapor edilmiştir. E-posta ile ilgili ihlaller ağ sunucularının ihlallerinin ardından ikinci sırada yer alırken ağ sunucuları genellikle büyük miktarda hasta verisi depolar ve bilgisayar korsanları ve fidye yazılımı çeteleri için birincil hedeftir. Sağlık hizmeti veri ihlallerinin çoğu elektronik korumalı sağlık bilgilerini içeriyor olsa da 2020'deki ihlallerin önemli bir yüzdesi, yetkisiz kişiler tarafından elde edilen, kaybolan veya güvenli olmayan bir şekilde imha edilen korunan sağlık bilgilerinin kâğıt / film kopyalarını içermektedir (Alder 2020).

Ülkemizde Kişisel Verileri Koruma Kurumu (KVKK) tarafından 6698 sayılı Kişisel Verilerin Korunması Kanununun "Veri güvenliğine ilişkin yükümlülükler" başlıklı 12'nci maddesinin (5) numaralı fıkrası "işlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve kurula bildirir. Kurul, gerekmesi hâlinde bu durumu, kendi internet sitesinde ya da uygun göreceği başka bir yöntemle ilan edebilir." hükmü uyarınca resmi internet sayfasında tespit edilmiş ve yayınlanmış bazı veri ihlal örnekleri aşağıda yer almaktadır.

- Denizli Özel Egekent Hastanesi tarafından kurula iletilen veri ihlal bildiriminde özetle; 10.10.2022 tarihinde fidye yazılımı saldırısına maruz kalması sonucu sistemlerinin şifrelendiği ve hastane sistemlerine erişim sağlanamadığı, ihlalden etkilenen ilgili kişi gruplarının çalışanlar, kullanıcılar, aboneler, öğrenciler, müşteriler, hastalar, çocuklar, korunmaya muhtaç yetişkinler olduğu, ihlalden etkilenen kişisel veri kategorilerinin kimlik, iletişim, lokasyon, özlük, hukuki işlem, müşteri işlem, fiziksel mekân güvenliği, işlem güvenliği, risk yönetimi, finans, mesleki deneyim, pazarlama bilgileri ile görsel ve işitsel kayıtlar olduğu, ihlalden etkilenen tahmini kişi sayısının 295 olduğu,

- Yonca Sağlık Hizmetleri Ltd. Şti. tarafından kurula iletilen veri ihlal bildiriminde özetle; veri sorumlusu sistemlerine siber bir saldırı gerçekleştirildiği, gerçekleştirilen saldırının tipik ransomware, ddos, vb. gibi bir saldırı olmadığı, saldırı tipinin tespiti için incelemelerin devam ettiği, ihlalin 15 mart 2022 tarihinde başladığı ve 16 mart 2022 tarihinde tespit edildiği, ihlalin veri sorumlusu bünyesinde bilgi işlem müdürü olarak çalışan personele iletilen bir e-posta ile öğrenildiği, saldırganın bir metin dosyası halinde tüm klasörlerin listesini veri sorumlusuna iletmek suretiyle veritabanı ve birçok dokümanı ele geçirdiğini belgelediği, saldırgan kişi veya kişilerin, klasörlerin içeriğine erişebilip erişemediği konusunda danışmanlık şirketi tarafından incelemenin devam ettiği, ihlalden etkilenen ilgili kişi gruplarının çalışanlar ve hastalar olduğu, ihlalden

etkilenen kişisel verilerin kimlik, iletişim, özlük, finans, mesleki deneyim, pazarlama bilgileri olduğu, ihlalden etkilenen özel nitelikli kişisel verilerin ise sağlık, ceza mahkumiyeti ve güvenlik tedbirlerine ilişkin bilgiler ile genetik veri olduğu, ihlalden etkilenen tahmini kişi sayısının 500.000 ve tahmini kayıt sayısının 2.500.000 olduğu,

- Düzen Biyolojik Bilimler Araştırma Geliştirme ve Üretim A.Ş. tarafından kuruma gönderilen veri ihlal bildiriminde özetle; veri işleyen konumundaki Fransa'daki Cerba Laboratuvarında yer alan kişisel verilerin yetkisi olmayan kişiler tarafından ulaşılabilir hale geldiğinin veri sorumlusuna bildirildiği, ihlalin 09.06.2021 tarihinde başladığı ve 24.06.2021 tarihinde sona erdiği, bu tarihler arasında veri sorumlusunun cerba laboratuvarına 991 adet numune ilettiği, ancak belirtilen tarihler arasındaki kayıtların ne kadarına ulaşıldığı veya ulaşılıp ulaşılmadığının bilinmediği, ihlalden etkilenen kişisel verilerin ad, soyad, doğum tarihi, cinsiyet, istenen tetkik bilgileriyle birlikte tetkik sonucu olduğu,
- Özel Dentapoint Diş Sağlığı Polikliniği (İzmir) tarafından kurumumuza gönderilen veri ihlali bildiriminde özetle; 12.07.2021 tarihinde yapılan siber saldırı sonucu hasta bilgilerini barındıran bilgisayarların şifrelenerek erişimin engellendiği, ihlalden etkilenen ilgili kişi gruplarının hastalar, müşteriler ve potansiyel müşteriler olduğu, ihlalden etkilenen kişisel verilerin kimlik, iletişim, lokasyon, müşteri işlem, işlem güvenliği, finans, görsel ve işitsel kayıtlar olduğu, ihlalden etkilenen özel nitelikli kişisel verilerin ise ırk ve etnik köken bilgisi ile sağlık bilgileri olduğu, ihlalden etkilenen kişi sayısının tahmini 14.000 olduğu,
- Clearvoiceresearch.com, llc tarafından gönderilen kişisel veri ihlali bildiriminde özetle; ihlalin yetkisiz bir kullanıcı tarafından 2015 ağustos ve eylül aylarına ait yedeklerin herkese açık hale getirilmesi sonucunda meydana geldiği, 17 nisan 2021 tarihinde yetkisiz bir kullanıcı tarafından, clearvoice'un 2015'teki anket katılımcılarının profil bilgilerini içeren eski veritabanlarından birine ilişkin, yedek dosyasına eriştiğini belirten bir e-posta alınması ile ihlalin tespit edildiği, ihlalden kimlik, iletişim, doğum tarihi, 2015 yılına ait şifreler, ırk ve etnik köken, siyasi düşünce, sendika üyeliği, sağlık bilgilerine ilişkin kişisel verilerin etkilendiği, ihladen etkilenen türkiye'de yerleşik kişi sayısının 184.205 olduğu, ihlalden etkilen ilgili kişi grubunun çalışanlar olduğu şeklindedir.

2021 yılında Türkiye'de Kişisel Verileri Koruma Kurumu'na (KVKK) bildirimi yapılan veri ihlali sayısı, bir önceki yıla göre yüzde 78 artmıştır. Geçen yıl eğitim, teknoloji,

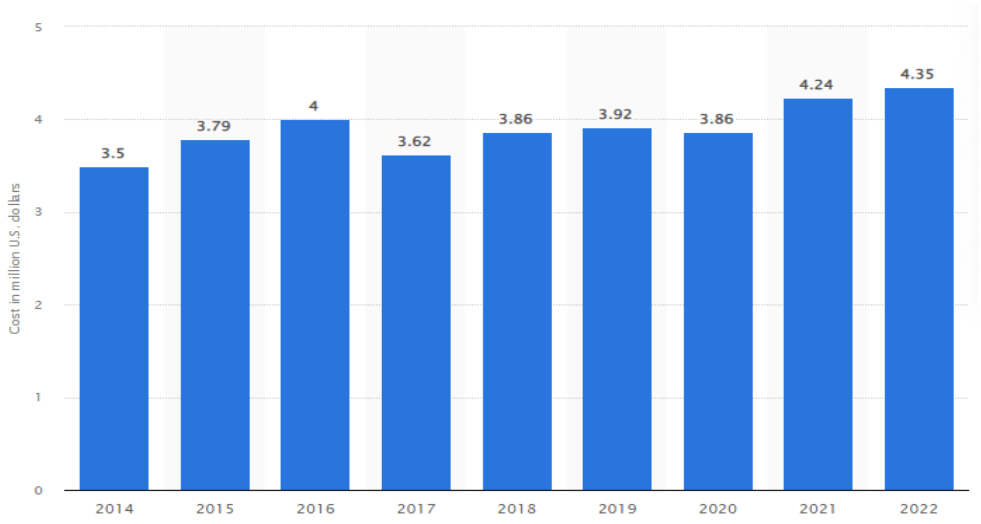
sağlık, bankacılık, kozmetik ve e-ticaret sektörlerinin öne çıktığı veri ihlallerinden 25 milyondan fazla kişi etkilendiği belirtilmiştir (Habertürk, 2022).

2.8.2. Bilgi Güvenliği İhlallerin Maliyeti

Birbirine bağlı çeşitli adımların atıldığı ve her adımın faaliyetlerinin bir önceki aşamanın sonuçlarından etkilendiği sistemlerin yoğun olduğu sağlık kuruluşları genellikle yüksek miktarda hassas veriye sahiptir. İsimleri, doğum tarihini, sosyal güvenlik numarasını ve kredi kartı bilgilerini içeren veriler hastane ve sigorta kayıtlarında bol miktarda bulunur. Dahası, bilgisayar korsanları sağlık kuruluşlarına odaklanmayı tercih ederken, sağlık verileri karaborsadaki diğer endüstrilerden gelen verilerden daha değerlidir. Elektronik sağlık kayıtları, karaborsadaki kredi kartı bilgilerinden 10 ila 100 kat daha değerlidir (Akpan, 2016).

Choi ve Johnson (2019), veri ihlalleri ve hastane reklam harcamaları arasındaki ilişkiyi anlamak için yapmış olduğu çalışmasında ihlal edilen hastanelerin önemli ölçüde daha yüksek reklam harcamalarıyla ilişkili olduğunu, etkilenen hastanenin imajını onarmak ve rakiplere karşı hasta kaybını en aza indirmek için yıllarca düzeltici faaliyetler yürüttüğünü tespit etmiştir. Bir veri ihlalinden kaynaklanan zararları düzeltme çabaları, sağlık hizmeti maliyetlerini artırmakta ve kaynaklarını bakım kalitesini iyileştirme girişimlerinden uzaklaştırabilmektedir.

Bilgi güvenliğine yönelik küresel harcamalar 2017'den 2022'ye kadar artarak 2017'de 101,5 milyar ABD dolarından 2022'de 169 milyar ABD dolarına yükselmiştir. Harcamaların çoğu güvenlik hizmetleri, altyapı koruması ve ağ güvenlik ekipmanlarına yoğunlaşmış olup, 2022 yılında güvenlik hizmeti harcaması dünya çapında 71,68 milyar ABD doları olarak gerçekleşmiştir. 2023 yılına kadar güvenlik hizmetleri harcamalarının 76 milyar ABD dolarını aşacağı tahmin edilmektedir (Statista, 2022).



Şekil 8. Yıllara göre dünya çapında bir veri ihlalinin ortalama maliyeti (Milyon $)(Statisca,2022)

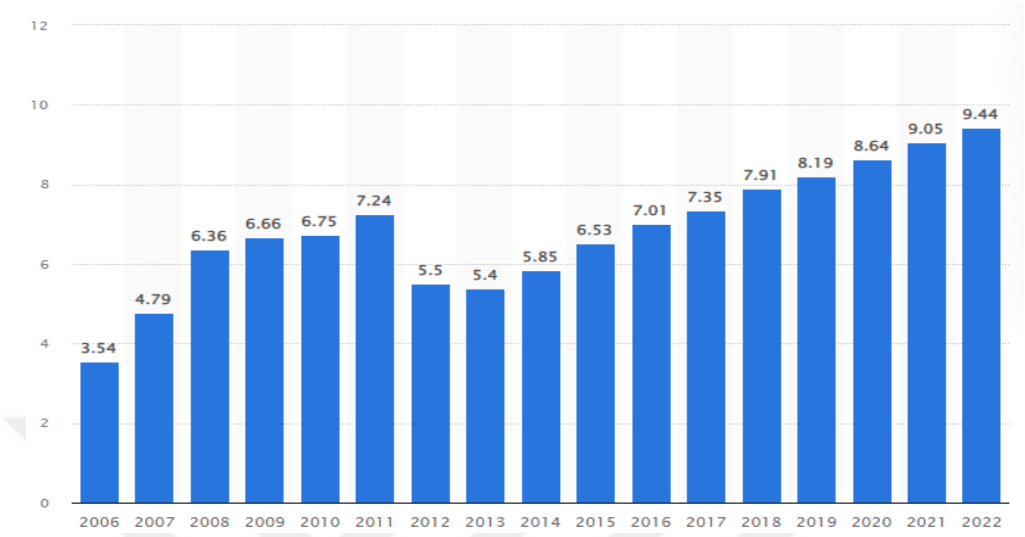
2022 yılı itibariyle, veri ihlali başına küresel ortalama maliyet, bir önceki yılda 4,24 milyon ABD dolarından 4,35 milyon ABD dolarına ulaşarak tüm zamanların rekorunu kırmıştır.

Sağlık hizmeti işletmeleri, bazı durumlarda Sosyal Güvenlik numaraları da dahil olmak üzere milyonlarca insanın hassas kayıtlarını ifşa eden en geniş kapsamlı veri ihlallerinden bazılarına maruz kalmaktadır (Chernyshev ve ark., 2019). Ele geçirilmiş sağlık kayıtları, yalnızca finansal kazanç için sosyal güvenlik numaralarını sömürmekle kalmayıp, aynı zamanda sahte iddialarda bulunmak ve sahte reçeteler yazmak için sağlık sigortası poliçelerini kullanmak isteyen suçlular için özellikle karlı olabilmektedir (Keckley ve ark., 2011).

IBM 2022 raporuna göre art arda on iki yıldır, sağlık sektörü en yüksek veri ihlali maliyetlerine sahip sektör olarak yer almaktadır. 2022'de sağlık sektörü, bir veri ihlali için ortalama 10 milyon ABD Doları öderken, bu durum 2021 yılına göre %9,4 daha yüksektir. Sağlık sektörünü sırasıyla finans ve teknoloji alanları takip etmektedir. Sağlık hizmetleri verileri, diğer verilerden önemli ölçüde daha değerlidir. Tam bir tıbbi kimlik bilgileri kümesinin değeri 1000 ABD $ üzerinde olabilir (Sulleyman, 2017).

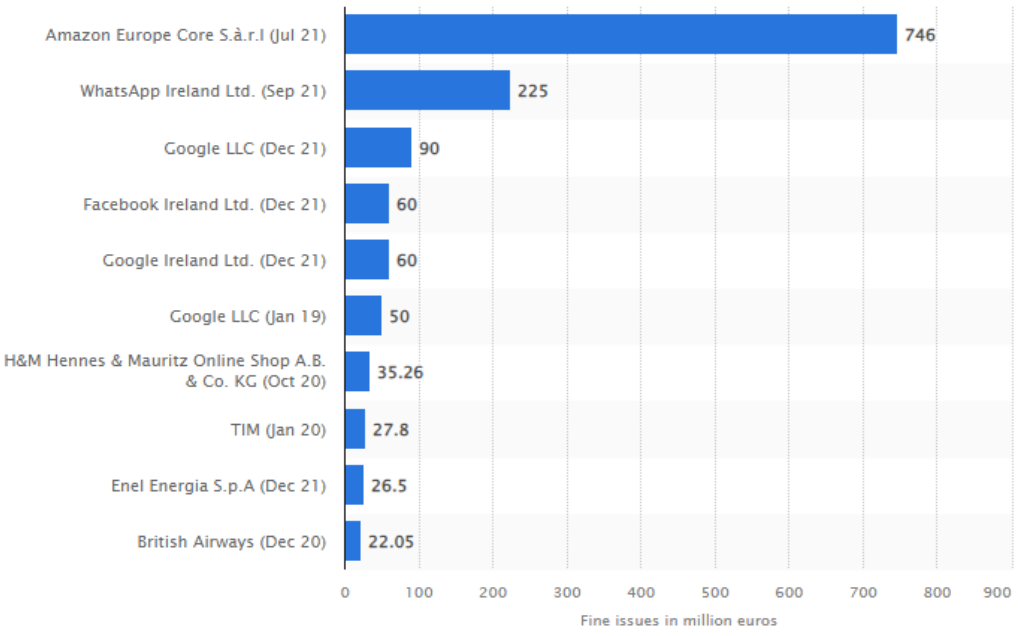
Günümüzde, kurumlar iş süreçlerinin birçoğunda elektronik iletişim sistemlerini ve bilgi kaynaklarını kullanmaktadırlar. Bilgi teknolojilerinin kullanılmasıyla iş süreçlerinin hızlandırılması, kalitenin artırılması ve denetimin kolaylaştırılması sağlanarak kurumun toplam etkinliğinin yükseltilmesi hedeflenmektedir. Ancak, iletişim altyapısında veya bilgi kaynaklarına erişimde meydana gelebilecek bir kesinti, iş süreçlerinin işleyememesine neden

olacak, eğer bu iş süreci kritik sistemlerden birine ait ise, kurumsal güvenlik zafiyetleri meydana gelebilecek, çalışanların ve müşterilerin kuruma ve kurumun bilişim altyapısına güveni olumsuz yönde etkilenecektir (İleri, 2016).



Şekil 9. 2006-2022 Yılları ABD'de Bir Veri İhlalinin Ortalama Maliyeti (Milyon $)(IBM ve Ponemon Enstitüsü, 2022)

IBM ve Ponemon enstitüsü tarafından hazırlanan 2022 veri ihlali maliyeti raporuna göre, 2022 itibariyle, ABD'ki bir veri ihlalinin ortalama maliyeti, bir önceki yılda 9,05 milyon ABD dolarından artarak 9,44 milyon ABD $ ulaşmıştır. Veri ihlali başına küresel ortalama maliyet 2022'de 4,35 milyon ABD $dır.



Şekil 10. GDPR İhlalleri İçin Verilen En Büyük Para Cezaları (GDPR, 2021)

Mayıs 2018'de AB tarafından Genel Veri Koruma Yönetmeliği'nin (GDPR) uygulanmasından bu yana, ihlal veya uyumsuzluk nedeniyle en az 1.163 milyar euro para cezası verildi. Bunlardan Amazon'un Temmuz 2021'de aldığı müşteri verilerini hedefli reklamcılık amaçları için nasıl kullandığına ilişkin 746 milyon Euro'luk para cezası açık ara en büyüğü olmuştur.

Bir veri ihlalinden kaynaklanan sonuçların tahminlerden büyük ölçüde değişebileceği özellikle veri ihlalleri de dahil olmak üzere siber suçların maliyet etkileriyle ilgili olan önemli veri boşluklarının devam edeceği ve tam olarak çözülemeyeceğidir. Bazı maliyet kategorileri nispeten kolay bir şekilde tahmin edilirken, diğerleri kesin olarak tahmin edilemez olsa da sonsuza dek sonuçları işletmeleri etkileyecektir (Wolff ve Lehr, 2017). Bilgi güvenliği yönetimi, sağlık hizmetlerinde kritik öneme sahiptir ve buna sahip olmamanın alternatifi, bir kurum için yıkıcı olmaktadır. Siber suçlular şirket itibarını zedeleyebilir ve etkilerinin üstesinden gelinmesi yıllar alabilmektedir (Roberts, 2014).

Siber güvenlik ihlallerinin geniş kapsamlı ve uzun vadeli etkileri olabileceğini, sistemleri ve verileri tehlikeye atabileceğini, müşteriler, tedarikçiler ve ortaklarla ilişkileri etkileyebileceğini ve aşırı durumlarda kurumlar varoluşsal yapılarını tehdit edebileceğini belirtmiştir (Furnell ve ark., 2020; Wasserman ve Wasserman 2022). Siber suçların ve saldırıların bir bütün olarak kurumların doğrudan ve dolaylı olarak etkileneceği maliyetleri tablo da gösterilmiştir.

Bischoff (2019), tarafından veri ihlalleri sonrası kurumların borsa hisse fiyatlarını nasıl etkilediği üzerine yapmış olduğu çalışmada; Teknoloji ve finans şirketleri, bir ihlalin ardından hisse fiyatı performansında en büyük düşüşü yaşarken, e-ticaret ve sosyal medya şirketleri en az etkilendiğini, kredi kartı ve sosyal güvenlik numaraları gibi son derece hassas bilgileri sızdıran ihlaller, daha az hassas bilgileri sızdıran şirketlere göre ortalama olarak hisse fiyatı performansında daha hızlı düşüş gösterdiklerini, ancak uzun vadede daha fazla zarar görmediklerini tespit etmiştir.

Tablo 2.8.2.1.Veri İhlali Durumunda Doğrudan ve Dolaylı Maliyetler

	Kısa vadeli	Orta vadeli	Uzun vadeli
Doğrudan maliyet	• Danışman ücretleri • Siber fidye ve gasp kayıpları • Finansal Hırsızlık • Sigorta fazlalığı • Personel yanıtı (ücretli fazla mesai) • Personel yanıt maliyetleri (sözleşmeli dış personel)	• Siber güvenlik uygulamalarındaki değişiklikler • Tazminat/indirimler • Şikayetler (harici) • Amaçlı • Soruşturma (harici) • Yasal • PR/pazarlama faaliyetleri (harici) • İşe alım maliyetleri • Üçüncü taraf sorumluluğu	• Kredi notu/sigorta primleri • Siber güvenlik iyileştirmeleri • Yatırım/bağışçı/fon kaybı • Personel maliyetleri (uzun vadeli) • Eğitim maliyetleri • Eğitim maliyetleri (Dış kaynaklar) • Hisse değeri
Dolaylı maliyet	• Çevreleme • Veri ve yazılım kaybı • Fikri mülkiyet hırsızlığı • Personelin olağan iş faaliyetlerinin kesintiye uğraması (fırsat maliyeti) • BT ekipmanı hasarı • Bildirim maliyetleri (yetkililer) • Bildirim maliyetleri (müşteri) • Fiziksel ekipman hasarı (BT ekipmanı hasarı dahil değildir) • Hizmetin kesintiye uğraması	• Şikayetler (dahili) • Soruşturma (dahili) • İhlal sonrası müşteri koruması • PR/pazarlama faaliyetleri (dahili)	• Müşteri yıpranması • Siber güvenlik iyileştirmeleri (Fırsat maliyeti) • Uzun vadeli üretkenlik • Tedarik zinciri yıpranması • Eğitim maliyetleri (Iç kaynaklar) • Eğitim maliyetleri (Fırsat maliyeti)

Kaynak: (Furnell ve ark., 2020; Wasserman ve Wasserman 2022)

Ayrıca, İngiltere Devlet Dijital Hizmet Kurumu (https://www.gov.uk/) tarafından 2020 yılında yayınlanan "Siber güvenlik ihlallerinin tüm maliyetlerinin analizi: Sonuç Raporu" adlı çalışmada, Aralık 2019 ile Mart 2020 arasında hükümet ve endüstrideki beş paydaşla görüşmelerde maliyet araştırması sırasında belirlenen maliyet kategorileri ile kuruluşlar tarafından tanımlanan maliyetler tanımlamarı ortaya konuşmuş olan ve Furnell ve ark. (2020), tarafından yapılan çalışma ile benzerlik göstermekte olup rapora göre bazı maliyet kalemleri şöyledir:

- **Tazminat/iskontolar**: İhlalden etkilenen müşterilere verilen ödemeler veya indirimler,
- **Şikâyetler:** İhlalin bir sonucu olarak şikayetlerle başa çıkmak için ek personel veya hizmetlerle sözleşme yapma maliyeti,
- **Danışman ücretleri**: İhlale yanıt vermek için harici danışmanları işe alma maliyetleri,
- **Çevreleme**: Güvenli olmayan uygulamalar, web siteleri, e-posta ve diğer yüksek riskli alanları kapatmak gibi ihlali içeren faaliyetlerin maliyetleri,
- **Kredi notu/sigorta primleri**: Uzun vadeli kredi notu/sigorta primlerinde ki hasar,

- **Müşteri kayıpları**: Gelecekteki kayıp müşteriler de dahil olmak üzere kayıp müşterilerden elde edilen gelir kaybı,
- **Siber fidye ve gasp kayıpları**: Siber güvenlik ihlali tarafından reddedilen hizmetlere erişimi geri almak için yapılan herhangi bir fidye ödemesinin maliyeti,
- **Siber güvenlik iyileştirmeleri**: Benzer bir oluşumu önlemek için siber güvenlik iyileştirmeleri, güvenliği artırmak için internet hizmeti sağlayıcıları (İSS'ler), güvenlik sağlayıcılarını veya ürünleri değiştirmenin maliyeti,
- **Veri ve yazılım kaybı**: Kaybolan, bozulan, çalınan, silinen veya şifrelenen verilerin veya yazılımların yeniden yapılandırılması, değiştirilmesi, yenilenmesi veya çoğaltılması maliyetleri,
- **Finansal**: Para hırsızlığı veya diğer finansal varlıkların (örneğin, hisse senetleri) çalınması da dahil olmak üzere siber güvenlik ihlalinden kaynaklanan finansal kayıplar,
- **Para cezaları**: İhlalin bir sonucu olarak düzenleyicilere veya yetkililere verilen para cezalarının maliyeti,
- **Sigorta:** Bir siber güvenlik ihlalinden kaynaklanan finansal kayıpların sigorta tarafından karşılanması durumunda, firma tarafından ödenen sigorta fazlalıklarını içerir,
- **Fikri mülkiyet hırsızlığı**: Bir fikri mülkiyet varlığının değer kaybı,
- **Olağan iş faaliyetlerinin kesintiye uğraması (fırsat maliyeti)**: Personelin olağan işlerini yürütmesi durdurulduğunda fırsat maliyeti,
- **Hizmetin kesintiye uğraması**: Müşteriler ihlal sırasında hizmete erişemediğinde ortaya çıkan gelir kaybı,
- **Soruşturma:** Siber güvenlik ihlalinin kaynağını, kapsamını ve büyüklüğünü ortaya çıkarmak için kullanılan faaliyetlerin maliyeti,
- **Yatırım / bağışçı / finansman kaybı**: İhlalin bir sonucu olarak yatırımcıların, bağışçıların veya diğer finansman kaynaklarının (örneğin, kitle fonlaması) kaybı,
- **Yasal:** İhlalin bir sonucu olarak gerekli olan yasal tavsiyenin maliyeti,
- **Uzun vadeli üretkenlik**: Firmaların ihlalin bir sonucu olarak daha fazla riskten kaçınması durumunda araştırma ve geliştirme (Ar-Ge) harcamalarındaki düşüşle ilişkili maliyetler ve bu da uzun vadeli üretkenlikte bir düşüş maliyeti,
- **Bildirim maliyetleri (yetkililer)**: Olayın ilgili makamlara bildirilmesinde yer alan maliyet ile verileri tehlikeye giren bireyleri bilgilendirmekle ilişkili doğrudan giderler,
- **Fiziksel ekipman hasarı**: İhlalden etkilenen bilgi teknoloji sistemleri,

- **İhlal sonrası müşteri koruması**: Bir bireyin güvenliği ihlal edilmiş kişisel verilerini doğrulanmamış amaçlar için kullanmaya yönelik potansiyel çabaları tespit etmek ve bunlara karşı korumak için ek hizmetlerle ilişkili maliyetler,
- **PR/pazarlama faaliyetleri** (harici): İhlalde ortaya çıkan marka hasarını onarmak için üçüncü tarafları işe alma maliyeti ve reklam faaliyetlerin maliyeti,
- **Hisse değeri**: İhlalin bir sonucu olarak firmanın değerindeki kayıp,
- **Personel maliyetleri (uzun vadeli):** Ek siber güvenlik personelinin işe alınması da dahil olmak üzere ihlalin bir sonucu olarak siber güvenliğe yapılan harcamaların artması ile ihlale yanıt vermek için gereken fazla mesai maliyetleri,
- **Tedarik zinciri yıpranması**: Tedarik zinciri üyelerinin bir ihlalin sonucu olarak artık bir kuruluşla iş yapmaya istekli olmamasının neden olduğu gelir kaybı,
- **Üçüncü taraf sorumluluğu**: İhlalin bir sonucu olarak açılan herhangi bir davanın sonucu olarak ortaya çıkan tüm ödemeler,
- **Eğitim maliyetleri (**fırsat maliyeti): Ek siber güvenlik eğitimine personel katılımının fırsat maliyeti,

Malliouris ve ark. (2020), tarafından 2005 ile 2019 yılları arasında ABD merkezli 202 ciddi güvenlik ihlali örneğini analiz ederek, ciddi güvenlik ihlallerinin maliyeti incelenmiş olup, genel olarak güvenlik ihlallerinin altta yatan ya da ortaya çıkan ekonomik etkileri ile özellikle özkaynakları içerisinde finansal sistematik risk maruziyetindeki değişiklikler hakkında literatüre yeni bakış açıları sunmaktadır.

Diğer taraftan günümüzde artık sağlık hizmetlerinde dijital çözümlere büyük ölçüde bağımlı olmakla birlikte (Gordon ve ark., 2017), dijital çözümlerin kesintiye uğraması, en kötü senaryoda, operasyonların tamamen durmasına yol açabilir ve bu da sağlık hizmetleri üzerinde ciddi etkilere neden olabilmektedir (Kaiser ve ark., 2021). 2022'de yapılan araştırma sonuçları fidye yazılımı saldırılarına maruz kalan şirketlerin çoğunun saldırgana fidye ücreti ödediğini göstermektedir (Cyberseason, 2022).

2.9. Sağlık Kurumlarında Bilgi Güvenliği İhlalleri ve İnsan Faktörün Önemi

Sağlık hizmet endüstrisi her yıl milyonlarca insana hizmet üretmektedir. Endüstri sürekli gelişmekte ve günlük işleri yürütmek için teknolojiyi giderek daha fazla kullanmaktadır. Sağlık hizmetleri, tıbbi kayıtlar, çalışan bilgileri, finansal veriler ve araştırma verileri gibi çok büyük miktarlarda hassas ve özel bilgiler üretmesinden dolayı siber suçların daha fazla dikkatini çekmektedir (Roberts, 2014).

Bütünsel güvenlik; teknoloji, insanlar ve prosedürlerin entegre karışımıdır. Günümüzün digital dünyasında, sağlık hizmetlerinde siber güvenlik ve bilgilerin korunması, kuruluşların normal işleyişi için hayati öneme sahiptir. Birçok sağlık kuruluşu, elektronik sağlık sistemleri, e-reçete sistemleri, muayenehane yönetimi destek sistemleri, klinik karar destek sistemleri, radyoloji bilgi sistemleri gibi çeşitli sağlık sistemleri ile sağlık sisteminin olmazsa olmaz altyapı sistemleri olan akıllı asansörler, akıllı ısıtma, havalandırma ve iklimlendirme sistemleri, infüzyon pompaları, uzaktan hasta izleme cihazları ve diğer sistemleri etkin bir şekilde kullanmaktadır (Patterson, 2003).

Elektronik sağlık kayıtları Murphy ve ark. (1999) tarafından tanımlandığı şekliyle, hastalar için elektronik sistem(ler)de bulunan bir bireyin geçmiş, şimdiki veya gelecekteki fiziksel/zihinsel sağlığı veya durumu ile ilgili herhangi bir bilgiyi elde etmek için kullanılan bilgisayarlı tıbbi kayıtlardır şeklinde tanımlanmıştır. Kumar ve ark. (2022), göre günümüzün dijital ortamında, kağıt tabanlı sağlık sisteminden elektronik sağlık sistemine doğru kaymaktadır. Elektronik sağlık sistemlerine özellikle kullanıcısının internet yardımıyla dünyanın herhangi bir yerindeki sağlık hizmetleri verilerine ve kaynaklarına erişmesine izin vermektedir. Elektronik sağlık sistemine geçiş nedeniyle sistemlerinin erişim kontrolü, güven, kimlik doğrulama, verilerin iletilmesi, paylaşılması, delegasyonu, sağlık hizmeti verilerinin kötüye kullanılması, veri gizliliği ve bütünlüğü gibi birçok güvenlik ve mahremiyet sorununu beraberinde getirmiştir (Singh ve Chatterjee, 2019).

Sağlık bilgi alışverişi terimi, bir bireyin kişisel sağlık kayıtlarının sağlık hizmeti sağlayıcıları arasında paylaşılmasını kolaylaştıran sistemlerin ortak tanımı olarak ortaya çıkmıştır (Huang ve ark., 2014). Sağlık sektörü paydaşları, son derece hassas ve gizli verilerin toplanmasından ve saklanmasından ve aynı zamanda çalışanlar ve hastalardan elde edilen verilerin diğer kuruluşlar arasında paylaşılmasından sorumlu olması ile birlikte elde etmiş olduğu veriyi aynı zamanda koruma ihtiyacını da ortaya çıkarmıştır (Fahey ve Hino, 2020).

Elektronik hasta bilgilerinin güvenliğinin kurumsal bir zorunluluk olduğunu günümüz gerçekleri özellikle vurgulamaktadır. Sağlık sektöründe bilgi güvenliği ve mahremiyeti önemi giderek artan bir konu olmakla beraber sorunun karmaşıklığı, artan güvenlik ihlalleri ve ihlal edilen hasta verilerinin yasal ve finansal sonuçları birlikte ele alındığında dijital hasta kayıtlarının benimsenmesi, artan düzenleme, sağlayıcı konsolidasyonu ve hastalar, sağlayıcılar ve ödeme yapanlar arasında artan bilgi alışverişi ihtiyacı, daha iyi bilgi güvenliğine ihtiyaç olduğuna işaret etmektedir (Appari ve Johnson, 2010).

Donaldson ve ark. (2000)'a göre "Hata yapmak insan olmaktır", tıbbi hatayı azaltmak için yeni teknolojilerin geliştirilmesi ve test edilmesi çağrısında bulunan kitapta daha güvenli bir sağlık sistemi tasarımı yoluyla tıbbi hataları azaltmak ve hasta güvenliğini artırmak için ulusal bir gündemin önemine değinirken asıl sorunun ise sağlık hizmetlerindeki çalışanların kötü insanların olmadığını, daha güvenli hale getirilmesi gereken kötü sistemlerde çalışan iyi insanlar olduğunu iddia etmektedir. Bilgi güvenliği doğası gereği multidisipliner olduğundan ve insan boyutu bunda önemli bir rol oynadığından, bilgi güvenliğinin sadece teknik yönlerine odaklanmak yeterli değildir. Önemli sayıda kurumsal bilgi güvenliği olayı, insan unsurlarının istismarından kaynaklanmaktadır (Stahl ve ark., 2012).

Birçok işletme, iş sürekliliği için çalışanlarının hem çalıştıkları yerlerde hem de işletme dışında bağlantı kurabildiği bu teknolojileri günlük işlerinde de kullanmaktadırlar. Ancak, kuruluşlar veri ihlali olayları yaşamaya devam ederken getirilen teknolojik çözümler ne olursa olsun, insan faktörü gereken özenin gösterilmediği bir alan olmaya devam etmektedir (Zahadat ve ark., 2015; Parasuraman ve Riley, 1997; Yusof ve ark., 2008). İnsanların beklenen güvenli davranış kalıplarını izleyeceği ve dolayısıyla sistem güvenlik beklentilerinin karşılanacağı varsayımı doğru olmayabilir. Güvenlik öylece satın alınabilecek bir şey değildir; insan faktörleri her zaman keşfedilecek önemli bir alan olacaktır. Bu nedenle, insan faktörü hiç şüphesiz bilgi güvenliğinde kritik bir noktadır (Hughes-Lartey ve ark., 2021).

Tıpkı bilgi teknolojisi gibi, çalışanlar bilgi güvenliğinin ayrılmaz bir parçasıdır ve bilgi teknolojisinde, veri ihlali olaylarının teknolojik düzeyde gerçekleşmesini zorlaştıracak kadar karmaşık birçok teknolojik gelişme olmasına rağmen, veri ihlali suçlularının ister hata ister davranış olsun, insan davranış faktörlerinin bir bilgi güvenliği yapısının zayıf noktası olabileceğinin giderek daha fazla farkına varılmaktadır (Mitnick ve Simon, 2002; Gonzalez ve Sawicka, 2002). Herhangi bir güvenlik sistemi, ne kadar iyi tasarlanmış ve uygulanmış olursa olsun, insanlara güvenmek zorunda kalacaktır. Veri ihlallerinin çoğunda insan faktörünün çok önemli bir rol oynamasına rağmen günümüzde en modern "güvenlik bilgi sistemlerinin" rahatsız edici bir özelliği insan faktörünü ele alınmamasıdır.

AlGhamdi ve ark. (2022), son zamanlarda bilgi güvenliğine yapılan yatırım artarken, dünya genelindeki birçok kuruluş, uyumlu olmayan çalışanlar nedeniyle güvenlik tehditlerinden ve veri ihlallerinden kaçınamıştır. Ayrıca kuruluşların çoğu zaman güvenlik ihlallerinin ana nedeni olarak insan faktörlerini sürekli olarak göz ardı etme "alışkanlığına"

sahip olduklarını ve kaynaklarını teknolojik kontroller ve çözümlere öncelik vermeyi tercih ettiklerini göstermektedir (Liginal ve ark., 2009).

Kessler ve ark. (2020), medya ve popüler basın genellikle veri ihlallerini harici "bilgisayar korsanlarına" bağlarken, araştırmalar veri ihlallerinin yaklaşık yüzde 82'sinin doğrudan veya dolaylı olarak çalışanların dikkatsizliğinin ve/veya çalışanların mevcut bilgi güvenliği (IS) düzenlemelerine, politikalarına ve prosedürlerine uyulmaması sonucu olduğunu göstermektedir (Verizon, 2022).

Muthuppalaniappan ve Stevenson (2021), göre sağlık kuruluşları, bireyler, altyapılar ve tedarik zincirleri hakkında hassas verileri rutin olarak toplayıp depolarken, sağlık çalışanları bu veri kaynaklarını kullanmak için bilgi sistemlerine güvenmektedir. Bu tür sistemleri etkileyen herhangi bir olayın, sağlık kuruluşu ve paydaşlarının stratejisi ve işleyişi üzerinde önemli bir etkisi olmaktadır. Bu nedenle, siber güvenlikle ilgili zorluklar son zamanlarda küresel sağlık için bir tehdit olarak kabul edilmektedir. Sağlık sistemlerinin siber güvenliğinin zorlukları çoğunlukla bilinmesine rağmen, bu sistemlerin karmaşıklığı ve çeşitliliği nedeniyle bunları incelemek ve çoğu duruma uyan çözümler sunmak zordur (Razaque ve ark., 2019).

Dünya Sağlık Örgütü'nün (WHO,2021a) birinci basamak sağlık hizmetlerine ilişkin yayınladığı teknik veriye göre bilgi ve iletişim teknolojisi, akıllı telefonların, tabletlerin ve dizüstü bilgisayarların kullanıma girmesiyle giderek daha yaygın hale gelmektedir. İnsanların sağlıklarını daha etkili bir şekilde yönetmelerine olanak tanıyan teknolojiden, hastalıkları teşhis etmenin daha iyi yollarına, politikaların nüfus sağlığı üzerindeki etkisinin izlenmesine kadar, sağlık için dijital teknolojiler, sağlık hizmetlerinin nasıl sunulduğunu ve işletildiğini etkilemektedir. Dijital dönüşüm stratejilerinin benimsenmesinin önündeki en büyük engellerden biri, sistemlerin güvenlik açıklarının yanı sıra insan kaynaklı zayıflıklardan da sorumlu olan siber suçlardır.

Sağlık personeli arasındaki bilgi iletişimi ve bilgi yönetim sistemleri bir sorun olarak görülmekte ve en önemli sorunların başında, sağlık bilgilerinin nasıl kullanılacağına ilişkin bilgisayar, çevre birimler, diğer teknik altyapı cihazları ile çalışanların bilgi güvenliği bilgisinin olmaması, sisteme eklenen bilgilerin iletilmesi ve alınması noktasında kontrollerin olmamasından kaynaklı çoğu zaman birçok hataya yol açarak sistemin güvenliğini tehlikeye atmaktadır (Hamdan, 2018; Zhang ve ark., 2014).

Çalışanların bilgi teknolojisi algısı, onların davranışları ve kararları üzerinde büyük bir etkiye sahiptir olmaktadır. Kuruluşların kullanıcıların bilgi güvenliği algısıyla uğraşırken, algılarının farkındalık, bilgi, kontrol edilebilirlik, ciddiyet ve olasılık gibi çeşitli faktörler tarafından belirlendiğini ve bunların da kendi güvenliklerini için karar ve davranışlarını etkileyen bir faktör haline geldiğini göstermektedir. Kullanıcıların bir bilgi güvenliği politikası alanında neler olup bittiğine dair tam bir resme ve tam farkındalığa sahip olduklarında, potansiyel tehditleri tanıma yeteneklerini olumlu yönde etkileyeceğini anlamak sistem ve kurumlar açısından önemlidir (Hu ve ark., 2012). Sağlık sektöründe dijital dönüşüm stratejilerinin başarılı bir şekilde benimsenmesi, sağlık uzmanları arasında siber tehditlerin oluşturduğu risklerin ele alınmasına yönelik başarılı kabule bağlıdır. Bu nedenle, sağlık profesyonelleri için farkındalık ve eğitim programları sunmanın önemli olduğunu belirtmiştir (Nifakos ve ark., 2021).

Kullanıcı güvenliği farkındalığı, herhangi bir kuruluşun genel güvenliği için kritik öneme sahiptir. Bilgi güvenliği farkındalığı, tüm çalışanların zihninde doğru güvenlik prosedürlerini ve güvenlik ilkelerini sağlam bir şekilde oluşturmak için kuruluşlar tarafından kullanılması gereken önleyici bir önlem olmalıdır. Artan farkındalık, kullanıcı kaynaklı güvenlik tehditlerini en aza indirirken güvenlik etkinliğini insan bakış açısından en üst düzeye çıkarmaktadır (Kruger ve ark., 2011).

Bilgi güvenliği sistemi değerlendirmeleri söz konusu olduğunda kurumlar içerisindeki personel arasındaki kaçınılmaz bağ göz ardı edilemez ancak kuruluşların çoğunlukla sistemin teknolojik yönünü değerlendirmekte ve güvenlik sisteminin savunmasızlığını büyük ölçüde etkileyebilecek insan faktörlerini çok az değerlendirmekte veya göz ardı etmektedir (Speed ve ark., 2018).

3. GEREÇ VE YÖNTEM

Bu bölümde, araştırmanın kapsamı, araştırmanın amacı, araştırmanın yöntemi hakkında bilgiler verilerek, araştırmadan elde edilen bulgular ve bulguların sonuçları değerlendirilmektedir.

3.1. Araştırmanın Amacı ve Önemi

Sağlık kurumları hastaların kişisel bilgilerinin yanı sıra tıbbi ve idari verilerin yoğun bir şekilde kullanıldığı ve bu bilgilerin tanımlaması, değerlendirilmesi, uygulanması, saklanması ve veri paylaşılmasına olanak sağlayan bilgi ve iletişim teknolojilerin yoğun ve etkin kullanıldığı bir sektör olarak yer almaktadır. Sağlık sektörü diğer sektörlere göre elde edilen verilerin önemi gereği daha büyük siber risklerle karşı karşıya kalmakta, karşılaşılabilecek veri ihlallerin kontrolü için de bilgi güvenliği politikalarının uygulanlması zorunlu bir süreç haline gelmektedir. Bilgi güvenliği yalnızca sağlık tesislerinin bilgi sistemlerinin güvenliğini ile ilgili olmadığı, bilgi güvenliği sürecinde insan faktörü, cihazların durumu, personel çeşitliliği, erişim yetkisi, mahremiyet, maliyet, etik, eğitim ve görev düzeyi ile ilgili birçok faktörün etki ettiği karmaşık bir süreç olarak karşımıza çıkmaktadır. Bu alanda, ISO/IEC 27001 kapsamında Bilgi Güvenliği Yönetimi ile bilgi güvenliğinin sağlık kuruluşlarında önemine yönelik literatürde az sayıda çalışmanın bulunmamasıyla birlikte birtakım araştırma faaliyetlerine ihtiyaç olduğu tespit edilmiştir.

Bu çalışma, sağlık kurumlarının bilgi işlem merkezlerindeki çalışanların ISO/IEC 27001 ve Sağlık Bakanlığı Bilgi Güvenliği Yönetmeliği hükümleri noktasında farkındalık seviyeleri ile uygulama süreçlerindeki bilgi düzeylerini ölçmeyi amaçlamaktadır.

3.2. Araştırma Evreni

Araştırma evrenini Ankara ili sınırları içerisinde bulunan Ankara İl Sağlık Müdürlüğü ve bağlı tüm sağlık tesislerinde (Merkez Müdürlük, Hastaneler, İlçe Hastaneler, İlçe Sağlık Müdürlükleri, Entegre Hastaneler) bilgi işlem biriminde çalışan mühendis, tekniker ve diğer kamu personeli meslek grupları oluşturmaktadır. Ankara ili sınırları içerisinde 50'nin üzerinde sağlık tesisi, merkez müdürlüğü ve ilçe sağlık müdürlükleri bulunmaktadır. Bir bilgi işlem birimde genellikle 6 personel olduğu göz önüne alındığında ulaşılabilir evrenin yaklaşık olarak 300 kişiden oluştuğu söylenebilir. Bu araştırma kapsamında evrenin yaklaşık olarak %90'ına (N=268) ulaşılmıştır.

3.3. Veri Toplama Yöntemi

Nicel bir araştırma olan bu çalışmada bilgiler online anket formu kullanılarak 1.11.2021-01.08.2022 tarihleri arasında toplanmıştır. Anket formu katılımcılara, Ankara İl Sağlık Müdürlüğü Bilgi İşlem Uzaktan Eğitim Modülü vasıtasıyla web mesaj olarak iletilmiştir ve anketi yanıtlamaları istenilerek cevaplar elde edilmiştir.

3.4. Araştırmanın Türü

Araştırma, nicel bir yöntem olup tanımlayıcı tipte bir çalışmadır.

3.5. Araştırmanın Yapıldığı Yer ve Özellikleri:

Ankara İl Sağlık Müdürlüğü ve Bağlı Tüm Sağlık Tesisleri (Merkez Müdürlük, Hastaneler, İlçe Hastaneler, İlçe Sağlık Müdürlükleri, Entegre Hastaneler) dahil edilmiştir. (Ek liste)

Tablo 3.5.1. Sağlık Tesis Listesi

2.ve 3. Basamak Sağlık Tesisi	38 Merkez
ADSM ve Diş Hastanesi	11 Merkez
İl, İlçe Sağlık Müdürlüğü ve TSM	22 Merkez

3.6. Araştırmaya Katılımcıların Dahil Edilme Kriterleri

Araştırmaya sadece Ankara İl Sağlık Müdürlüğü ve bağlı tüm sağlık tesislerinde (Merkez Müdürlük, Hastaneler, İlçe Hastaneler, İlçe Sağlık Müdürlükleri, Entegre Hastaneler) bilgi işlem biriminde çalışan mühendis, tekniker ve diğer kamu personeli çalışanları ile hizmet alım yöntemi ile istihdam edilen bilgi işlem personeli dahil edilmiştir.

3.7. Veri Toplama Tekniği ve Araçları

Çalışmada online anket formu kullanılmıştır. Anket formu, sosyodemografik özellikleri belirleyen sorular ile çalışma için ISO/IEC 27001 Bilgi Teknolojisi, Güvenlik Teknikleri, Bilgi Güvenliği Yönetim Sistemleri, Gereksinimler dokümanı EK-A' da yer alan Referans Kontrol Amaçları ve Kontroller başlığı altında yer alan kontrol listesi paralelinde hazırlanan maddelerden oluşan anket (EK-4) kullanılmıştır. Anket formu iki kısımdan oluşmaktadır. Birinci kısımda kişisel bilgi formu, ikinci kısımda ise sağlık çalışanlarına yönelik anket formu bulunmaktadır. Kişisel bilgi formunda; katılımcıların cinsiyeti, yaşı, medeni durumu, öğrenim durumu, ünvanı, hangi tür hastanede çalıştığı, çalıştığı bölüm/departman, aylık geliri ve meslekte toplam deneyimi bilgilerini tespit etmeye yönelik sorular sorulmuştur. Bölüm -1-

Kişisel Bilgiler- 9 Soru dan oluşmaktadır. İkinci kısımda (Kılıç 2019) tarafından oluşturulan ISO/IEC 27001 Bilgi Teknolojisi, Güvenlik Teknikleri, Bilgi Güvenliği Yönetim Sistemleri, Gereksinimler dokümanı EK-A' da yer alan Referans Kontrol Amaçları ve Kontroller başlığı altında yer alan kontrol listesi paralelinde hazırlanan maddelerden oluşan anket (EK-3) kullanılmıştır.

Çalışma sorularının ana başlıkları şu şekildedir:

- Bölüm 1: Bilgi Güvenliği Politikaları- 5 Soru
- Bölüm 2: Bilgi Güvenliği Organizasyonu-10 Soru
- Bölüm 3: İnsan Kaynakları Güvenliği-10 Soru
- Bölüm 4: Varlık Yönetimi-17 Soru
- Bölüm 5: Erişim Kontrolü-16 Soru
- Bölüm 6: Kriptografi- 3 Soru
- Bölüm 7: Fiziksel ve Çevresel Güvenlik 14 Soru
- Bölüm 8: İşlem Güvenliği 19 Soru
- Bölüm 9: Haberleşme Güvenliği 6 Soru
- Bölüm 10: Sistem Temini, Geliştirme ve Bakımı 11 Soru
- Bölüm 11: Tedarikçi İlişkileri 5 Soru
- Bölüm 12: Bilgi Güvenliği İhlal Olayı Yönetimi 6 Soru
- Bölüm 13: İş Sürekliliğinin Bilgi Güvenliği Hususları 4 Soru
- Bölüm 14: Uyum 5 Soru

2. Kısım, 14 bölüm ve 131 sorudan oluşmakta olup, "Evet", "Hayır" ve "Kısmen" olarak derecelendirilmiştir.

3.8. Araştırmanın Değişkenleri

Bağımlı değişkenler: Farkındalık düzeyi,

Bağımsız değişkenler: Yaş, Medeni Durum, Unvan, Cinsiyet, Eğitim, Deneyim, Görev, Sağlık Tesis Türü

3.9. Araştırmanın Etik Boyutu

Araştırmanın sürdürülebilmesi için Necmettin Erbakan Üniversitesi Sağlık Bilimleri Bilimsel Araştırmalar Etik Kurul izni alınmıştır. Ankara İl Sağlık Müdürlüğü'ne bağlı Sağlık Hizmetleri Başkanlığı ile Destek Hizmetleri Başkanlığının koordinasyonunda çalışmaya katılım izni veren sağlık tesisleri için 31.01.2022 tarih ve E-E-90739940-799-193(Barkod No:

0157942208) sayılı yazı ile anket uygulamasının gerçekleştirilmesi için gerekli izin alınmıştır. Çalışanların araştırmaya katılımında gönüllülük esas alınmıştır. (EK 2).

3.10. Araştırmanın Sınırlılıkları

Araştırmada veri toplama usülü çevrimiçi kanallar aracılığıyla yapılmıştır. Ankara il sınırları içerisinde yer alan tüm sağlık tesisleri pandemi sürecinde olması, sağlık tesisleri arasındaki mesafe ile maliyet ve zaman açısından çalışma çevrimiçi yöntemle yapılmıştır. Bu nedenle araştırma sonuçları, sadece güncel araştırmadaki örneklem grubuna genellenebilir. Araştırmanın Türkiye'de bulunan tüm sağlık tesislerinin genellenebilmesi için daha geniş kapsamlı örneklem üzerinde çalışılması gerekmektedir.

3.11. Araştırmanın Problemi

3.11.1. Araştırma soruları

Bu kapsamda araştırmanın soruları aşağıdaki gibidir:

S_1: Cinsiyet ile Bilgi Güvenliği yönetimi kavramsal farkındalık düzeyi arasında anlamlı bir ilişki var mıdır?

S_2: Mesleki deneyimlere göre Bilgi Güvenliği yönetimi kavramsal farkındalık düzeyi arasında anlamlı bir ilişki var mıdır?

S_3: Eğitim durumu ile Bilgi Güvenliği yönetimi kavramsal farkındalık düzeyi arasında anlamlı bir ilişki var mıdır?

S_4: Unvanlar ile Bilgi Güvenliği yönetimi kavramsal farkındalık düzeyi arasında anlamlı bir ilişki var mıdır?

S_5: Çalıştığı Kurum türü ile Bilgi Güvenliği yönetimi kavramsal farkındalık düzeyi arasında anlamlı bir ilişki var mıdır?

S_6: Çalıştığı Kurum Kapasitesi ile Bilgi Güvenliği yönetimi kavramsal farkındalık düzeyi arasında anlamlı bir ilişki var mıdır?

S_7: 3. *ISO27001 Bilgi Yönetim Sistem Politikaları ile Sağlık Bakanlığı Bilgi Yönetim Politikaları farkındalık düzeyi arasında anlamlı bir ilişki var mıdır?*

Bu araştırmada bilgi güvenliği politikaları bölümlerine göre sağlık kurumları bilgi işlem birimi çalışanlarının; cinsiyete, deneyime, eğitim düzeyine, unvana, çalıştığı birime, çalıştığı kurumun türüne ve çalıştığı kurumun kapasitesine göre değişmekte midir?" sorusuna göre alt problemler oluşturularak yanıt aranmaktadır.

3.12. Verilerin İstatistiksel Değerlendirmesi:

İlk olarak araştırmaya gönüllü olarak katılan 268 sağlık çalışanının veri toplama aracına verdiği cevaplar SPSS 21 programına aktarılmıştır. Anket verilerinin kayıp ve uç değerler için ön analizleri yapılmıştır. Bu ön analizlere bağlı olarak maddelerin bir kısmına cevap vermeyen ve uç değer olarak gözlemlenen kişiler veri setinden çıkarılmış ve araştırmanın sonuçları 260 çalışana ait cevaplardan elde edilmiştir.

Sağlık çalışanlarının bilgi güvenliği yönetim farkındalığını değerlendirme formunda yer alan her soruya verdikleri evet, kısmen ve hayır cevaplarına karşılık olarak sırasıyla 2, 1 ve 0 olarak puan verilmiş ve çalışanların ilgili bölüm soruları toplanarak bölüm puanları elde edilmiştir. Bilgi Güvenliği Yönetim Farkındalığını değerlendirme formunda yer alan 14 alt bölüm puanlarının normalliği hem genel toplam hem de bağımsız değişkenlerin her bir kategorisi için basıklık ve çarpıklık katsayıları incelenerek değerlendirilmiştir. Basıklık ve çarpıklık katsayılarının ±1.5 sınırı içerisinde bulunması durumunda veri setinin normal dağıldığı kabul edilmektedir (Pituch ve Stevens, 2016, s.228). Ancak bu araştırmada anket formundan elde bu katsayıların ±1,5 dışında kaldığı gözlenmiş ve bölüm puanlarının normal dağılmadığı sonucuna ulaşılmıştır.

Tablo 3.12.1. Bölüm Puanlarının Çarpıklık Ve Basıklık Değerleri

Bölüm	Çarpıklık	Çarpıklık hatası	Basıklık	Basıklık hatası
Bilgi Güvenliği Politikaları	-2,188	,151	3,867	,301
Bilgi Güvenliği Organizasyonu	-1,486	,151	1,702	,301
İnsan Kaynakları Güvenliği	-1,636	,151	2,216	,301
Varlık Yönetimi	-1,914	,151	3,318	,301
Erişim Kontrolü	-2,445	,151	6,059	,301
Kriptografi	-1,959	,151	3,136	,301
Fiziksel ve Çevresel Güvenlik	-1,924	,151	2,704	,301
İşlem Güvenliği	-1,685	,151	2,067	,301
Haberleşme Güvenliği	-1,577	,151	1,671	,301
Sistem Temini, Geliştirme Ve Bakımı	-1,676	,151	2,058	,301
Tedarikçi İlişkileri	-1,774	,151	2,437	,301
Bilgi Güvenliği İhlal Olayı Yönetimi	-1,837	,151	2,799	,301
İş Sürekliliğinin Bilgi Güvenliği Hususları	-1,681	,151	2,108	,301
Uyum	-1,684	,151	1,616	,301

Bölüm puanları normal dağılmadığı için cinsiyet ve unvan değişkenleri için grup ortalamalarının karşılaştırılmasında parametrik olmayan yöntemlerden Mann_Whitney U testi kullanılmıştır. Benzer şekilde ikiden fazla düzeyi olan sağlık çalışanlarının çalıştığı kuruluşun türü, kapasitesi, birimi ile çalışanların eğitim durumu ve deneyimi değişkenlerinde grup

ortalamalarının karşılaştırılmasında parametrik olmayan yöntemlerden Kruskall-Wallis H testi kullanılmıştır.

Çalışanların 14 bölüme ilişkin genel görüşleri bölüm ortalamaları ve bölüm ortalama düzeyleri incelenerek değerlendirilmiştir. Bölüm ortalama düzeyleri her bir katılımcının bölüm toplam puanlarının bölümdeki soru sayısına bölünmesi ile elde edilmiştir. Genel ortalama düzeyleri ise hayır, kısmen ve evet kategorilerine bölünerek yorumlanmıştır. Kategoriler, anketteki sorular üçlü derecelendiği için hesaplanan aralık katsayısına göre (2/3=0,69) şu şekilde düzenlemiştir: hayır=0,00-0,68; kısmen=0,69-1,37; evet=1,38-2,00.

Her bir araştırma problemi için alt amaç soru gruplarına ait Cronbach Alfa değerleri Tablo2 'de gösterilmiştir. Cronbach Alfa değerleri incelendiğinde sonuçların 0,88 ile 0,98 arasında olduğu görülmüş ve analizlerde kullanılan ölçeklerin güvenilir oldukları gözlenmiştir.

Tablo 3.12.2. Bölümlerin Güvenirlik Değerleri

Bölüm	Madde sayısı	Güvenirlik
Bilgi Güvenliği Politikaları	5	0,95
Bilgi Güvenliği Organizasyonu	10	0,91
İnsan Kaynakları Güvenliği	10	0,92
Varlık Yönetimi	17	0,97
Erişim Kontrolü	16	0,98
Kriptografi	3	0,93
Fiziksel ve Çevresel Güvenlik	14	0,96
İşlem Güvenliği	19	0,97
Haberleşme Güvenliği	6	0,88
Sistem Temini, Geliştirme ve Bakımı	11	0,96
Tedarikçi İlişkileri	5	0,94
Bilgi Güvenliği İhlal Olayı Yönetimi	6	0,94
İş Sürekliliğinin Bilgi Güvenliği Hususları	4	0,91
Uyum	5	0,93

Bilgi Güvenliği Yönetim Farkındalığını değerlendirme formunda yer alan 14 alt bölüm puanlarının güvenirliği Cronbach Alfa katsayısı ile incelenmiş ve sonuçlar Tablo 2'de özetlenmiştir. Büyüköztürk (2011, s.171) güvenirlik katsayısının 0,70 ve üzerinde olması ölçme aracında elde edilen puanların güvenirliği için yeterli görüldüğü belirtilmektedir. Buna göre bölüm puanlarının güvenilir olduğu sonucuna varılmıştır.

4. BULGULAR

Bu bölümde, Ankara ili sağlık kurumları bilgi işlem birimi çalışanlarının demografik özellikleri ile "ISO/IEC 27001 Bilgi Teknolojisi, Güvenlik Teknikleri, Bilgi Güvenliği Yönetim Sistemleri, Gereksinimler dokümanı EK-A' da yer alan Referans Kontrol Amaçları ve Kontroller başlığı altında yer alan kontrol listesi paralelinde hazırlanan maddelerin; cinsiyete, deneyime, eğitim düzeyine, unvana, çalıştığı birime, çalıştığı kurumun türüne ve çalıştığı kurumun kapasitesine göre bilgi güvenliği yönetim farkındalığı arasındaki ilişkiyi bulmak amacıyla SPSS programı ile gerçekleştirilmiş olan analizler, elde edilen bulgular ve yorumlamalar yer almaktadır.

4.1. Demografik Özellikler

Tablo 4.1.1. Ankete Katılanların Tanımlayıcı Özelliklerine İlişkin Bulgular

Sosyodemografik Özellikler		Sayı(n)	Yüzde%
Eğitim Durumu	Lise	76	29,2
	Yüksekokul	66	25,4
	Lisans	91	35
	Lisansüstü	27	10,4
Yaş	18-25 yaş	7	2,7
	26-33 yaş	54	20,8
	34-41 yaş	98	37,6
	42-49 yaş	68	26,2
	50-57 yaş	30	11,5
	58-64 yaş	3	1,2
Cinsiyet	Kadın	71	27,3
	Erkek	189	72,7
Medeni Durum	Evli	208	80
	Bekar	52	20
Gelir	4000 TL ve altı	20	7,7
	4001-6000 TL	97	37,3
	6001-8000 TL	89	34,2
	8001 TL ve üstü	54	20,8
Çalışma Süresi	0-1 yıl	11	4,2
	2-5 yıl	44	16,9
	6-10 yıl	66	25,4
	11-15 yıl	52	20
	16-20 yıl	39	15
	21 ve üzeri	48	18,5

Tablo 4.1.1. incelendiğinde çalışanları %29,2 lise, %25,4 yüksekokul, %35'i lisans ve %10,4 lisans üstü eğitime sahip olup, 37,7'si 34-41 yaş aralığında, 26,2'sı 42,49 yaş aralığındadır. Ankete katılanların %27,3 kadın, %72,7'si erkek olup katılımcıların %80,00 evlidir. Katılımcıların %25'i 6-10 yıl, %20'si 11-15 yıl arasında çalışma yılına sahiptirler.

Tablo 4.1.2. Ankete Katılanların Çalıştıkları Sağlık Kuruluşlarına Göre Dağılımı

Sağlık Tesisi	Sayı(n)	Yüzde%
2. ve 3. Basamak Sağlık Tesisi	172	66,1
ADSM ve Diş Hastanesi	26	10
İlçe Sağlık Müdürlüğü	14	5,4
İl Sağlık Müdürlüğü ve Bağlı Birimler	48	18,5
Toplam	260	100

Tablo 4.1.2 de görüldüğü üzere ankete katılan 260 sağlık çalışanın %66,2'si 2.ve 3.basamak sağlık tesisi kapsamında yer alan sağlık kuruluşlarında çalışırken, %18,5'i il sağlık müdürlüğü ve bağlı birimlerde çalışan bilgi işlem personelini ve yöneticilerini oluşturmaktadır.

Tablo 4.1.3. Ankete Katılanların Çalıştıkları Sağlık Kuruluşlarında Unvan ve Görev Dağılımı

Unvan ve Görev Dağılımı		Sayı(n)	Yüzde%
Unvan	Başhekim, Başhekim Yardımcısı (Doktor, Diş Hekimi)	10	3,8
	Bilgi İşlem/ HBYS Birim Sorumlusu	12	4,6
	Bilgi İşlem/HBYS Personeli (Tekniker, Teknisyen)	163	62,7
	Bilgisayar Mühendisi	5	1,9
	Hastane Müdür/Müdür Yardımcısı	16	6,2
	İstatistikçi	2	0,8
	Programcı	6	2,3
	Şube Müdürü, Araştırmacı, Apk Uzmanı	8	3,1
	Tıbbi Teknolog	1	0,4
	Uzman (İdari Yönetici/Bilgi İşlem/ Birim Sorumlusu)	11	4,2
	V.H.K. İ	15	5,8
	Yardımcı Sağlık Personeli	11	4,2
Çalışılan Birimler	Bilgi işlem Birimi	172	66,2
	Yönetim	30	11,5
	Tıbbi Birimler	34	13,1
	İdari Birimler	24	9,2
Görevi	Yönetici (Başhekim, Hastane Müd. Uzman, Şube Müd. Vb)	45	17,3
	Bilgi İşlem Personeli	215	82,7

Tablo 4.1.3 incelendiğinde ankete katılan sağlık çalışanlarının dağılımları görülmektedir. Katılımcılardan%62,7'si kamu alımları ile yerleşen tekniker, teknisyen veya hizmet alım yöntemi ile ihale çalışan bilgi işlem/HBYS personelinden oluşmaktadır. Katılımcılar %66,2'si bilgi işlem biriminde doğrudan çalışırken, diğer katılımcıları sağlık tesisi içerisinde yönetim, tıbbi ve idari birimlerde çalışmaktadırlar.

Araştırmaya katılan katılımcılardan %17,3'ü sağlık tesislerinde yönetici (İlçe Sağlık Müdürü, Başhekim, Başhekim yardımcısı, Müdür, Müdür Yardımcısı, Şube Müdürü, Uzman) olarak yer almaktadırlar.

4.2. Fark İstatistikleri:

Bu bölümde bulgular alt problemlerin sırasına uygun olarak ayrı başlıklar halinde sunulmuştur.

4.2.1. Bilgi güvenliği politikaları alt bölümüne ilişkin bulgular

Bilgi güvenliği politikaları bölümüne çalışanların verdiği cevapların ortalaması 8,78'dir (medyan=10,00) ve çalışanların ortalama görüşlerinin 1,76 ile evet düzeyinde olduğu gözlenmiştir. Sağlık personelinin cinsiyete, deneyime, eğitim düzeyine, unvana, çalıştığı birime, çalıştığı kurumun türüne ve çalıştığı kurumun kapasitesine göre bilgi güvenliği politikaları ortalamaları arasındaki ilişkiler aşağıda özetlenmiştir.

Tablo 4.2.1. Bilgi Güvenliği Politikaları Bölüm Puanının Cinsiyet ve Unvana Göre Mann-Whitney U Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	Z	p
Cinsiyet	Kadın	71	8,49	123,70	2,70	-1,16	0,25
	Erkek	189	8,89	133,05	2,48		
Unvan	Yönetici	45	8,27	120,03	3,04	-1,32	0,18
	Bilgi işlem personeli	215	8,89	132,69	2,42		

Tablo 4.2.1. incelendiğinde kadın çalışanların bilgi güvenliği politikaları bölüm ortalaması ile erkek personelin ortalamalar arasında gözlenen farklar istatistiksel olarak anlamlı bulunmamıştır (Z=-1,16; p>0,05).

Tablo 4.2.2 Bilgi Güvenliği Politikaları Bölüm Puanının Çalışanların Eğitim Düzeyi ve Deneyimine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Eğitim	Lise	76	8,75	131,41	2,66	3,57	0,31
	Yüksekokul	66	9,12	136,05	2,02		
	Lisans	91	8,74	131,38	2,76		
	Lisansüstü	27	8,19	111,37	2,57		
Kıdem	0-1 yıl	11	9,09	131,36	1,81	9,01	0,11
	2-5 yıl	44	9,59	148,41	1,44		
	6-10 yıl	66	8,41	120,76	2,80		
	11-15 yıl	52	9,08	139,18	2,19		
	16-20 yıl	39	8,41	118,38	2,84		
	21 ve üzeri	48	8,46	127,72	3,07		

Tablo 4.2.2 incelendiğinde lise, yüksekokul, lisans ve lisan üstü eğitim düzeyinde çalışanların bilgi güvenliği politikaları bölüm ortalaması görülmektedir. Bölüm puanı ile

personelin eğitim düzeyi arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=3,57; p>0,05). Kıdem yılı açısından sağlık kuruluşunda çalışan personelin bilgi güvenliği politikaları bölüm ortalaması incelenmiş olup, personelin kıdem yılı arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ2=9,01; p>0,05).

Tablo 4.2.3 Bilgi Güvenliği Politikaları Bölüm Puanının Çalışanların Birimine Göre Kruskall-Wallis H Testi Sonucu

Birim	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Bilgi işlem	172	8,93	132,67	2,37	1,55	0,67
Yönetim	30	8,80	130,10	2,41		
Tıbbi	34	8,68	129,40	2,69		
İdari	24	7,83	117,00	3,50		

Tablo 4.2.3. incelendiğinde bilgi işlem birimi, yönetim kademesi, tıbbi hizmetler birimi ve idari kısımda çalışanların bilgi güvenliği politikaları bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=1,55; p>0,05). Birimlere göre katılımcıların çalıştıkları yerlere göre benzer düzeyde bilgi güvenliği politikaları farkındalığına sahiptirler.

Tablo 4.2.4 Bilgi Güvenliği Politikaları Bölüm Puanının Personelin Çalıştığı Sağlık Kuruluşunun Türü ve Kapasitesine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p	Fark
Tür	2. ve 3. Basamak Sağlık Tesisi	172	8,91	134,81	2,45	3,63	0,22	-
	ADSM ve Diş Hastanesi	26	9,23	144,17	2,21			
	İlçe Sağlık Müdürlüğü	14	7,07	96,07	3,93			
	İl Sağlık Müdürlüğü	48	8,56	117,71	2,40			
Kapasite	Büyük (1)	119	8,66	131,43	2,74	10,08	0,01*	2-3
	Küçük(2)	80	9,40	143,24	1,74			
	İdari (3)	61	8,20	111,98	2,87			

*p<0,05

Tablo 4.2.4. incelendiğinde 2.-3. Basamak hastanede, ADSM ve Diş Hastanesinde, İlçe Sağlık Müdürlüğünde ve İl Sağlık Müdürlüğünde çalışanların bilgi güvenliği politikaları bölüm puanı ile personelin hangi tür kurumda çalıştığı arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=3,63; p>0,05). Kapasitesi açısından büyük, küçük ve idari sağlık kuruluşunda çalışan personelin bilgi güvenliği politikaları arasında gözlenen bu farkların en az

biri istatistiksel olarak anlamlıdır (χ^2=10,08; p<0,05). Farkın kaynağını belirlemek için yapılan Dunn testleri sonucunda yalnızca küçük kuruluşlarda çalışan personelin bilgi güvenliği politikaları bölüm ortalaması idari kuruluşlarda çalışanlardan daha yüksek bulunuştur.

4.2.2. Bilgi güvenliği organizasyonu alt bölümüne ilişkin bulgular

Bilgi güvenliği organizasyonu bölümüne çalışanların verdiği cevapların ortalaması 16,06'dır (medyan=18,00) ve çalışanların ortalama görüşlerinin 1,61 ile evet düzeyinde olduğu gözlenmiştir. Sağlık personelinin cinsiyete, deneyime, eğitim düzeyine, unvana, çalıştığı birime, çalıştığı kurumun türüne ve çalıştığı kurumun kapasitesine göre bilgi güvenliği organizasyonu ortalamaları arasındaki ilişkiler aşağıda özetlenmiştir.

Tablo 4.2.5. Bilgi Güvenliği Organizasyonu Bölüm Puanının Cinsiyet ve Unvana Göre Mann-Whitney U Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	Z	p
Cinsiyet	Kadın	71	16,38	136,12	4,75	-0,76	0,45
	Erkek	189	15,94	128,39	5,04		
Unvan	Yönetici	45	15,47	124,69	5,55	-0,59	0,56
	Bilgi işlem personeli	215	16,19	131,72	4,83		

Tablo 4.2.5 incelendiğinde kadın çalışanların bilgi güvenliği organizasyonları bölüm ortalamaları arasında gözlenen farklar istatistiksel olarak anlamlı bulunmamıştır (Z=-0,76; p>0,05). Yöneticilerin ($\bar{X}$=15,47) ve bilgi işlem personelinin ($\bar{X}$=16,19) ortalamaları istatistiksel olarak benzerdir (Z=-0,59; p>0,05).

Tablo 4.2.6. Bilgi Güvenliği Organizasyonu Bölüm Puanının Çalışanların Eğitim Düzeyi ve Deneyimine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Eğitim	Lise	76	16,50	141,51	5,10	4,71	0,20
	Yüksekokul	66	16,59	135,10	4,35		
	Lisans	91	15,68	123,81	5,15		
	Lisansüstü	27	14,81	110,81	5,26		
Kıdem	0-1 yıl	11	16,73	137,05	4,20	5,58	0,35
	2-5 yıl	44	16,05	125,28	4,33		
	6-10 yıl	66	15,94	131,84	5,35		
	11-15 yıl	52	16,67	139,47	4,49		
	16-20 yıl	39	15,21	108,27	4,82		
	21 ve üzeri	48	16,13	140,28	5,77		

Tablo 4.2.6 incelendiğinde lise, yüksekokul, lisans ve lisan üstü eğitim düzeyinde çalışanların bilgi güvenliği organizasyonları bölüm puanı ile personelin eğitim düzeyi arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=4,71; p>0,05). Kıdem yılı açısından sağlık kuruluşunda çalışan personelin bilgi güvenliği organizasyonları bölüm ortalaması ve personelin kıdem yılı arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ2=5,58; p>0,05).

Tablo 4.2.7. Bilgi Güvenliği Organizasyonu Bölüm Puanının Çalışanların Birimine Göre Kruskall-Wallis H Testi Sonucu

Birim	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Bilgi işlem	172	15,83	122,92	4,73	7,03	0,07
Yönetim	30	17,03	143,78	3,98		
Tıbbi	34	16,91	156,12	5,62		
İdari	24	15,33	131,94	6,51		

Tablo 4.2.7 incelendiğinde Bilgi işlem birimi, Yönetim kademesi, Tıbbi hizmetler birimi ve İdari kısımda çalışanların bilgi güvenliği organizasyonları bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=7,03; p>0,05). Birimlere göre katılımcıların çalıştıkları yerlere göre benzer düzeyde bilgi güvenliği organizasyon farkındalığına sahiptirler.

Tablo 4.2.8. Bilgi Güvenliği Organizasyonu Bölüm Puanının Personelin Çalıştığı Sağlık Kuruluşunun Türü ve Kapasitesine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Tür	2. ve 3. Basamak Sağlık Tesisi	172	16,06	130,33	5,03	4,94	0,18
	ADSM ve Diş Hastanesi	26	16,50	128,40	4,00		
	İlçe Sağlık Müdürlüğü	14	13,14	93,79	6,53		
	İl Sağlık Müdürlüğü	48	16,67	142,94	4,48		
Kapasite	Büyük	119	16,30	137,57	5,20	2,227	0,25
	Küçük	80	15,90	119,97	4,43		
	İdari	61	15,80	130,52	5,19		

Tablo 4.2.8 incelendiğinde 2.- 3. Basamak hastanede, ADSM ve Diş Hastanesinde, İlçe Sağlık Müdürlüğünde ve İl Sağlık Müdürlüğünde çalışanların bilgi güvenliği organizasyonları bölüm puanı ile personelin hangi tür kurumda çalıştığı arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=4,94; p>0,05). Kapasitesi açısından büyük, küçük ve idari sağlık kuruluşunda çalışan personelin bilgi güvenliği organizasyonları bölüm puanı ile personelin çalıştığı sağlık tesisinin kapasitesi açısından anlamlı bir ilişki bulunmamıştır (χ^2=2,227; p>0,05).

4.2.3. İnsan kaynakları güvenliği alt bölümüne ilişkin bulgular

İnsan Kaynakları Güvenliği bölümüne çalışanların verdiği cevapların ortalaması 16,78'dir (medyan=19,00) ve çalışanların ortalama görüşlerinin 1,68 ile evet düzeyinde olduğu gözlenmiştir. Sağlık personelinin cinsiyete, deneyime, eğitim düzeyine, unvana, çalıştığı birime, çalıştığı kurumun türüne ve çalıştığı kurumun kapasitesine göre insan kaynakları güvenliği ortalamaları arasındaki ilişkiler aşağıda özetlenmiştir.

Tablo 4.2.9. İnsan Kaynakları Güvenliği Bölüm Puanının Cinsiyet ve Unvana Göre Mann-Whitney U Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	Z	p
Cinsiyet	Kadın	71	17,34	137,80	3,98	-1,02	0,31
	Erkek	189	16,57	127,76	4,84		
Unvan	Yönetici	45	16,18	126,46	5,51	-0,42	0,67
	Bilgi işlem personeli	215	16,90	131,35	4,43		

Tablo 4.2.9 incelendiğinde kadın çalışanların insan kaynakları güvenliği organizasyonları arasında gözlenen farklar istatistiksel olarak anlamlı bulunmamıştır (Z=-1,02; p>0,05). Yöneticilerin ve bilgi işlem personelinin ortalamaları istatistiksel olarak benzerdir (Z=-0,42; p>0,05).

Tablo 4.2. 10. İnsan Kaynakları Güvenliği Bölüm Puanının Çalışanların Eğitim Düzeyi ve Deneyimine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Eğitim	Lise	76	17,17	139,63	4,69	7,80	0,06
	Yüksekokul	66	17,14	135,75	4,38		
	Lisans	91	16,69	129,13	4,54		
	Lisans üstü	27	15,07	96,59	5,17		
Kıdem	0-1 yıl	11	16,09	120,18	4,74	1,51	0,91
	2-5 yıl	44	17,36	134,93	3,69		
	6-10 yıl	66	16,65	129,46	4,79		
	11-15 yıl	52	17,13	137,75	4,46		
	16-20 yıl	39	16,13	122,18	5,45		
	21 ve üzeri	48	16,71	129,14	4,74		

Tablo 4.2.10 incelendiğinde lise, yüksekokul, lisans ve lisan üstü eğitim düzeyinde çalışanların insan kaynakları güvenliği bölüm puanı ile personelin eğitim düzeyi arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=7,80; p>0,05). Kıdem yılı açısından sağlık kuruluşunda çalışan personelin insan kaynakları güvenliği bölüm ortalaması ve personelin kıdem yılı arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ2=1,51; p>0,05).

Tablo 4.2.11. İnsan Kaynakları Güvenliği Bölüm Puanının Çalışanların Birimine Göre Kruskall-Wallis H Testi Sonucu

Birim	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Bilgi işlem	172	16,64	126,15	4,51	6,20	0,10
Yönetim	30	18,17	153,30	3,54		
Tıbbi	34	17,24	143,87	4,64		
İdari	24	15,38	114,27	6,16		

Tablo 4.2.11 incelendiğinde Bilgi işlem birimi, Yönetim kademesi, Tıbbi hizmetler birimi ve İdari kısımda çalışanların insan kaynakları güvenliği bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=6,20; p>0,05). Birimlere göre katılımcıların çalıştıkları yerlere göre benzer düzeyde insan kaynakları güvenliği farkındalığına sahiptirler.

Tablo 4.2.12. İnsan Kaynakları Güvenliği Bölüm Puanının Personelin Çalıştığı Sağlık Kuruluşunun Türü ve Kapasitesine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p	Fark
Tür	2. ve 3. Basamak Sağlık Tesisi (1)	172	16,98	132,43	4,49	8,86	0,03	2-3
	ADSM ve Diş Hastanesi (2)	26	18,27	157,56	3,69			
	İlçe Sağlık Müdürlüğü (3)	14	14,00	93,18	6,30			
	İl Sağlık Müdürlüğü (4)	48	16,04	119,80	4,71			
Kapasite	Büyük	119	16,74	134,23	5,02	5,374	0,07	-
	Küçük	80	17,80	138,76	3,19			
	İdari	61	15,51	112,39	5,14			

Tablo 4.2.12 incelendiğinde 2.- 3. Basamak sağlık tesisi, ADSM ve Diş Hastanesinde, İlçe Sağlık Müdürlüğünde ve İl Sağlık Müdürlüğünde çalışanların insan kaynakları güvenliği bölüm ortalaması açısından gözlenen farkların en az biri istatistiksel olarak anlamlıdır (χ2=8,86; p<0,05). Farkın kaynağını belirlemek için yapılan Dunn testleri sonucunda yalnızca ADSM ve Diş Hastanesinde çalışan personelin bilgi güvenliği politikaları bölüm ortalaması İlçe Sağlık Müdürlüğü çalışanlardan daha yüksek bulunuştur. Kapasitesi açısından büyük, küçük ve idari sağlık kuruluşunda çalışan personelin insan kaynakları güvenliği bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ2=5,374; p<0,05).

4.2.4. Varlık yönetimi alt bölümüne ilişkin bulgular

Varlık yönetimi bölümüne çalışanların verdiği cevapların ortalaması 29,68'dir (medyan=34,00) ve çalışanların ortalama görüşlerinin 1,75 ile evet düzeyinde olduğu gözlenmiştir. Sağlık personelinin cinsiyete, deneyime, eğitim düzeyine, unvana, çalıştığı birime, çalıştığı kurumun türüne ve çalıştığı kurumun kapasitesine göre varlık yönetimi ortalamaları arasındaki ilişkiler aşağıda özetlenmiştir.

Tablo 4.2.13. Varlık Yönetimi Bölüm Puanının Cinsiyet ve Unvana Göre Mann-Whitney U Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	Z	p
Cinsiyet	Kadın	71	29,70	131,41	7,11	-0,13	0,90
	Erkek	189	29,68	130,16	7,39		
Unvan	Yönetici	45	29,24	133,58	8,21	-0,34	0,74
	Bilgi işlem personeli	215	29,78	129,86	7,11		

Tablo 4.2.13 incelendiğinde kadın çalışanların varlık yönetimi bölüm ortalaması açısından gözlenen farklar istatistiksel olarak anlamlı bulunmamıştır (Z=-0,13; p>0,05). Yöneticilerin ve bilgi işlem personelinin ortalamaları istatistiksel olarak benzerdir (Z=-0,34; p>0,05).

Tablo 4.2. 14. Varlık Yönetimi Bölüm Puanının Çalışanların Eğitim Düzeyi ve Deneyimine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p	Fark
Eğitim	Lise (1)	76	30,54	141,11	6,63	8,31	0,04	1-4
	Yüksekokul (2)	66	33,70	130,30	6,86			
	Lisans (3)	91	32,70	120,54	8,02			
	Lisans üstü (4)	27	29,85	107,48	9,97			
Kıdem	0-1 yıl	11	28,27	128,00	8,06	2,18	0,82	
	2-5 yıl	44	30,48	135,32	5,53			
	6-10 yıl	66	29,15	134,15	8,94			
	11-15 yıl	52	29,69	121,23	6,00			
	16-20 yıl	39	29,21	124,10	8,08			
	21 ve üzeri	48	30,40	136,88	6,87			

Tablo 4.2. 14 incelendiğinde lise, yüksekokul, lisans ve lisan üstü eğitim düzeyinde çalışanların varlık yönetimi bölüm puanı ile personelin eğitim düzeyi arasında istatiksel olarak gözlenen farkların en az biri istatistiksel olarak anlamlıdır (χ^2=8,31; p>0,05). Farkın kaynağını belirlemek için yapılan Dunn testleri sonucunda yalnızca lise eğitim düzeyine sahip personelin varlık yönetimi bölüm ortalaması eğitim düzeyi lisans üstü eğitim düzeyine sahip personelden

daha yüksek bulunuştur. Kıdem yılı sağlık kuruluşunda çalışan personelin bilgi güvenliği politikaları ve personelin kıdem yılı arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır ($\chi 2=2,18$; $p>0,05$).

Tablo 4.2.15. Varlık Yönetimi Bölüm Puanının Çalışanların Birimine Göre Kruskall-Wallis H Testi Sonucu

Birim	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Bilgi işlem	172	29,62	126,67	7,07	3,67	0,30
Yönetim	30	31,40	151,58	5,86		
Tıbbi	34	29,59	134,40	8,07		
İdari	24	28,17	126,08	9,23		

Tablo 4.2.15 incelendiğinde Bilgi işlem birimi, Yönetim kademesi, Tıbbi hizmetler birimi ve İdari kısımda çalışanların varlık yönetimi bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır ($\chi^2=3,67$; $p>0,05$). Birimlere göre katılımcıların çalıştıkları yerlere göre benzer düzeyde varlık yönetimi farkındalığına sahiptirler.

Tablo 4.2.16. Varlık Yönetimi Bölüm Puanının Personelin Çalıştığı Sağlık Kuruluşunun Türü ve Kapasitesine Göre Kruskall-Wallis H Testi Sonucu

Değişken	**Düzey**	**n**	**$\bar{X}$**	**Sıra Ortalaması**	**S.S.**	**χ^2**	**p**
Tür	2. ve 3. Basamak Sağlık Tesisi	172	29,85	132,31	7,37	3,97	0,27
	ADSM ve Diş Hastanesi	26	31,38	140,77	4,77		
	İlçe Sağlık Müdürlüğü	14	25,50	98,25	10,88		
	İl Sağlık Müdürlüğü	48	29,40	127,85	6,63		
					Tablo 4.2.16. devamı		
Kapasite	Büyük	119	29,85	138,71	7,99	3,249	0,20
	Küçük	80	30,20	124,33	5,64		
	İdari	61	28,69	122,58	7,81		

Tablo 4.2.16 incelendiğinde 2.-3. Basamak hastanede, ADSM ve Diş Hastanesinde, İlçe Sağlık Müdürlüğünde ve İl Sağlık Müdürlüğünde çalışanların varlık yönetimi bölüm puanı ile personelin hangi tür kurumda çalıştığı arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır ($\chi^2=3,97$; $p>0,05$). Kapasitesi açısından büyük, küçük ve idari sağlık kuruluşunda çalışan personelin varlık yönetimi organizasyonları bölüm puanı ile personelin çalıştığı sağlık tesisinin kapasitesi açısından anlamlı bir ilişki bulunmamıştır ($\chi^2=3,249$; $p>0,05$).

4.2.5. Erişim kontrolü alt bölümüne ilişkin bulgular

Erişim kontrolü bölümüne çalışanların verdiği cevapların ortalaması 28,69'dur (medyan=32,00) ve çalışanların ortalama görüşlerinin 1,79 ile evet düzeyinde olduğu gözlenmiştir. Sağlık personelinin cinsiyete, deneyime, eğitim düzeyine, unvana, çalıştığı birime, çalıştığı kurumun türüne ve çalıştığı kurumun kapasitesine göre erişim kontrolü ortalamaları arasındaki ilişkiler aşağıda özetlenmiştir.

Tablo 4.2.17. Erişim Kontrolü Bölüm Puanının Cinsiyet ve Unvana Göre Mann-Whitney U Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	Z	p
Cinsiyet	Kadın	71	28,80	130,26	6,32	-0,04	0,97
	Erkek	189	28,65	130,59	6,74		
Unvan	Yönetici	45	28,31	134,23	7,11	-0,43	0,67
	Bilgi işlem personeli	215	28,77	129,72	6,52		

Tablo 4.2.17 incelendiğinde kadın çalışanların erişim kontrolü bölüm ortalamalar arasında gözlenen farklar istatistiksel olarak anlamlı bulunmamıştır (Z=-0,04; p>0,05). Yöneticilerin ve bilgi işlem personelinin ortalamaları istatistiksel olarak benzerdir (Z=-0,43; p>0,05).

Tablo 4.2.18. Erişim Kontrolü Bölüm Puanının Çalışanların Eğitim Düzeyi ve Deneyimine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Eğitim	Lise	76	29,37	142,34	6,00	6,03	0,11
	Yüksekokul	66	28,83	128,44	6,25		
	Lisans	91	29,19	128,87	5,58		
	Lisans üstü	27	24,78	107,70	10,42		
Kıdem	0-1 yıl	11	28,45	127,32	6,31	4,85	0,43
	2-5 yıl	44	30,09	143,09	4,02		
	6-10 yıl	66	27,82	127,14	8,52		
	11-15 yıl	52	28,79	121,80	5,16		
	16-20 yıl	39	27,79	121,49	8,03		
	21 ve üzeri	48	29,29	141,05	5,70		

Tablo 4.2.18 incelendiğinde lise, yüksekokul, lisans ve lisan üstü eğitim düzeyinde çalışanların erişim kontrolü bölüm puanı ile personelin eğitim düzeyi arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=6,03; p>0,05). Kıdem yılı açısından sağlık kuruluşunda çalışan personelin erişim kontrolü bölüm ortalaması ve personelin kıdem yılı arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ2=4,85; p>0,05).

Tablo 4.2.19. Erişim Kontrolü Bölüm Puanının Çalışanların Birimine Göre Kruskall-Wallis H Testi Sonucu

Birim	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Bilgi işlem	172	28,64	128,08	6,57	5,03	0,17
Yönetim	30	30,33	154,85	4,59		
Tıbbi	34	28,32	127,60	7,30		
İdari	24	27,54	121,52	7,98		

Tablo 4.2.19 incelendiğinde Bilgi işlem birimi, Yönetim kademesi, Tıbbi hizmetler birimi ve İdari kısımda çalışanların erişim kontrolü güvenliği bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=5,03; p>0,05). Birimlere göre katılımcıların çalıştıkları yerlere göre benzer düzeyde erişim kontrolü güvenliği farkındalığına sahiptirler.

Tablo 4.2.20. Erişim Kontrolü Bölüm Puanının Personelin Çalıştığı Sağlık Kuruluşunun Türü ve Kapasitesine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Tür	2. ve 3. Basamak Sağlık Tesisi	172	28,80	131,88	6,81	2,65	0,45
	ADSM ve Diş Hastanesi	26	30,23	137,77	4,09		
	İlçe Sağlık Müdürlüğü	14	24,93	104,75	9,89		
	İl Sağlık Müdürlüğü	48	28,56	129,14	5,54		
Kapasite	Büyük	119	28,76	135,63	7,19	1,397	0,50
	Küçük	80	29,16	126,79	5,59		
	İdari	61	27,93	125,36	6,73		

Tablo 4.2.20 incelendiğinde 2.- 3. Basamak hastanede, ADSM ve Diş Hastanesinde, İlçe Sağlık Müdürlüğünde ve İl Sağlık Müdürlüğünde çalışanların erişim kontrolü bölüm puanı ile personelin hangi tür kurumda çalıştığı arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=2,65; p>0,05). Kapasitesi açısından büyük, küçük ve idari sağlık kuruluşunda çalışan personelin erişim kontrolü bölüm puanı ile personelin çalıştığı sağlık tesisinin kapasitesi açısından anlamlı bir ilişki bulunmamıştır (χ^2=1,397; p>0,05).

4.2.6. Kriptografi alt bölümüne ilişkin bulgular

Kriptografi bölümüne çalışanların verdiği cevapların ortalaması 5,18'dir (medyan=6,00) ve çalışanların ortalama görüşlerinin 1,73 ile evet düzeyinde olduğu gözlenmiştir. Sağlık personelinin cinsiyete, deneyime, eğitim düzeyine, unvana, çalıştığı birime, çalıştığı kurumun türüne ve çalıştığı kurumun kapasitesine göre kriptografi ortalamaları arasındaki ilişkiler aşağıda özetlenmiştir.

Tablo 4.2.21. Kriptografi Bölüm Puanının Cinsiyet ve Unvana Göre Mann-Whitney U Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	Z	p
Cinsiyet	Kadın	71	5,29	136,24	1,49	-0,20	0,07
	Erkek	189	5,26	133,56	1,55		
Unvan	Yönetici	45	5,12	128,26	1,61	-0,35	0,40
	Bilgi işlem personeli	215	5,50	146,68	1,38		

Tablo 4.2.21 incelendiğinde kadın çalışanların kriptografi bölüm ortalaması erkek personelin bölüm ortalaması arasında gözlenen farklar istatistiksel olarak anlamlı bulunmamıştır (Z=0,20; p>0,05). Yöneticilerin ve bilgi işlem personelinin ortalamaları istatistiksel olarak benzerdir (Z=-0,35; p>0,05).

Tablo 4.2.22. Kriptografi Bölüm Puanının Çalışanların Eğitim Düzeyi ve Deneyimine Göre Kruskall-Wallis H Testi Sonucu

Değişken	**Düzey**	**n**	$\bar{X}$	**Sıra Ortalaması**	**S.S.**	χ^2	**p**
Eğitim	Lise	76	5,49	142,13	1,28	6,85	0,77
	Yüksekokul	66	5,20	128,78	1,48		
	Lisans	91	5,13	128,47	1,59		
	Lisans üstü	27	4,48	108,81	2,10		
Kıdem	0-1 yıl	11	5,27	130,73	1,27	3,44	0,63
	2-5 yıl	44	5,45	137,45	1,15		
	6-10 yıl	66	5,00	126,45	1,83		
	11-15 yıl	52	5,31	133,79	1,35		
	16-20 yıl	39	4,77	117,73	1,97		
	21 ve üzeri	48	5,38	136,45	1,31		

Tablo 4.2.22 incelendiğinde lise, yüksekokul, lisans ve lisan üstü eğitim düzeyinde çalışanların kriptografi bölüm puanı ile personelin eğitim düzeyi arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=6,85; p>0,05). Kıdem yılı açısından sağlık kuruluşunda çalışan personelin kriptografi bölüm ortalaması ve personelin kıdem yılı arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ2=3,44; p>0,05).

Tablo 4.2. 23. Kriptografi Bölüm Puanının Çalışanların Birimine Göre Kruskall-Wallis H Testi Sonucu

Birim	**n**	$\bar{X}$	**Sıra Ortalaması**	**S.S.**	χ^2	**p**
Bilgi işlem	172	5,12	128,26	1,61	2,98	0,40
Yönetim	30	5,50	146,68	1,38		
Tıbbi	34	5,32	132,79	1,39		
İdari	24	5,04	123,04	1,63		

Tablo 4.2.23 incelendiğinde Bilgi işlem birimi, Yönetim kademesi, Tıbbi hizmetler birimi ve İdari kısımda çalışanların kriptografi bölüm puanı ile personelin çalıştıkları birim

arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=2,98; p>0,05). Birimlere göre katılımcıların çalıştıkları yerlere göre benzer düzeyde kriptografi farkındalığına sahiptirler.

Tablo 4.2.24. Kriptografi Bölüm Puanının Personelin Çalıştığı Sağlık Kuruluşunun Türü ve Kapasitesine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p	Fark
Tür	2. ve 3. Basamak Sağlık Tesisi (1)	172	5,29	135,70	1,51	10,36	0,02	1-3
	ADSM ve Diş Hastanesi (2)	26	5,31	135,62	1,49			
	İlçe Sağlık Müdürlüğü (3)	14	3,93	86,86	2,20			
	İl Sağlık Müdürlüğü (4)	48	5,10	121,82	1,42			
Kapasite	Büyük	119	5,29	136,24	1,49	5,46	0,07	
	Küçük	80	5,26	133,56	1,55			
	İdari	61	4,87	115,30	1,68			

Tablo 4.2.24 incelendiğinde 2.- 3. Basamak sağlık tesisi, ADSM ve Diş Hastanesinde, İlçe Sağlık Müdürlüğünde ve İl Sağlık Müdürlüğünde çalışanların kriptografi bölüm ortalaması en az biri istatistiksel olarak anlamlıdır (χ2=10,36; p<0,05). Farkın kaynağını belirlemek için yapılan Dunn testleri sonucunda yalnızca 2.- 3. Basamak hastanesinde çalışan personelin kriptografi bölüm ortalaması İlçe Sağlık Müdürlüğü çalışanlardan daha yüksek bulunmuştur. Kapasitesi açısından büyük, küçük ve idari sağlık kuruluşunda çalışan personelin insan kaynakları güvenliği bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ2=5,46; p<0,05).

4.2.7. Fiziksel ve çevresel güvenlik alt bölümüne ilişkin bulgular

Fiziksel ve çevresel güvenlik bölümüne çalışanların verdiği cevapların ortalaması 25,05'tir (medyan=28,00) ve çalışanların ortalama görüşlerinin 1,79 ile evet düzeyinde olduğu gözlenmiştir. Sağlık personelinin cinsiyete, deneyime, eğitim düzeyine, unvana, çalıştığı birime, çalıştığı kurumun türüne ve çalıştığı kurumun kapasitesine göre fiziksel ve çevresel güvenlik ortalamaları arasındaki ilişkiler aşağıda özetlenmiştir.

Tablo 4.2.25. Fiziksel ve Çevresel Güvenlik Bölüm Puanının Cinsiyet ve Unvana Göre Mann-Whitney U Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	Z	p
Cinsiyet	Kadın	71	25,21	132,07	5,03	-0,24	0,81
	Erkek	189	24,99	129,91	5,52		
Unvan	Yönetici	45	24,93	129,02	5,62	-0,17	0,87
	Bilgi işlem personeli	215	25,08	130,81	5,34		

Tablo 4.2.25 incelendiğinde kadın çalışanların fiziksel ve çevresel güvenlik arasında gözlenen farklar istatistiksel olarak anlamlı bulunmamıştır (Z=-0,24; p>0,05). Yöneticilerin ve bilgi işlem personelinin ortalamaları istatistiksel olarak benzerdir (Z=-0,17; p>0,05).

Tablo 4.2.26. Fiziksel ve Çevresel Güvenlik Bölüm Puanının Çalışanların Eğitim Düzeyi ve Deneyimine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Eğitim	Lise	76	25,78	144,80	4,76	6,98	0,07
	Yüksekokul	66	24,98	126,37	5,40		
	Lisans	91	25,37	128,08	4,73		
	Lisans üstü	27	22,11	108,52	7,87		
Kıdem	0-1 yıl	11	24,27	109,09	5,37	2,21	0,82
	2-5 yıl	44	25,36	132,86	4,86		
	6-10 yıl	66	24,62	133,24	6,36		
	11-15 yıl	52	25,02	130,39	5,30		
	16-20 yıl	39	24,95	122,71	5,49		
	21 ve üzeri	48	25,67	135,92	4,51		

Tablo 4.2.26 incelendiğinde lise, yüksekokul, lisans ve lisan üstü eğitim düzeyinde çalışanların fiziksel ve çevresel güvenlik bölüm puanı ile personelin eğitim düzeyi arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=6,98; p>0,05). Kıdem yılı açısından sağlık kuruluşunda çalışan personelin fiziksel ve çevresel güvenlik bölüm ve personelin kıdem yılı arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ2=2,211; p>0,05).

Tablo 4.2.27. Fiziksel ve Çevresel Güvenlik Bölüm Puanının Çalışanların Birimine Göre Kruskall-Wallis H Testi Sonucu

Birim	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Bilgi işlem	172	24,92	126,62	5,42	2,72	0,44
Yönetim	30	26,30	147,52	4,03		
Tıbbi	34	24,79	134,21	5,87		
İdari	24	24,83	131,79	5,99		

Tablo 4.2.27 incelendiğinde Bilgi işlem birimi, Yönetim kademesi, Tıbbi hizmetler birimi ve İdari kısımda çalışanların fiziksel ve çevresel güvenlik bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=2,72; p>0,05). Birimlere göre katılımcıların çalıştıkları yerlere göre benzer düzeyde fiziksel ve çevresel güvenlik farkındalığına sahiptirler.

Tablo 4.2.28. Fiziksel ve Çevresel Güvenlik Bölüm Puanının Personelin Çalıştığı Sağlık Kuruluşunun Türü ve Kapasitesine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p	Fark
Tür	2. ve 3. Basamak Sağlık Tesisi (1)	172	25,31	134,67	5,30	10,47	0,02	1-3 2-3 3-4
	ADSM ve Diş Hastanesi (2)	26	25,31	132,27	5,38			
	İlçe Sağlık Müdürlüğü (3)	14	21,14	75,54	7,42			
	İl Sağlık Müdürlüğü (4)	48	25,13	130,63	4,69			
Kapasite	Büyük	119	25,14	135,27	5,46	2,2249	0,33	-
	Küçük	80	25,43	131,54	5,20			
	İdari	61	24,39	119,83	5,50			

Tablo 4.2.28 incelendiğinde 2.- 3. Basamak hastanede, ADSM ve Diş Hastanesinde, İlçe Sağlık Müdürlüğünde ve İl Sağlık Müdürlüğünde çalışanların fiziksel ve çevresel güvenlik bölüm ortalaması en az biri istatistiksel olarak anlamlıdır (χ^2=10,47; p<0,05). Farkın kaynağını belirlemek için yapılan Dunn testleri sonucunda yalnızca 2.- 3. Basamak hastanede, ADSM ve Diş Hastanesinde ve İl Sağlık Müdürlüğünde çalışanların fiziksel ve çevresel güvenlik bölüm ortalaması İlçe Sağlık Müdürlüğünde çalışanlardan daha yüksek bulunmuştur. Sağlık tesislerinin kapasite büyüklükleri açısından büyük, küçük ve idari sağlık kuruluşunda çalışan personelin fiziksel ve çevresel güvenlik bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ2=2,2249; p<0,05).

4.2.8. İşlem güvenliği alt bölümüne ilişkin bulgular

İşlem güvenliği bölümüne çalışanların verdiği cevapların ortalaması 33,30'dur (medyan=38,00) ve çalışanların ortalama görüşlerinin 1,75 ile evet düzeyinde olduğu gözlenmiştir. Sağlık personelinin cinsiyete, deneyime, eğitim düzeyine, unvana, çalıştığı birime, çalıştığı kurumun türüne ve çalıştığı kurumun kapasitesine göre işlem güvenliği ortalamaları arasındaki ilişkiler aşağıda özetlenmiştir.

Tablo 4.2.29. **İşlem Güvenliği Bölüm Puanının Cinsiyet ve Unvana Göre Mann-Whitney U Testi Sonucu**

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	Z	p
Cinsiyet	Kadın	71	33,17	131,49	8,07	-0,14	0,89
	Erkek	189	33,35	130,13	7,50		
Unvan	Yönetici	45	32,76	129,87	8,46	-0,07	0,95
	Bilgi işlem personeli	215	33,41	130,63	7,48		

Tablo 4.2.29 incelendiğinde kadın çalışanların işlem güvenliği bölüm ortalaması ile erkek personelin ortalamları istatistiksel olarak anlamlı bulunmamıştır (Z=-0,14; p>0,05). Yöneticilerin ve bilgi işlem personelinin ortalamaları istatistiksel olarak benzerdir (Z=-0,07; p>0,05).

Tablo 4.2.30. İşlem Güvenliği Bölüm Puanının Çalışanların Eğitim Düzeyi ve Deneyimine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p	Fark
Eğitim	Lise (1)	76	34,89	150,78	6,48	11,75	0,01	1-4
	Yüksekokul (2)	66	33,70	130,30	6,86			
	Lisans (3)	91	32,70	120,54	8,02			
	Lisans üstü (4)	27	29,85	107,48	9,97			
Kıdem	0-1 yıl	11	30,82	112,32	9,40	1,78	0,88	-
	2-5 yıl	44	33,16	124,90	6,88			
	6-10 yıl	66	32,86	129,03	8,97			
	11-15 yıl	52	33,87	137,09	7,10			
	16-20 yıl	39	33,87	130,42	6,54			
	21 ve üzeri	48	33,52	134,75	7,55			

Tablo 4.2.30 incelendiğinde lise, yüksekokul, lisans ve lisan üstü eğitim düzeyinde çalışanların işlem güvenliği bölüm puanı ile personelin eğitim düzeyi arasında istatiksel olarak gözlenen bu farkların en az biri istatistiksel olarak anlamlıdır (χ^2=11,75; p>0,05). Farkın kaynağını belirlemek için yapılan Dunn U testleri sonucunda yalnızca lise eğitim düzeyine sahip personelin varlık yönetimi bölüm ortalaması eğitim düzeyi lisansüstü eğitim düzeyine sahip personelden daha yüksek bulunmuştur. Kıdem yılı açısından sağlık kuruluşunda çalışan personelin işlem güvenliği bölüm ve personelin kıdem yılı arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ2=1,78; p>0,05).

Tablo 4.2.31. İşlem Güvenliği Bölüm Puanının Çalışanların Birimine Göre Kruskall-Wallis H Testi Sonucu

Birim	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Bilgi işlem	172	33,23	126,01	7,29	2,38	0,80
Yönetim	30	34,83	143,33	6,54		
Tıbbi	34	32,85	137,90	9,30		
İdari	24	32,54	136,19	9,01		

Tablo 4.2.31 incelendiğinde Bilgi işlem birimi, Yönetim kademesi, Tıbbi hizmetler birimi ve İdari kısımda çalışanların işlem güvenliği bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=2,38; p>0,05). Birimlere göre katılımcıların çalıştıkları yerlere göre benzer düzeyde işlem güvenliği farkındalığına sahiptirler.

Tablo 4.2.32. İşlem Güvenliği Bölüm Puanının Personelin Çalıştığı Sağlık Kuruluşunun Türü ve Kapasitesine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p	Fark
Tür	2. ve 3. Basamak Sağlık Tesisi (1)	172	33,94	135,60	7,24	15,63	0,00	1-3 2-3 3-4
	ADSM ve Diş Hastanesi (2)	26	34,08	137,88	7,56			
	İlçe Sağlık Müdürlüğü (3)	14	25,64	61,57	9,04			
	İl Sağlık Müdürlüğü (4)	48	32,83	128,33	7,68			
Kapasite	Büyük	119	33,85	138,41	7,61	4,856	0,09	-
	Küçük	80	33,93	130,74	6,91			
	İdari	61	31,41	114,75	8,41			

Tablo 4.2.32 incelendiğinde 2.- 3. Basamak hastanede, ADSM ve Diş Hastanesinde, İlçe Sağlık Müdürlüğünde ve İl Sağlık Müdürlüğünde çalışanların işlem güvenliği bölüm ortalaması farklarından en az biri istatistiksel olarak anlamlıdır (χ^2=15,63; p<0,05). Farkın kaynağını belirlemek için yapılan Dunn testleri sonucunda yalnızca 2.- 3. Basamak hastanede, ADSM ve Diş Hastanesinde ve İl Sağlık Müdürlüğünde çalışanların işlem güvenliği bölüm ortalaması İlçe Sağlık Müdürlüğünde çalışanlardan daha yüksek bulunmuştur. Sağlık tesislerinin kapasite büyüklükleri açısından büyük, küçük ve idari sağlık kuruluşunda çalışan personelin işlem güvenliği bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ2=4,856; p<0,05).

4.2.9. Haberleşme güvenliği politikaları alt bölümüne ilişkin bulgular

Haberleşme güvenliği bölümüne çalışanların verdiği cevapların ortalaması 10,41'dir (medyan=12,00) ve çalışanların ortalama görüşlerinin 1,73 ile evet düzeyinde olduğu gözlenmiştir. Sağlık personelinin cinsiyete, deneyime, eğitim düzeyine, unvana, çalıştığı birime, çalıştığı kurumun türüne ve çalıştığı kurumun kapasitesine göre haberleşme güvenliği ortalamaları arasındaki ilişkiler aşağıda özetlenmiştir.

Tablo 4.2.33. Haberleşme Güvenliği Bölüm Puanının Cinsiyet ve Unvana Göre Mann-Whitney U Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	Z	p
Cinsiyet	Kadın	71	10,68	135,99	2,32	-0,85	0,40
	Erkek	189	10,31	128,44	2,72		
Unvan	Yönetici	45	10,22	131,20	2,95	-0,08	0,94
	Bilgi işlem personeli	215	10,45	130,35	2,54		

Tablo 4.2.33 incelendiğinde kadın çalışanların haberleşme güvenliği bölüm ortalaması ile erkek personelin ortalamalar arasında gözlenen farklar istatistiksel olarak anlamlı bulunmamıştır (Z=-0,85; p>0,05). Yöneticilerin ve bilgi işlem personelinin ortalamaları istatistiksel olarak benzerdir (Z=-0,08; p>0,05).

Tablo 4.2.34. Haberleşme Güvenliği Bölüm Puanının Çalışanların Eğitim Düzeyi ve Deneyimine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Eğitim	Lise	76	10,92	144,05	2,24	6,61	0,09
	Yüksekokul	66	10,41	126,90	2,39		
	Lisans	91	10,35	127,96	2,59		
	Lisans üstü	27	9,15	109,74	3,71		
Kıdem	0-1 yıl	11	10,09	125,05	3,11	1,83	0,87
	2-5 yıl	44	10,25	122,15	2,49		
	6-10 yıl	66	10,39	128,90	2,80		
	11-15 yıl	52	10,63	137,86	2,43		
	16-20 yıl	39	10,64	135,71	2,30		
	21 ve üzeri	48	10,21	129,41	2,86		

Tablo 4.2.34. incelendiğinde lise, yüksekokul, lisans ve lisan üstü eğitim düzeyinde çalışanların haberleşme bölüm puanı ile personelin eğitim düzeyi arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=6,61; p>0,05). Kıdem yılı açısından sağlık kuruluşunda çalışan personelin haberleşme güvenliği bölüm ortalaması ve personelin kıdem yılı arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ2=1,83; p>0,05).

Tablo 4.2.35. Haberleşme Güvenliği Bölüm Puanının Çalışanların Birimine Göre Kruskall-Wallis H Testi Sonucu

Birim	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Bilgi işlem	172	10,22	125,02	2,70	5,74	0,12
Yönetim	30	11,23	153,73	1,92		
Tıbbi	34	10,85	139,19	2,16		
İdari	24	10,08	128,44	3,11		

Tablo 4.2.35 incelendiğinde Bilgi işlem birimi, Yönetim kademesi, Tıbbi hizmetler birimi ve İdari kısımda çalışanların haberleşme güvenliği bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=5,74; p>0,05). Birimlere göre katılımcıların çalıştıkları yerlere göre benzer düzeyde haberleşme güvenliği farkındalığına sahiptirler.

Tablo 4.2.36. Haberleşme Güvenliği Bölüm Puanının Personelin Çalıştığı Sağlık Kuruluşunun Türü ve Kapasitesine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p	Fark
Tür	2. ve 3. Basamak Sağlık Tesisi (1)	172	10,66	135,54	2,37	15,08	0,00	1-3 2-3 3-4
	ADSM ve Diş Hastanesi (2)	26	10,54	139,71	2,98			
	İlçe Sağlık Müdürlüğü (3)	14	7,93	68,43	3,15			
	İl Sağlık Müdürlüğü (4)	48	10,17	125,56	2,75			
Kapasite	Büyük	119	10,81	139,02	2,25	6,119	0,05	1-3
	Küçük	80	10,34	130,33	2,75			
	İdari	61	9,72	114,11	2,96			

Tablo 4.2.36 incelendiğinde 2.- 3. Basamak hastanede, ADSM ve Diş Hastanesinde, İlçe Sağlık Müdürlüğünde ve İl Sağlık Müdürlüğünde çalışanların haberleşme güvenliği bölüm ortalaması en az biri istatistiksel olarak anlamlıdır (χ^2=15,08; p<0,05). Farkın kaynağını belirlemek için yapılan Dunn testleri sonucunda yalnızca 2.- 3. Basamak hastanede, ADSM ve Diş Hastanesinde ve İl Sağlık Müdürlüğünde çalışanların haberleşme güvenliği bölüm ortalaması İlçe Sağlık Müdürlüğünde çalışanlardan daha yüksek bulunuştur. Sağlık tesislerinin kapasite büyüklükleri açısından büyük, küçük ve idari sağlık kuruluşunda çalışan personelin işlem güvenliği bölüm ortalaması en az biri istatistiksel olarak anlamlıdır (χ^2=6,119; p<0,05). Farkın kaynağını belirlemek için yapılan Dunn testleri sonucunda yalnızca büyük sağlık tesisinde çalışanların haberleşme güvenliği bölüm ortalaması idari yapıda çalışanlardan daha yüksek bulunuştur.

4.2.10. Sistem temini, geliştirme ve bakımı alt bölümüne ilişkin bulgular

Sistem temini, geliştirme ve bakımı bölümüne çalışanların verdiği cevapların ortalaması 19,11'dir (medyan=22,00) ve çalışanların ortalama görüşlerinin 1,74 ile evet düzeyinde olduğu gözlenmiştir. Sağlık personelinin cinsiyete, deneyime, eğitim düzeyine, unvana, çalıştığı birime, çalıştığı kurumun türüne ve çalıştığı kurumun kapasitesine göre sistem temini, geliştirme ve bakımı ortalamaları arasındaki ilişkiler aşağıda özetlenmiştir.

Tablo 4.2.37. Sistem Temini, Geliştirme ve Bakımı Bölüm Puanının Cinsiyet ve Unvana Göre Mann-Whitney U Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	Z	p
Cinsiyet	Kadın	71	19,58	136,28	4,34	-0,88	0,38
	Erkek	189	18,94	128,33	5,00		
Unvan	Yönetici	45	18,76	128,61	5,05	-0,22	0,83
	Bilgi işlem personeli	215	19,19	130,90	4,79		

Tablo 4.2.37 incelendiğinde kadın çalışanların Sistem Temini, Geliştirme ve Bakımı bölüm ortalaması ile erkek personelin ortalamalar arasında gözlenen farklar istatistiksel olarak anlamlı bulunmamıştır (Z=-0,88; p>0,05). Yöneticilerin ve bilgi işlem personelinin ortalamaları istatistiksel olarak benzerdir (Z=-0,22; p>0,05).

Tablo 4.2.38. Sistem Temini, Geliştirme ve Bakımı Bölüm Puanının Çalışanların Eğitim Düzeyi ve Deneyimine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Eğitim	Lise	76	19,84	143,34	4,36	5,57	0,13
	Yüksekokul	66	19,29	129,50	4,67		
	Lisans	91	19,03	126,16	4,62		
	Lisans üstü	27	16,89	111,43	6,50		
Kıdem	0-1 yıl	11	17,55	120,82	6,33	2,31	0,80
	2-5 yıl	44	18,80	121,56	4,64		
	6-10 yıl	66	19,67	139,11	4,53		
	11-15 yıl	52	19,31	131,73	4,65		
	16-20 yıl	39	19,13	128,82	4,81		
	21 ve üzeri	48	18,77	129,11	5,34		

Tablo 4.2.38 incelendiğinde lise, yüksekokul, lisans ve lisan üstü eğitim düzeyinde çalışanların sistem temini, geliştirme ve bakımı bölüm puanı ile personelin eğitim düzeyi arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=5,57; p>0,05). Kıdem yılı açısından sağlık kuruluşunda çalışan personelin sistem temini, geliştirme ve bakımı bölüm

ortalaması ve personelin kıdem yılı arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır ($\chi 2$=2,31; p>0,05).

Tablo 4.2.39. Sistem Temini, Geliştirme ve Bakımı Bölüm Puanının Çalışanların Birimine Göre Kruskall-Wallis H Testi Sonucu

Birim	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Bilgi işlem	172	18,85	124,80	5,01	6,25	0,10
Yönetim	30	20,57	152,43	3,45		
Tıbbi	34	19,59	143,41	4,63		
İdari	24	18,50	125,65	5,17		

Tablo 4.2.39 incelendiğinde Bilgi işlem birimi, Yönetim kademesi, Tıbbi hizmetler birimi ve İdari kısımda çalışanların sistem temini, geliştirme ve bakım bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=2,72; p>0,05). Birimlere göre katılımcıların çalıştıkları yerlere göre benzer düzeyde sistem temini, geliştirme ve bakım bölüm farkındalığına sahiptirler.

Tablo 4.2.40. Sistem Temini, Geliştirme ve Bakımı Bölüm Puanının Personelin Çalıştığı Sağlık Kuruluşunun Türü ve Kapasitesine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p	Fark
Tür	2. ve 3. Basamak Sağlık Tesisi (1)	172	19,52	135,80	4,45	16,47	0,00	1-3 2-3 3-4
	ADSM ve Diş Hastanesi (2)	26	19,69	142,35	5,14			
	İlçe Sağlık Müdürlüğü (3)	14	15,29	65,75	5,21			
	İl Sağlık Müdürlüğü (4)	48	18,44	123,97	5,43			
Kapasite	Büyük (1)	119	19,50	138,74	4,73	6,826	0,03	1-3
	Küçük (2)	80	19,51	132,18	4,33			
	İdari (3)	61	17,84	112,22	5,47			

Tablo 4.2.40 incelendiğinde 2.- 3. Basamak hastanede, ADSM ve Diş Hastanesinde, İlçe Sağlık Müdürlüğünde ve İl Sağlık Müdürlüğünde çalışanların sistem temini, geliştirme ve bakımı bölüm ortalaması en az biri istatistiksel olarak anlamlıdır (χ^2=16,47; p<0,05). Farkın kaynağını belirlemek için yapılan Dunn testleri sonucunda yalnızca 2.- 3. Basamak hastanede, ADSM ve Diş Hastanesinde ve İl Sağlık Müdürlüğünde çalışanların sistem temini, geliştirme ve bakımı bölüm ortalaması İlçe Sağlık Müdürlüğünde çalışanlardan daha yüksek bulunuştur. Sağlık tesislerinin kapasite büyüklükleri açısından büyük, küçük ve idari sağlık kuruluşunda çalışan personelin sistem temini, geliştirme ve bakımı bölüm ortalaması en az biri istatistiksel olarak anlamlıdır (χ^2=6,826; p<0,05). Farkın kaynağını belirlemek için yapılan Dunn testleri

sonucunda yalnızca büyük sağlık tesisinde çalışanların sistem temini, geliştirme ve bakımı bölüm ortalaması idari yapıda çalışanlardan daha yüksek bulunuştur.

4.2.11. Tedarikçi ilişkileri alt bölümüne ilişkin bulgular

Tedarikçi ilişkileri bölümüne çalışanların verdiği cevapların ortalaması 8,63'tür (medyan=10,00) ve çalışanların ortalama görüşlerinin 1,73 ile evet düzeyinde olduğu gözlenmiştir. Sağlık personelinin cinsiyete, deneyime, eğitim düzeyine, unvana, çalıştığı birime, çalıştığı kurumun türüne ve çalıştığı kurumun kapasitesine göre tedarikçi ilişkileri ortalamaları arasındaki ilişkiler aşağıda özetlenmiştir.

Tablo 4.2.41. Tedarikçi İlişkileri Bölüm Puanının Cinsiyet ve Unvana Göre Mann-Whitney U Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	Z	p
Cinsiyet	Kadın	71	8,86	131,61	1,96	-0,18	0,86
	Erkek	189	8,55	130,08	2,60		
Unvan	Yönetici	45	8,56	128,66	2,41	-0,22	0,82
	Bilgi işlem personeli	215	8,65	130,89	2,46		

Tablo 4.2.41 incelendiğinde kadın çalışanların tedarikçi ilişkileri bölüm ortalaması ile erkek personelin ortalamaları arasında gözlenen farklar istatistiksel olarak anlamlı bulunmamıştır (Z=-0,18; p>0,05). Yöneticilerin ve bilgi işlem personelinin ortalamaları istatistiksel olarak benzerdir (Z=-0,22; p>0,05).

Tablo 4.2. 42. Tedarikçi İlişkileri Bölüm Puanının Çalışanların Eğitim Düzeyi ve Deneyimine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Eğitim	Lise	76	8,97	141,82	2,31	5,25	0,15
	Yüksekokul	66	8,50	128,06	2,51		
	Lisans	91	8,74	128,24	2,16		
	Lisans üstü	27	7,67	112,22	3,28		
Kıdem	0-1 yıl	11	8,73	117,82	1,95	2,01	0,85
	2-5 yıl	44	8,18	121,67	2,97		
	6-10 yıl	66	8,79	135,38	2,32		
	11-15 yıl	52	8,65	131,82	2,47		
	16-20 yıl	39	8,74	129,62	2,27		
	21 ve üzeri	48	8,71	134,08	2,35		

Tablo 4.2.42 incelendiğinde lise, yüksekokul, lisans ve lisan üstü eğitim düzeyinde çalışanların tedarikçi ilişkileri bölüm puanı ile personelin eğitim düzeyi arasında istatiksel

olarak anlamlı bir ilişki bulunmamıştır (χ^2=5,25; p>0,05). Kıdem yılı açısından sağlık kuruluşunda çalışan personelin tedarikçi ilişkileri bölüm ortalaması ve personelin kıdem yılı arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ2=2,01; p>0,05).

Tablo 4.2.43. Tedarikçi İlişkileri Bölüm Puanının Çalışanların Birimine Göre Kruskall-Wallis H Testi Sonucu

Birim	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Bilgi işlem	172	8,49	126,78	2,61	4,48	0,21
Yönetim	30	9,47	150,42	1,43		
Tıbbi	34	8,94	136,68	1,92		
İdari	24	8,21	123,52	2,70		

Tablo 4.2.43 incelendiğinde Bilgi işlem birimi, Yönetim kademesi, Tıbbi hizmetler birimi ve İdari kısımda çalışanların tedarikçi ilişkileri bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=4,48; p>0,05). Birimlere göre katılımcıların çalıştıkları yerlere göre benzer düzeyde tedarikçi ilişkileri bölüm farkındalığına sahiptirler.

Tablo 4.2.44. Tedarikçi İlişkileri Bölüm Puanının Personelin Çalıştığı Sağlık Kuruluşunun Türü ve Kapasitesine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p	Fark
Tür	2. ve 3. Basamak Sağlık Tesisi (1)	172	8,84	134,90	2,25	9,46	0,02	1-3 2-3
	ADSM ve Diş Hastanesi (2)	26	8,92	139,96	2,50			
	İlçe Sağlık Müdürlüğü (3)	14	7,21	87,07	2,52			
	İl Sağlık Müdürlüğü (4)	48	8,17	122,26	2,91			
Kapasite	Büyük	119	8,79	134,21	2,27	4,741	0,09	-
	Küçük	80	8,89	136,28	2,32			
	İdari	61	8,00	115,68	2,83			

Tablo 4.2.44 incelendiğinde 2.- 3. Basamak hastanede, ADSM ve Diş Hastanesinde, İlçe Sağlık Müdürlüğünde ve İl Sağlık Müdürlüğünde çalışanların tedarikçi ilişkileri bölüm ortalaması en az biri istatistiksel olarak anlamlıdır (χ^2=9,46; p<0,05). Farkın kaynağını belirlemek için yapılan Dunn testleri sonucunda yalnızca 2.- 3. Basamak hastanede ve ADSM ve Diş Hastanesinde ve tedarikçi ilişkileri bölüm ortalaması İlçe Sağlık Müdürlüğünde çalışanlardan daha yüksek bulunuştur. Sağlık tesislerinin kapasite büyüklükleri açısından büyük, küçük ve idari sağlık kuruluşunda çalışan personelin tedarikçi ilişkileri bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ2=4,741; p<0,05).

4.2.12. Bilgi güvenliği ihlal olayı yönetimi alt bölümüne ilişkin bulgular

Bilgi güvenliği ihlal olayı yönetimi bölümüne çalışanların verdiği cevapların ortalaması 10,48'tir (medyan=12,00) ve çalışanların ortalama görüşlerinin 1,75 ile evet düzeyinde olduğu gözlenmiştir. Sağlık personelinin cinsiyete, deneyime, eğitim düzeyine, unvana, çalıştığı birime, çalıştığı kurumun türüne ve çalıştığı kurumun kapasitesine göre bilgi güvenliği ihlal olayı yönetimi ortalamaları arasındaki ilişkiler aşağıda özetlenmiştir.

Tablo 4.2.45. Bilgi Güvenliği İhlal Olayı Yönetimi Bölüm Puanının Cinsiyet ve Unvana Göre Mann-Whitney U Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	Z	p
Cinsiyet	Kadın	71	10,56	129,47	2,39	-0,17	0,87
	Erkek	189	10,44	130,89	2,91		
Unvan	Yönetici	45	10,27	126,42	2,82	-0,50	0,62
	Bilgi işlem personeli	215	10,52	131,35	2,77		

Tablo 4.2.45 incelendiğinde kadın çalışanların bilgi güvenliği ihlal olayı yönetimi bölüm ortalaması ile erkek personelin ortalamalar arasında gözlenen farklar istatistiksel olarak anlamlı bulunmamıştır (Z=-0,17; p>0,05). Yöneticilerin ve bilgi işlem personelinin ortalamaları istatistiksel olarak benzerdir (Z=-0,50; p>0,05).

Tablo 4.2.46. Bilgi Güvenliği İhlal Olayı Yönetimi Bölüm Puanının Çalışanların Eğitim Düzeyi ve Deneyimine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Eğitim	Lise	76	11,00	139,92	2,28	6,04	0,11
	Yüksekokul	66	10,29	129,14	3,12		
	Lisans	91	10,53	130,68	2,65		
	Lisans üstü	27	9,30	106,69	3,29		
Kıdem	0-1 yıl	11	10,00	118,64	2,93	2,61	0,76
	2-5 yıl	44	10,23	122,02	3,02		
	6-10 yıl	66	10,53	135,18	2,76		
	11-15 yıl	52	10,81	137,31	2,53		
	16-20 yıl	39	10,54	125,46	2,55		
	21 ve üzeri	48	10,33	131,27	3,05		

Tablo 4.2.46 incelendiğinde lise, yüksekokul, lisans ve lisan üstü eğitim düzeyinde çalışanların bilgi güvenliği ihlal olayı yönetimi bölüm puanı ile personelin eğitim düzeyi arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=6,04; p>0,05). Kıdem yılı açısından sağlık kuruluşunda çalışan personelin bilgi güvenliği ihlal olayı yönetimi bölüm

ortalaması ve personelin kıdem yılı arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır ($\chi 2=2,61$; $p>0,05$).

Tablo 4.2.47. Bilgi Güvenliği İhlal Olayı Yönetimi Bölüm Puanının Çalışanların Birimine Göre Kruskall-Wallis H Testi Sonucu

Birim	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Bilgi işlem	172	10,40	129,10	2,94	3,12	0,37
Yönetim	30	11,27	148,23	1,76		
Tıbbi	34	10,44	127,19	2,51		
İdari	24	10,13	123,08	2,97		

Tablo 4.2.47 incelendiğinde Bilgi işlem birimi, Yönetim kademesi, Tıbbi hizmetler birimi ve İdari kısımda çalışanların bilgi güvenliği ihlal olayı yönetimi bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır ($\chi^2=3,12$; $p>0,05$). Birimlere göre katılımcıların çalıştıkları yerlere göre benzer düzeyde ihlal olayı bölüm farkındalığına sahiptirler.

Tablo 4.2.48. Bilgi Güvenliği İhlal Olayı Yönetimi Bölüm Puanının Personelin Çalıştığı Sağlık Kuruluşunun Türü ve Kapasitesine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p	Fark
Tür	2. ve 3. Basamak Sağlık Tesisi (1)	172	10,65	133,42	2,56	11,44	0,01	1-3 2-3
	ADSM ve Diş Hastanesi (2)	26	10,96	144,12	2,78			
	İlçe Sağlık Müdürlüğü (3)	14	8,36	80,36	3,30			
	İl Sağlık Müdürlüğü (4)	48	10,23	127,28	3,15			
Kapasite	Büyük	119	10,63	136,28	2,74	3,635	0,16	-
	Küçük	80	10,71	131,32	2,38			
	İdari	61	9,87	118,15	3,24			

Tablo 4.2.48 incelendiğinde 1. ve 2. ile 2.- 3. basamak hastanede, ADSM ve Diş Hastanesinde, İlçe Sağlık Müdürlüğünde ve İl Sağlık Müdürlüğünde çalışanların bilgi güvenliği ihlal olayı yönetimi bölüm ortalaması en az biri istatistiksel olarak anlamlıdır ($\chi^2=11,44$; $p<0,05$). Farkın kaynağını belirlemek için yapılan Dunn testleri sonucunda yalnızca 2.- 3. Basamak hastanede ve ADSM ve Diş Hastanesinde bilgi güvenliği ihlal olayı yönetimi bölüm ortalaması İlçe Sağlık Müdürlüğünde çalışanlardan daha yüksek bulunuştur. Sağlık tesislerinin kapasite büyüklükleri açısından büyük, küçük ve idari sağlık kuruluşunda çalışan personelin çalışanların bilgi güvenliği ihlal olayı yönetimi bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır ($\chi 2=3,635$; $p<0,05$).

4.2.13. İş sürekliliğinin bilgi güvenliği alt bölümüne ilişkin bulgular

İş sürekliliğinin bilgi güvenliği bölümüne çalışanların verdiği cevapların ortalaması 6,9'dir (medyan=8,00) ve çalışanların ortalama görüşlerinin 1,77 ile evet düzeyinde olduğu gözlenmiştir. Sağlık personelinin cinsiyete, deneyime, eğitim düzeyine, unvana, çalıştığı birime, çalıştığı kurumun türüne ve çalıştığı kurumun kapasitesine göre iş sürekliliğinin bilgi güvenliği ortalamaları arasındaki ilişkiler aşağıda özetlenmiştir.

Tablo 4.2. 49. İş Sürekliliğinin Bilgi Güvenliği Hususları Bölüm Puanının Cinsiyet ve Unvana Göre Mann-Whitney U Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	Z	p
Cinsiyet	Kadın	71	7,03	132,65	1,69	-0,35	0,73
	Erkek	189	6,87	129,69	1,97		
Unvan	Yönetici	45	6,60	124,01	2,20	-0,78	0,44
	Bilgi işlem personeli	215	6,98	131,86	1,83		

Tablo 4.2.49 incelendiğinde kadın çalışanların iş sürekliliğinin bilgi güvenliği hususları bölüm ortalaması ile erkek personelin ortalamalar arasında gözlenen farklar istatistiksel olarak anlamlı bulunmamıştır (Z=-0,35; p>0,05). Yöneticilerin ve bilgi işlem personelinin ortalamaları istatistiksel olarak benzerdir (Z=-0,78; p>0,05).

Tablo 4.2.50. İş Sürekliliğinin Bilgi Güvenliği Hususları Bölüm Puanının Çalışanların Eğitim Düzeyi ve Deneyimine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Eğitim	Lise	76	7,13	139,20	1,75	5,32	0,15
	Yüksekokul	66	6,94	127,39	1,78		
	Lisans	91	6,95	132,09	1,90		
	Lisans üstü	27	6,11	108,24	2,39		
Kıdem	0-1 yıl	11	6,82	123,86	1,83	1,68	0,89
	2-5 yıl	44	6,80	122,22	1,76		
	6-10 yıl	66	6,92	129,55	1,86		
	11-15 yıl	52	7,06	137,23	1,84		
	16-20 yıl	39	6,92	130,87	1,94		
	21 ve üzeri	48	6,85	133,33	2,17		

Tablo 4.2.50 incelendiğinde lise, yüksekokul, lisans ve lisan üstü eğitim düzeyinde çalışanların iş sürekliliğinin bilgi güvenliği hususları bölüm puanı ile personelin eğitim düzeyi arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=5,32; p>0,05). Kıdem yılı açısından sağlık kuruluşunda çalışan personelin iş sürekliliğinin bilgi güvenliği hususları bölüm

ortalaması ve personelin kıdem yılı arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır ($\chi 2=1,68$; $p>0,05$).

Tablo 4.2.51. İş Sürekliliğinin Bilgi Güvenliği Hususları Bölüm Puanının Çalışanların Birimine Göre Kruskall-Wallis H Testi Sonucu

Birim	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Bilgi işlem	172	6,93	129,96	1,87	2,59	0,46
Yönetim	30	7,20	145,67	1,86		
Tıbbi	34	6,79	126,81	1,86		
İdari	24	6,58	120,67	2,22		

Tablo 4.2.51 incelendiğinde Bilgi işlem birimi, Yönetim kademesi, Tıbbi hizmetler birimi ve İdari kısımda çalışanların iş sürekliliğin bilgi güvenliği hususları bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır ($\chi^2=2,59$; $p>0,05$). Birimlere göre katılımcıların çalıştıkları yerlere göre benzer düzeyde iş sürekliliği bilgi güvenliği hususları bölüm farkındalığına sahiptirler.

Tablo 4.2. 52. İş Sürekliliğinin Bilgi Güvenliği Hususları Bölüm Puanının Personelin Çalıştığı Sağlık Kuruluşunun Türü ve Kapasitesine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p	Fark
Tür	2. ve 3. Basamak Sağlık Tesisi (1)	172	7,02	133,60	1,77	10,29	0,02	1-3 2-3
	ADSM ve Diş Hastanesi (2)	26	7,23	141,83	1,86			
	İlçe Sağlık Müdürlüğü (3)	14	5,29	81,75	2,55			
	İl Sağlık Müdürlüğü (4)	48	6,83	127,49	1,97			
Kapasite	Büyük	119	7,05	136,88	1,83	3,602	0,17	-
	Küçük	80	7,00	130,11	1,74			
	İdari	61	6,52	118,57	2,19			

Tablo 4.2.52 incelendiğinde 2.- 3. Basamak hastanede, ADSM ve Diş Hastanesinde, İlçe Sağlık Müdürlüğünde ve İl Sağlık Müdürlüğünde çalışanların iş sürekliliği bilgi güvenliği bölüm ortalaması en az biri istatistiksel olarak anlamlıdır ($\chi^2=10,29$; $p<0,05$). Farkın kaynağını belirlemek için yapılan Dunn testleri sonucunda yalnızca 2.- 3. Basamak hastanede ve ADSM ve Diş Hastanesinde ve iş sürekliliği bilgi güvenliği bölüm ortalaması İlçe Sağlık Müdürlüğünde çalışanlardan daha yüksek bulunuştur. Sağlık tesislerinin kapasite büyüklükleri açısından büyük, küçük ve idari sağlık kuruluşunda çalışan personelin çalışanların bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır ($\chi 2=3,602$; $p<0,05$).

4.2.14. Uyum alt bölümüne ilişkin bulgular

Uyum bölümüne çalışanların verdiği cevapların ortalaması 8,86'dir (medyan=10,00) ve çalışanların ortalama görüşlerinin 1,77 ile evet düzeyinde olduğu gözlenmiştir. Sağlık personelinin cinsiyete, deneyime, eğitim düzeyine, unvana, çalıştığı birime, çalıştığı kurumun türüne ve çalıştığı kurumun kapasitesine göre uyum ortalamaları arasındaki ilişkiler aşağıda özetlenmiştir.

Tablo 4.2. 53. Uyum Bölüm Puanının Cinsiyet ve Unvana Göre Mann-Whitney U Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	Z	p
Cinsiyet	Kadın	71	8,94	131,13	1,90	-0,11	0,92
	Erkek	189	8,83	130,26	2,20		
Unvan	Yönetici	45	8,58	124,57	2,41	-0,74	0,46
	Bilgi işlem personeli	215	8,92	131,74	2,06		

Tablo 4.2.53 incelendiğinde kadın çalışanların uyum bölüm ortalaması ile erkek personelin ortalamalar arasında gözlenen farklar istatistiksel olarak anlamlı bulunmamıştır (Z=-0,11; p>0,05). Yöneticilerin ve bilgi işlem personelinin ortalamaları istatistiksel olarak benzerdir (Z=-0,74; p>0,05).

Tablo 4.2. 54. Uyum Bölüm Puanının Çalışanların Eğitim Düzeyi ve Deneyimine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Eğitim	Lise	76	9,21	139,84	1,78	7,79	0,06
	Yüksekokul	66	8,88	132,78	2,19		
	Lisans	91	8,90	129,15	2,01		
	Lisans üstü	27	7,70	103,19	2,81		
Kıdem	0-1 yıl	11	8,55	119,64	2,30	4,24	0,51
	2-5 yıl	44	8,61	120,98	2,32		
	6-10 yıl	66	9,20	142,17	1,87		
	11-15 yıl	52	8,90	129,74	2,10		
	16-20 yıl	39	8,79	126,97	2,03		
	21 ve üzeri	48	8,71	129,35	2,34		

Tablo 4.2.54 incelendiğinde lise, yüksekokul, lisans ve lisan üstü eğitim düzeyinde çalışanların uyum bölüm puanı ile personelin eğitim düzeyi arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=7,79; p>0,05). Kıdem yılı açısından sağlık kuruluşunda çalışan personelin uyum bölüm ortalaması ve personelin kıdem yılı arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ2=4,24; p>0,05).

Tablo 4.2. 55. Uyum Bölüm Puanının Çalışanların Birimine Göre Kruskall-Wallis H Testi Sonucu

Birim	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p
Bilgi işlem	172	8,83	128,87	2,15	2,35	0,50
Yönetim	30	9,37	145,90	1,56		
Tıbbi	34	8,79	128,38	2,06		
İdari	24	8,58	125,96	2,59		

Tablo 4.2. 55 incelendiğinde Bilgi işlem birimi, Yönetim kademesi, Tıbbi hizmetler birimi ve İdari kısımda çalışanların uyum bölüm puanı ile personelin çalıştıkları birim arasında istatiksel olarak anlamlı bir ilişki bulunmamıştır (χ^2=2,35; p>0,05). Birimlere göre katılımcıların çalıştıkları yerlere göre benzer düzeyde uyum bölüm farkındalığına sahiptirler.

Tablo 4.2. 56. Uyum Bölüm Puanının Personelin Çalıştığı Sağlık Kuruluşunun Türü ve Kapasitesine Göre Kruskall-Wallis H Testi Sonucu

Değişken	Düzey	n	$\bar{X}$	Sıra Ortalaması	S.S.	χ^2	p	Fark
Tür	2. ve 3. Basamak Sağlık Tesisi (1)	172	9,06	136,36	1,88	16,37	0,00	1-3 2-3 3-4
	ADSM ve Diş Hastanesi (2)	26	9,12	136,87	2,10			
	İlçe Sağlık Müdürlüğü (3)	14	6,93	72,07	2,89			
	İl Sağlık Müdürlüğü (4)	48	8,58	123,10	2,43			
Kapasite	Büyük (1)	119	9,13	140,66	1,85	8,933	0,01	1-3
	Küçük(2)	80	8,91	128,77	2,03			
	İdari (3)	61	8,26	112,95	2,60			

Tablo 4.2.56 incelendiğinde 2.- 3. Basamak hastanede, ADSM ve Diş Hastanesinde, İlçe Sağlık Müdürlüğünde ve İl Sağlık Müdürlüğünde çalışanların uyum bölüm ortalaması en az biri istatistiksel olarak anlamlıdır (χ^2=16,37; p<0,05). Farkın kaynağını belirlemek için yapılan Dunn testleri sonucunda yalnızca 2.- 3. Basamak hastanede, ADSM ve Diş Hastanesinde ve İl Sağlık Müdürlüğünde çalışanların uyum bölüm ortalaması İlçe Sağlık Müdürlüğünde çalışanlardan daha yüksek bulunuştur. Sağlık tesislerinin kapasite büyüklükleri açısından büyük, küçük ve idari sağlık kuruluşunda çalışan personelin uyum bölüm en az biri istatistiksel olarak anlamlıdır (χ^2=8,933; p<0,05). Farkın kaynağını belirlemek için yapılan Dunn testleri sonucunda yalnızca büyük sağlık tesisinde çalışanların uyum bölüm ortalaması idari yapıda çalışanlardan daha yüksek bulunuştur.

5. TARTIŞMA

Çalışmanın bu bölümünde yapılan analizler neticesinde elde edilen bulguların ilgili literatür çerçevesinde tartışmasına yer verilmiştir.

Bilgi sistemlerinde karşılaşılan güvenlik risklerinin yönetilebilmesi amacıyla kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerce uyulması gereken bilgi ve iletişim güvenliği tedbirlerini içeren Cumhurbaşkanlığı Genelgesi 6 Temmuz 2019 tarih ve 30823 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Sağlık Bakanlığının uygulamalarının yer aldığı ve Bilgi ve İletişim Güvenliği Rehberinin eki olan 10.10.2021 tarihli Bilgi ve İletişim Güvenliği Denetim Rehberi içerisinde TS ISO/IEC 27001:2017 Kontrolleri ile uygulanması gereken süreçlere göre değerlendirildiğinde ankete katılanların yüksek düzeyde farkındalık seviyesine sahip oldukları bölümlere verdikleri cevapların dağılımı incelendiğinde bölüm sorularına evet yanıtını verdiği görülmüşür.

- Bölüm 1: Bilgi Güvenliği Politikaları- % 96,15'i
- Bölüm 2: Bilgi Güvenliği Organizasyonu-% 96,92'si
- Bölüm 3: İnsan Kaynakları Güvenliği-% 98,46'sı
- Bölüm 4: Varlık Yönetimi-% 99,23'ü
- Bölüm 5: Erişim Kontrolü-% 98,46'sı
- Bölüm 6: Kriptografi- % 95,77'si
- Bölüm 7: Fiziksel ve Çevresel Güvenlik- % 100'ü
- Bölüm 8: İşlem Güvenliği- % 99,62'si
- Bölüm 9: Haberleşme Güvenliği- % 99,62'si
- Bölüm 10: Sistem Temini, Geliştirme ve Bakımı- % 99,23'ü
- Bölüm 11: Tedarikçi İlişkileri- % 97,31'i
- Bölüm 12: Bilgi Güvenliği İhlal Olayı Yönetimi- % 98,08'i
- Bölüm 13: İş Sürekliliğinin Bilgi Güvenliği Hususları- % 98,08'i
- Bölüm 14: Uyum- % 99,62'i.

Araştırmanın bulguları doğrultusunda, çalışmada kurulan hipotezlerin kabul ve reddedilme durumları Tablo 5.1'de gösterilmiştir.

Tablo 5. 1. Araştırma sorularının kabul/red durumu

Araştırma Soruları	Kabul /Red
- S_1: Cinsiyet ile bilgi güvenliği yönetimi kavramsal farkındalık düzeyi arasında anlamlı ve pozitif yönlü bir ilişki vardır.	Red
- S_2: Mesleki deneyimlere göre bilgi güvenliği yönetimi kavramsal farkındalık düzeyi arasında anlamlı ve pozitif yönlü bir ilişki vardır.	Red
- S_3: Eğitim durumu ile bilgi güvenliği yönetimi kavramsal farkındalık düzeyi arasında anlamlı ve pozitif yönlü bir ilişki vardır.	Kabul
- S_4: Unvanlar ile bilgi güvenliği yönetimi kavramsal farkındalık düzeyi arasında anlamlı ve pozitif yönlü bir ilişki vardır.	Kabul
- S_5: Çalıştığı kurum türü ile bilgi güvenliği yönetimi kavramsal farkındalık düzeyi arasında anlamlı ve pozitif yönlü bir ilişki vardır.	Kabul
- S_6: Çalıştığı kurum kapasitesi ile bilgi güvenliği yönetimi kavramsal farkındalık düzeyi arasında anlamlı ve pozitif yönlü bir ilişki vardır.	Kabul
- S_7: 3. ISO27001 Bilgi Yönetim Sistem Politikaları ile Sağlık Bakanlığı Bilgi Yönetim Politikaları farkındalık düzeyi arasında anlamlı ve pozitif yönlü bir ilişki vardır.	Kabul

Ankete katılan çalışanların %72,7'si erkek olup, kadın çalışanların bilgi güvenliği politikaları bölüm ortalaması ile erkek personelin ortalamalar arasında gözlenen farklar istatistiksel olarak anlamlı bulunmamıştır. Literatüre bakıldığında benzer sonuçlarla karşılaşmaktayız. Başdinkçi (2017), Sağlık kurumlarında bilgi güvenliği risk değerlendirmesi ve kullanıcıların bilgi güvenliği farkındalık düzeyinin ölçülmesi adlı çalışması ile çalışmamızın bulguların genelinde kontrol listesine verilen cevaplardan kadın çalışanların bölüm ortalaması ile erkek personel arasındaki ortalamalar, yöneticiler ile bilgi işlem personeli arasındaki ortalamalar, eğitim düzeyi, kıdem yılı ve çalıştıkları birim açısından benzer düzeyde farkındalığına sahip oldukları görülmüştür. Aslan (2019), çalışmasında hemşire akademisyenlerin bilgi güvenliği farkındalık düzeyleri ile yaş, cinsiyet, medeni durum, gelir durumu ve mesleki deneyimleri arasında çalışmamızda olduğu gibi istatistiksel olarak anlamlı bir fark bulunmadığı belirtilmiştir. Aynı şekilde tıbbi ve idari birim çalışanlarının bilgi güvenliği ölçeğine göre yaş, cinsiyet, medeni durum, eğitim durumu ve gelir durumu gibi demografik değişkenlerine bakıldığında anlamlı bir farklılık bulunmamıştır (Çimen 2021).

Özdemir ve Uluyol (2021), kamu kurum ve kuruluşlarında bilgi güvenliği farkındalığı çalışmasında kadın ve erkek katılımcılarının ortalama puanlarının birbirinden anlamlı olarak farklılaşmadığı, Baran ve Şener (2020), cinsiyet değişkeninde anlamlı fark olmadığını, Alemdaroğlu (2020) çalışmasında ise erkek çalışanların kadın çalışanlara göre daha fazla

farkındalığa sahip olduğu görülmüştür. Kowalski, ve ark.(2008) genel olarak kadın ve erkek katılımcılar cinsiyet durumuna göre benzer düzeyde bilgi güvenliği farkındalığına sahip olduklarını belirtirken her iki cinsiyetin de bilgi güvenliği için eşit tehdit oluşturduğunu, Lubis ve ark. (2020) insan faktörlerinin, yüksek kalitede bilgi güvenliği sağlamak için kuruluşa yönelik en büyük tehditler olabileceğini belirtmektedir.

Özaslan (2019) çalışmasında hastane bilgi yönetim sistemi kullanan çalışanlar üzerinde, bilgi güvenliği ve mahremiyetin korunmasına yönelik eğitimin etkilerini değerlendirmiş olup tıbbi ve idari birim çalışanları puanları bakıldığında gruplar arasında anlamlı bir fark tespit edilmemiştir. Safa ve ark. (2018) tarafından uygulayıcılar için bilgi güvenliği alanındaki istenmeyen davranışların azaltılmasında rol oynayan faktörlere göre kavramsallaştıran, Kurt (2019) çalışmasında tespit ettiği ve Kılıç (2014) çalışmasında belirttiği gibi bilgi işlem çalışanlarının kurumda çalışma süresi ile ve kurumun faaliyet süresi ile bilgi güvenliği ölçeği puan ortalamaları arasında anlamlı bir ilişkinin olmadığı görülmektedir.

Katılımcıların "Bölüm 4: Varlık Yönetimi" ve "Bölüm 8 İşlem Güvenliği" verdikleri yanıtların incelenmesinde bölüm puanları ile personelin eğitim düzeyi arasında istatistiksel olarak anlamlıdır. Farkın kaynağını belirlemek için yapılan Dunn testleri sonucunda yalnızca lise eğitim düzeyine sahip personelin "Bölüm 4: Varlık Yönetimi" ve "Bölüm 8: İşlem Güvenliği" bölüm ortalaması eğitim düzeyi lisansüstü eğitim düzeyine sahip personelden daha yüksek bulunmuştur. Alemdaroğlu (2020), bankacılık sektöründe çalışanların, bilgi güvenliği farkındalığı seviyesinin belirlenmesi ve geliştirilmesi gereken alanlara yönelik yapmış olduğu çalışmasında; öğrenim durumu ile bilgi güvenliği farkındalığının alt boyutları arasındaki ilişki incelenmiş ve güvenlik önlemi alma konusunda ön lisans mezunları ile lisans mezunları arasında fark gözlemlenmesine rağmen diğer öğrenim durumu grupları ile diğer alt boyutlar arasında herhangi bir farka rastlanmamıştır. Bu araştırmada ise ön lisans mezunlarının Bölüm 4: Varlık Yönetimi" ve "Bölüm 8: İşlem Güvenliği" konularında operasyonel durumlarından dolayı farkındalık seviyeleri yüksek lisans mezunlarına göre daha yüksek çıkmış olabileceği düşünülmektedir. Kurt (2019) çalışanların niteliği arttıkça güvenlik uygulamalarından memnuniyet düzeylerinin azaldığı ve uygulamaların yüksek lisans ve üzeri mezun çalışanları daha az tatmin edici olduğu sonucu elde edilirken, Akal (2022) çalışmasında eğitim düzeyinin firmadaki bilgi güvenliği farkındalık düzeyini doğrudan etkilediği sonucuna ulaşmıştır. Lise mezunu çalışanların bilgi güvenliği yönetiminden genel olarak daha memnun oldukları sonucuna ulaşmıştır.

2. ve 3. basamak sağlık tesisi, ADSM ve Diş Hastanesinde, İlçe Sağlık Müdürlüğünde ve İl Sağlık Müdürlüğünde çalışanların "Bölüm 4: İnsan Kaynakları Güvenliği", "Bölüm 6: Kriptografi", "Bölüm 7: Fiziksel ve Çevresel Güvenlik", "Bölüm 8: İşlem Güvenliği", "Bölüm 9: Haberleşme Güvenliği", "Bölüm 11: Tedarikçi İlişkileri ", "Bölüm 12: Bilgi Güvenliği İhlal Olayı Yönetimi", " Bölüm 13: İş Sürekliliğinin Bilgi Güvenliği Hususları" ve "Bölüm 14: Uyum" bölüm ortalaması gözlenen farklara göre istatiksel olarak anlamlıdır. Farkın kaynağını belirlemek için yapılan Dunn testleri sonucunda yalnızca 2. ve 3. Basamak hastanede, ADSM ve Diş Hastanesinde ve İl Sağlık Müdürlüğünde çalışanların "Bölüm 4: İnsan Kaynakları Güvenliği", "Bölüm 6: Kriptografi", "Bölüm 7: Fiziksel ce Çevresel Güvenlik", "Bölüm 8: İşlem Güvenliği", "Bölüm 9: Haberleşme Güvenliği", "Bölüm 11: Tedarikçi İlişkileri ", "Bölüm 12: Bilgi Güvenliği İhlal Olayı Yönetimi", " Bölüm 13: İş Sürekliliğinin Bilgi Güvenliği Hususları" ve "Bölüm 14: Uyum" İlçe Sağlık Müdürlüğü'nde çalışan bilgi işlem personelinden daha yüksek bulunmuştur. Farkın sebebi incelendiğinde 2. ve 3. Basamak sağlık tesisi, ADSM ve Diş Hastanesinde, İlçe Sağlık Müdürlüğünde ve İl Sağlık Müdürlüğünde çalışanların bilgi güvenliği faaliyetlerine yönelik çalışmaların süreklilik arz etmesi, ilçe sağlık müdürlüğünde çalışan personelin daha çok donanım ve uygulamaya yönelik süreçlerin koordine etmesinden ve bilgi güvenliği yönetim ve politikalarından il sağlık müdürlüğüne bağlı olmasından kaynaklı olabileceği düşünülmektedir. Özdemir ve Uluyol (2021), eğitim düzeyine göre lise ve altı eğitim seviyesine sahip katılımcıların farkındalık seviyelerinin düşük, üniversite ve üstü eğitime sahip katılımcıların ise yüksek olduğu sonucuna ulaşılmıştır.

ISO 27001 alt maddelerine verilen cevaplardan sağlık tesislerinin kapasitesi büyüklükleri açısından büyük (400 yatak ve üzeri), küçük (400 yatak ve altı) ve idari sağlık kuruluşunda çalışan "Bölüm 8: İşlem Güvenliği", "Bölüm 10: Sistem Temini, Geliştirme ve Bakımı" ve "Bölüm 14: Uyum" bölüm ortalamaları kendi içlerinde gözlenen farklardan en az biri istatistiksel olarak anlamlıdır. Farkın kaynağını belirlemek için yapılan Dunn testleri sonucunda yalnızca büyük sağlık kuruluşlarda çalışan personelin "Bölüm 8: İşlem Güvenliği", "Bölüm 10: Sistem Temini, Geliştirme ve Bakımı" ve "Bölüm 14: Uyum" bölüm ortalaması idari yapıda çalışanlardan daha yüksek bulunuştur.

Tuygun (2019) çalışmasında olduğu gibi yönetici pozisyonunda olanların cevapları incelendiğinde, ISO27001 tüm maddelerine göre değerlendirildiğinde uygulama ve politikalara yüksek düzeyde hâkim oldukları görülmektedir. Sağlık Bakanlığı Sözleşmeli Yönetici Performans Değerlendirme Yönergesi "Bilgi Güvenliği (BG) Politikalarına Uyum Oranı"

göstergelerinin değerlendirme ve raporlanması esaslara göre yöneticilerin puanlama kriterleri içerisinde olmasından dolayı yüksek düzeyde farkındalık olduğu düşünülmektedir. Mete 2010, çalışmasında belirttiği gibi: ISO/IEC 27001 BGYS standardını, kurmak ve yönetmek isteyen bilgi işlem merkezi yöneticilerine sistemin kurulup, yönetilmesi aşamalarında dışarıdan destek alınsa dahi, kendi çalışanları içinden konu hakkında yüksek bilgi düzeyine erişmiş ve süreçlere hâkim bir ekibin varlığı anketin uygulandığı sağlık tesislerinde görülmektedir.

Diesch ve ark (2020) tarafından kurumsal bilgi güvenliği bağlamında; fiziksel güvenlik, güvenlik açığı, altyapı, farkındalık, erişim kontrolü, risk, kaynaklar, organizasyonel faktörler, süreklilik, güvenlik yönetimi, uyumluluk ve politika önemine vurgu yaparken çalışmada elde edilen veriler çerçevesinde sağlık tesislerinde bilgi sistemleri ve teknik altyapının yönetiminden görevli çalışanların genel farkındalık seviyeleri çok yüksek düzeyde olduğu tespit edilmiştir. Bilen (2016)'in çalışmasında tespit etmiş olduğu üzere kamu kurumundaki teknik birimlerde çalışan personelin bilgi güvenliği konusunda farkındalık düzeyinin yeterli olduğu görülmektedir. Bunun nedeninin ağırlıklı olarak bilişim alanında almış oldukları eğitim durumları ve Sağlık Bakanlığının bu alandaki politikaların sıkı bir şekilde denetleme ve takibinden kaynaklı sürecin farkındalığı olarak söylenebilir. Baran ve Şener (2020), çalışılan birimlere göre yaptıkları çalışmada Bilgi Teknolojileri Daire Başkanlığında görev yapan katılımcıların diğer birimlerde görev yapan katılımcılara oranla daha yüksek bilgi güvenliği farkındalığına sahip olduğu sonucuna varmıştır.

Meral ve Bülbül (2022), çalışmasında bilgi güvenliği politikalarının %77,80 oranında etkin olduğu, farkındalık ve eğitim konularında %66 oranında etkin tespit etmiş olmasına rağmen çalışmamızın bu oran %96 üzerinde olduğu sonucuna ulaşılmıştır. Chua ve ark. (2018); Alkalbani ve ark (2017) tarafından kuruluşlarda bilgi güvenliği politikalarının farkındalığı ve uyumu üzerinde önemli etkileri olduğunu belirtirmiştir. Yıldız (2022), çalışmasında bilgi güvenliğinin sağlıklı ve dinamik şekilde gerçekleştirilmesi için en önemli kuralın tüm kurum personelinin süreç hakkında bilgi sahibi olması ve özellikle teknik personelin ISO27001'in kurumsal teknik süreçler üzerinde uygulamasının olduğunu, Sabbagh ve ark.,(2012) bilgi güvenliği kültürü, çalışanların düşüncelerini, duygularını ve günlük faaliyetlerini kapsadığını belirtmektedir.

6. SONUÇ VE ÖNERİLER

Bu çalışmada; Ankara ili sağlık kurumları bilgi işlem birimi çalışanlarının "ISO/IEC 27001 Bilgi Teknolojisi, Güvenlik Teknikleri, Bilgi Güvenliği Yönetim Sistemleri, Gereksinimler dokümanı EK-A' da yer alan Referans Kontrol Amaçları ve Kontroller başlığı altında yer alan kontrol listesi paralelinde hazırlanan maddelerin; cinsiyete, deneyime, eğitim düzeyine, unvana, çalıştığı birime, çalıştığı kurumun türüne ve çalıştığı kurumun kapasitesine göre bilgi güvenliği yönetim farkındalığı arasındaki ilişkiyi bulmak amaçlanmıştır. Genel olarak değerlendirildiğinde bilgi işlem biriminde çalışan personel ile yöneticilerin kavramsal kontrol maddelere göre farkındalık düzeyinin yüksek olduğu tespit edilmiştir.Katılımcıların cinsiyet ile mesleki deneyimlerine göre bilgi güvenliği yönetimi kavramsal farkındalık düzeyi arasında çalışmamızda anlamlı ve pozitif yönlü bir farklılık bulunamamştır. Eğitim durumu, unvan, çalıştığı kurum türü ve kapasitesi ile bilgi güvenliği yönetimi kavramsal farkındalık düzeyi arasında anlamlı ve pozitif yönlü bir ilişki olduğu tespit edilmiştir.

Kurumsal bilgiler kurumlar için varlıklarını devam ettirebilmeleri açısından hayati bir önem taşımaktadır. Kurumsal bilgi kaybı, kurumlar için ciddi maddi ve manevi kayıplara neden olabilmektedir. Bu nedenle kurumların kurumsal bilgilerini korumak için öncelikle sahip olduğu bilgilerin ve bu bilgilerin yer aldığı, oluştuğu, işletildiği ve iletildiği her bilgi varlığının farkında olması gerekmektedir. Ülkemizde TS ISO/IEC 17021 standardı kapsamında Türk Akreditasyon Kurumundan (TÜRKAK) akredite edilmiş kurum ve kuruluşlardan alınmış TS ISO/IEC 27001 bilgi güvenliği yönetim sistemi olarak da uygulanan bilgi güvenliği standardı, uygulanması için bir dizi ilkeyi özetleyen bir klavuz olarak yer almaktadır.

Literatür çalışmalarında ve veri ihlali gerçekleşen olayların incelenmesinde; veri ihlalinin bir süreç olduğu, ihlalın başlangıcından tespit edildiği ana kadar geçen sürenin uzun olduğu ve ihlalil boyutlarını etkisi daha sonradan anlaşılabileceği tespit edilmiştir. İhlal sonrasında kurumsal itibar, finansal yapı, rakipler, sigorta, rekabet, personel, toplumsal itibar ve reklam gibi etkileri üzerinde sonucuna varılmıştır.

Sağlık hizmetlerinin dijitalleşmesi süreci ile birlikte; hasta bilgilerine en hızlı şekilde ulaşım, sağlık profesyonelleri birbirleri arasında etkileşimi, tedavi ve uygulama sonuçlarına erişim, maliyetleri düşürmek ve insan hatalarını en aza indirmek için tıbbi yazılım sistemleri, mobil ve web uygulamaları sayesinde süreçler günümüzde etkin bir şekilde yürütülmektedir. Sağlık kayıtlarının tıbbi geçmiş, gözlemler, teşhisler, numuneler ve raporlar gibi hastalıklar hakkında kümülatif bilgiler içermesi ile birlikte sağlık verisinin önemi, piyasa değeri

noktasında kanun koyucuların bu alanda verilerin saklanmasında, korunmasında ve erişimi noktasında belirli bir değişikliği de zorunlu olarak beraberinde getirmiştir.Çalışmanın literatür kısmından elde edilen veriler çerçevesinde sağlık hizmetleri de dahil olmak üzere tüm sektörlerde siber saldırılar giderek artmaktadır. E-posta, internet sitesi, kimlik avı dolandırıcılığı, personel hataları vb. işlemler sonucu kurumlar ciddi saldırılar ile yüz yüze gelebilmektedir. Saldırıların en büyük nedeni sağlık verilerin mali değeri olarak düşünülmesine karşın siyasi amaçlar, hizmeti kesintiye uğratmak, ayrıcalık edinme gibi birçok nedeni de olabilmektedir. Örn: Laboratuvar sonuçlarını değiştirmek, radyolojik görüntüler üzerinde değişiklik, maaş ve özlük haklarında değişiklik, fatura bilgilerinde değişiklik, sağlık tesisinin tıbbi kayıtlara erişimi engellemek, arşiv dosyalarını silme, kopyalama veya değiştirme vb.

Sağlık hizmeti veren kuruluşların bilgi güvenliği kavramı, hastanın elektronik sağlık kayıtlarının güvenliğini/gizliliğini sağlamak için her bir süreci etkin bir şekilde kontrol ve yönetmesi gerekirken, sağlık hizmeti sağlayıcılarının paydaşları arasında herhangi bir bilginin işlenmesi sırasında, bilgi güvenliği, bütünlük, gizlilik ve hesap verebilirlik özelliklerine sahip olmanın temel gerekliliklerin yasalar tarafından oluşturulan kuralara ve uluslararası standartlara göre düzenlenmesi gerekir. Çalışma kısmında literatürden elde edilen veriler ışığında bilgi, bilgi güvenliği teknolojileri, veri ihlali sonuçlarına yönelik kavramsal bilgiler elde edilmiştir. Sağlık bilgi teknolojilerinin temel amacı klinisyen ve hasta memnuniyetini artırmak, bakıma ilişkin erişimi artırmak, zaman, maliyetleri azaltmak veya kontrol altın almak, gerek hasta gerekse personelin herhangi bir yerden uzak bağlantı yoluyla verilere 7/24 ulaşımı sağlarken gelişen teknolojiler ve artan bağlantı sebebiyle siber güvenlik ve tehdit noktasında idari ve klinik sistemleri tehdit etmektedir. Sağlık yöneticileri tarafından teknolojiler ve risklerin belirlenmesi, tespit ve müdahale süreci, cihaz gereksinimi ve düzenleyici önlemler için stratejilerini teknik, mali ve idari olarak ayrı ayrı oluşturup politikaların uygulamaları gerekmektedir.

Prognostik ve sağlık yönetimi açısından uygulamada birçok yöntem bulunmakla birlikte sağlık tesis yöneticileri açısından;

- Siber güvenlik aynı zamanda ödün verme meselesidir (Epfl 2017). Sağlık tesislerinde personel ilişkilerinden dolayı bilgi işlem personelinin standart kullanıcılara idari ayrıcalıklar verilmesi davranış durumu çok fazladır. Yönetici veya ayrıcalıklı hesap verilen standart idari kullanıcılarının ayrıcalıklarının getirdiği riskler hakkında önlemler alınmalıdır.

- Sağlık hizmet sunulan her noktada genellikle ağa entegre edilmiş çok sayıda personelin ya da hastaların kişisel cihazları (cep telefonu, notebook, tablet vb.) bulunmaktadır. Sağlık kuruluşu, mobil cihaz yönetimi için makul önlemler ve politikalar oluşturarak şifrelemeyi ve korunmayı zorunlu kılmalıdır.
- Sağlık tesisi yöneticileri tıbbi cihaz ve hizmet sunan diğer cihazlaın güncelleme ve yamalarını uygulanması noktasında aksatmadan yapmaları gerekmektedir. Güncelleme sırasında çalışan sistemin bozulacak düşüncesi, hizmet veren personelin rahatsızlık duyacak algısına yönelik süreçten taviz verilmemesi gerekmektedir.
- Sağlık Bakanlığı Sağlık Bilgi Yönetim Sistemleri Hakkında Yönetmelik hükümleri uyarınca sağlık bilgi yönetim sistemi hizmeti sağlayıcıları ile bu hizmetten yararlanan sağlık bilgi yönetim sistemi hizmet alıcılarının uymaları gereken kurallara ilişkin hükümleri kapsamaktadır. Sağlık tesis yöneticileri ilgili yönetmelikler kapsamında; sağlık bilişim standartlarına ve veri gönderimi süreçlerine, hizmet alımı kapsamında teknik şartnamelere, yetki belgelerine, veri tabanı yönetim sistemi süreçlerine, sistem güncelleme, iyileştirme ve değerlendirme süreçlerine, veri yedekleme, uyum, akreditasyon, veri ihlali, gizlilik ve denetim noktalarında bilgi sahibi olmaları ve her bir aşamanın yönetiminde dikkat etmeleri gerekmektedir.
- Sağlık tesislerinin her aşamasında üretilen değerli bilgilerin korunması, saklanması ve erişimi noktasında ister hata ister davranış sonucu oluşabilecek durumların önüne geçmeye çalışmak için uygulamaya yönelik faaliyetler oluşturulmalıdır. Bilgi işlem personelinin veri ihlali durumunda yönetmeliklerle düzenlenmiş politikaları uyması noktasında birim içi eğitimlere önem verilmelidir. Sağlık tesis yöneticileri; aynı zamanda karşılaşılabilecek durumlara yönelik düzenli olarak veri ihlali olabilecek her noktanın test etmeli, uygulamaya yönelik süreçlerin tabiki yapmalıdır.

Hastanelerdeki bilgi sistemlerine yönelik tehditler, iç tehditler(dâhili) ve dış tehditler(harici) olmak üzere iki ana ihlali olarak sınıflandırılmıştır. Personelden kaynaklı olarak yer almakta olan dahili tehditler, bilgisizlik, merak, yetersiz eğitim, sosyal ve kültürel durumlar, etik, ahlaki, başkasının şifresini almak ve şifresini başka bir çalışana vermek gibi çeşitli çalışan davranışlarını içermektedir. Harici tehditlere örnek ise virüsleri ve casus yazılım saldırılarını, bilgisayar korsanları örnek verilebilir. Her iki durum için de iyi bir bilgi güvenliği sisteminin sadece teknolojik olarak değil araştırmacıların onu kullananların elinde olduğuna yönelik çok düzeyli, boylamsal çalışmalar yaparak farkındalık ve durum tespiti yapmaları

gerekmektedir. Sağlık personelinin aşağıda yer alan maddelere yönelik bilgi işlem personeli tarafından bilinçlerini artırmaya yönelik çalışmalar yapılmalıdır. Bunlardan bazıları;

- Bilgi güvenliği politikalarına ve yönergelerine yeterince dikkat etmezsem, kuruluşumun verileri ve kaynakları tehlikeye girebileceğini,
- Bilgisayarıma virüs bulaşması benim ve kuruluşum için ciddi bir soruna neden olabileceğini,
- İş yerinde, gizli bilgilerime birinin iznim veya bilgim olmadan erişmesi ciddi bir sorun olabileciğini,
- Bilgi güvenliği ilkelerini izlersem, kuruluşumun bilgi güvenliğini sağlamaya yardımcı olma konusunda bir fark yaratabileceğini,
- Bir ihlal sorunu ortaya çıkarsa bunun olumsuz etkileri olabileceğinin,
- Çalışanlar, sosyal saldırıları tanıma ve bunlara tepki verme eğitimlerinin alması gerektiğinin, Sosyal ağ sitelerinde herhangi bir şey yayınlamadan önce bilgi ihaleline yönelik olumsuz sonuçlarının olabileceğini,
- Çalışanlar hassas/gizli bilgilerini güvenli olmayan yerlere bırakılmaması gerektiğini,
- Çalıştığım sağlık tesisinin bilgi güvenliği politikası, kurumsal bilgi varlıklarına erişimi ve kullanımıyla ilgili bir dizi kural ve ilkelere uyulması gerektiğinin,
- Uzun yıllardır odak noktası esas olarak bilgi işlem birimine ve teknik uzmanlara bırakılmasına rağmen dikkat etmem gereken kuralların ve sorumluluklarımın bilincinde olduğuna yönelik çalışmalardır.

Sağlık hizmetlerinde bilgi güvenliği, veri ihlali, mahremiyet vb kavramların ağırlıklı olarak hasta bilgileri, hastaya ait tani ve tedavi dosyalarına ilişkin bilgiler olarak düşünülmektedir. Sağlık tesisinde satınalma, faturalandırma, sevk işlemleri, maaş, özlük vb idari alanlar ile birlikte tesisin ıstma ve soğutma sistemleri, asansör ve bakım sistemleri, medikal gaz sistemleri, kamera, santral ile her türlü kompanizasyon sistemleri de düşünüldüğünde hekim ve hekim dışı sağlık personeli açısından gizlilik, bilgi mahremiyeti, teknoloji okuryazarlığı ve veri ihlali farkındalığı noktasında ayrı ayrı da incelenmesi gerektiği düşünülmektedir.

KAYNAKLAR

Abidi, S. S. R. (2001). Knowledge management in healthcare: towards 'knowledge-driven'decision-support services. International journal of medical informatics, 63(1-2), 5-18. https://doi.org/10.1016/S1386-5056(01)00167-8

Abouelmehdi, K., Beni-Hessane, A., & Khaloufi, H. (2018). Big healthcare data: preserving security and privacy. Journal of big data, 5(1), 1-18. https://link.springer.com/article/10.1186/s40537-017-0110-7

Acharyulu, G. V. R. K. (2011). Information management in a health care system: Knowledge management perspective. *International Journal of Innovation, Management and Technology*, *2*(6), 534-537. http://www.ijimt.org/papers/187-M639.pdf

Adsivera. What is The Meaning of ISO 27001?.https://advisera.com/27001academy/what-is-iso-27001/Erişim Tarihi: 19.04.2021

Agarwal, R., Gao, G., DesRoches, C., & Jha, A. K. (2011). The role of information systems in healthcare: Current research and road ahead. Information Systems Research, 22, 419-428.

Ahıma. Health Information, https://www.ahima.org/certification-careers/certifications-overview/career-tools/career-pages/health-information-101/, Erişim Tarihi: 15.09.2022

Akpan, A. Has Health Care Hacking Become an Epidemic?The Public Broadcasting Service.2016 Https://Www.Pbs. Org/Newshour/Science/Has-Health-Care-Hacking-Become-An- Epidemic. Erişim Tarihi: 01.10.2022

Akal, M. (2022). Bilişim firmalarında bilgi güvenliği farkındalığı. Ufuk Üniversitesi / Sosyal Bilimler Enstitüsü / Yönetim Bilişim Sistemleri Ana Bilim Dalı / Yönetim Bilişim Sistemleri Bilim Dalı

Alder, S. Healthcare Data Breach Report: 25% Increase in Breaches in 2020, Https://Www.Hipaajournal.Com/2020-Healthcare-Data-Breach-Report-Us/, Erişim Tarihi: 19.04.2021

AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2022). Employees' intentions toward complying with information security controls in Saudi Arabia's public organisations. *Government Information Quarterly*, *39*(4), 101721.https://doi.org/10.1016/j.giq.2022.101721.

Alemdaroglu, A. (2020). *Çalışanların bilgi güvenliği farkındalığına ilişkin algıları: bankacılık sektöründe bir araştırma* (Master's thesis, İstinye Üniversitesi/Sosyal Bilimler Enstitüsü/İşletme).

Alkalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Information security compliance in organizations: An institutional perspective. Data and Information Management, 1(2), 104-114.

Al Sabbagh, B., Ameen, M., Wätterstam, T., & Kowalski, S. (2012, September). A prototype For HI 2 Ping information security culture and awareness training. In 2012 international conference on E-learning and E-technologies in education (ICEEE) (pp. 32-36). IEEE.

Aslan, Z. Hemşire Akademisyenlerin Bilgi Güvenliği Farkındalık Düzeylerinin Ve Etkileyen Faktörlerin Belirlenmesi. Ege Üniversitesi Sağlık Bilimleri Enstitüsü, Yüksek Lisans Tezi 2019. Yöktez.

Altameem, A., Kovtun, V., Al-Ma'aitah, M., Altameem, T., Fouad, H., & Youssef, A. E. (2022). Patient's data privacy protection in medical healthcare transmission services using back propagation learning. Computers and Electrical Engineering, 102, 108087 ISSN 0045-7906

Alotaibi, Y. K., & Federico, F. (2017). The impact of health information technology on patient safety. *Saudi medical journal*, *38*(12), 1173. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5787626/

Antunes, H. D. J. G., & Pinheiro, P. G. (2020). Linking knowledge management, organizational learning and memory. *Journal of Innovation & Knowledge*, *5*(2), 140-149. https://doi.org/10.1016/j.jik.2019.04.002

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International journal of Internet and enterprise management*, *6*(4), 279-314. https://doi.org/10.1504/IJIEM.2010.035624

Aras, M. (2018). İşletmelerde bilgi koruma stratejileri. *Ordu Üniversitesi Sosyal Bilimler Enstitüsü Sosyal Bilimler Araştırmaları Dergisi*, *8*(3), 613-621.

Argaw, S. T., Troncoso-Pastoriza, J. R., Lacey, D., Florin, M. V., Calcavecchia, F., Anderson, D., ... & Flahault, A. (2020). Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. *BMC medical informatics and decision making*, *20*, 1-10. https://link.springer.com/article/10.1186/s12911-020-01161-7

Askari-Majdabadi, H., Valinejadi, A., Mohammadpour, A., Bouraghi, H., Abbasy, Z., & Alaei, S. (2019). Use of health information technology in patients care management: A mixed methods study in Iran. *Acta Informatica Medica*, *27*(5), 311. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7085310/

Baran, S, Şener E. (2020). Örgütlerde bilgi güvenliğini etkileyen bir unsur: örgütsel bilgi paylaşımı. *Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (41), 410-427.

Başdinkçi, N. (2017). Sağlık kurumlarında bilgi güvenliği risk değerlendirmesi ve kullanıcıların bilgi güvenliği farkındalık düzeyinin ölçülmesi (Doctoral dissertation, Yüksek Lisans Tezi). Çukurova Üniversitesi, Adana).

Beckers, K., Faßbender, S., Heisel, M., & Schmidt, H. (2012, August). Using security requirements engineering approaches to support ISO 27001 information security management systems development and documentation. In *2012 seventh international conference on availability, reliability and security* (pp. 242-248). IEEE. DOI: 10.1109/ARES.2012.35

Bhuyan, S. S., Kabir, U. Y., Escareno, J. M., Ector, K., Palakodeti, S., Wyant, D., ... & Dobalian, A. (2020). Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations. *Journal of medical systems*, *44*, 1-9. https://link.springer.com/article/10.1007/s10916-019-1507-y

Bischoff, P. (2019). How data breaches affect stock market share prices. Hentet, 5, 21. https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/ Erişim Tarihi: 03.12.2022

Bilen, A.(2016) Bir Kurumun Bilgi Güvenliği Farkındalığının İncelenmesi. Fırat Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi. https://openaccess.firat.edu.tr/xmlui/bitstream/handle/11508/18009/458010.pdf?sequence= 1&isAllowed=y

Bilgi Güvenliği Politikaları Kılavuzu. Sağlık Bakanlığı Sağlık Bilgi Sistemleri Genel Müdürlüğü, Sürüm 2.1., https://bilgiguvenligi.saglik.gov.tr/home/mevzuat, Erişim Tarihi: 10.09.2022

Bloomberglaw. China Personal Information Protection Law (PIPL) Faqs. https://pro.bloomberglaw.com/brief/china-personal-information-protection-law-pipl-faqs/

Blakley, B., McDermott, E., & Geer, D. (2001, September). Information security is information risk management. In Proceedings of the 2001 workshop on New security paradigms (pp. 97-104).

Buckland, M. K. (1991). Information as thing. Journal of the American Society for information science, 42(5), 351-360. https://doi.org/10.1002/(SICI)1097-4571(199106)42:5<351::AID-ASI5>3.0.CO;2-3

Brunner, M., Sauerwein, C., Felderer, M., & Breu, R. (2020). Risk management practices in information security: Exploring the status quo in the DACH region. *Computers & Security*, *92*, 101776. https://doi.org/10.1016/j.cose.2020.101776

Bokhari, S. A. A., & Manzoor, S. (2022). Impact of information security management system on firm financial performance: perspective of corporate reputation and branding. American Journal of Industrial and Business Management, 12(5), 934-954. DOI: 10.4236/ajibm.2022.125048

Bose, R. (2003). Knowledge management-enabled health care management systems: capabilities, infrastructure, and decision-support. Expert systems with Applications, 24(1), 59-71. https://doi.org/10.1016/S0957-4174(02)00083-0

Büyüköztürk, Ş.(2011). *Sosyal Bilimler İçin Veri Analizi El Kitabı*. Pegem Akademi.

Büyüköztürk, Ş. (2012). Çakmak, EÇ, Akgün, ÖE, Karadeniz, Ş., and Demirel, F. Bilimsel araştırma yöntemleri.

Carcary, M., Renaud, K., Mclaughlin, S., O'Brien, C.A. (2016). Framework For Information Security Governance And Management. It Professional. 18(2), 22-30. https://pureportal.strath.ac.uk/en/publications/a-framework-for-information-security-governance-and-management DOI:10.1109/MITP.2016.27

CDC. Health Insurance Portability and Accountability Act of 1996 (HIPAA), https://www.cdc.gov/phlp/publications/topic/hipaa.html, Erişim Tarihi: 12.10.2022

CDC.Health Information and Public Health, https://www.cdc.gov/phlp/publications/topic/healthinformation.html

Chernyshev, M., Zeadally, S., & Baig, Z. (2019). Healthcare data breaches: Implications for digital forensic readiness. Journal of medical systems, 43, 1-12. https://link.springer.com/article/10.1007/s10916-018-1123-2

Choi, S. J., & Johnson, M. E. (2019). Understanding the relationship between data breaches and hospital advertising expenditures. Am J Manag Care, 25(1), e14-e20. http://ajmc.s3.amazonaws.com/_media/_pdf/AJMC_01_2019_Choi%20final.pdf

Choobineh, J., Dhillon, G., Grimaila, M. R., & Rees, J. (2007). Management of information security: Challenges and research directions. Communications of the Association for Information Systems, 20(1), 57. DOI:10.17705/1CAIS.02057

Chua, H. N., Wong, S. F., Low, Y. C., & Chang, Y. (2018). Impact of employees' demographic characteristics on the awareness and compliance of information security policy in organizations. Telematics and Informatics, 35(6), 1770-1780.

Cisco. What Is Information Security? https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html, Erişim Tarihi: 15.11.2022

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48-52.Https://Doi.Org/10.1016/J.Maturitas.2018.04.008.

Coronado, A. J., & Wong, T. L. (2014). Healthcare cybersecurity risk management: Keys to an effective plan. Biomedical instrumentation & technology, 48(s1), 26-30. https://doi.org/10.2345/0899-8205-48.s1.26

Cyberseason. Ransomware The True Cost to Business 2022, https://www.cybereason.com/hubfs/dam/collateral/reports/ransomware-the-true-cost-to-business-2022.pdf, erişim tarihi. 01.10.2022

Çimen, Z.(2021). Sağlık Kurumlarında Bilgi Güvenliği Ve Çalışan Görüşleri: Ankara İli Özel Hastane Örneği: Ankara Hacı Bayram Veli Üniversitesi / Lisansüstü Eğitim Enstitüsü / Sağlık Yönetimi Ana Bilim Dalı / Hastane İşletmeciliği Bilim Dalı. Yöktez

Çubukçu, F.(2018). Bilgi Güvenliği Yönetim Sistemi ISO27001: 2013 Uygulama Kılavuzu. Pusula.

Dash, S., Shakyawar, S. K., Sharma, M., & Kaushik, S. (2019). Big data in healthcare: management, analysis and future prospects. Journal of Big Data, 6(1), 1-25. https://link.springer.com/article/10.1186/s40537-019-0217-0

Davenport, T. H., De Long, D. W., & Beers, M. C. (1998). Successful knowledge management projects. MIT Sloan management review, 39(2), 43. https://www.proquest.com/openview/76ca6820cf905f6422a30b881ac0c9ea/1?pq-origsite=gscholar&cbl=26142

Data Protection Act, (2018). UK Public General Acts. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

Demirdöğen, G., Işık, Z., & Arayici, Y. (2021). Facility management information taxonomy framework for queries in healthcare buildings. Journal of Building Engineering, 44, 102510. https://doi.org/10.1016/j.jobe.2021.102510

Derrick, H. D., Behara, R. S., & Goo, J. (2014). Optimal information security investment in a Healthcare Information Exchange: An economic analysis. Decision Support Systems, 61, 1–11. doi:10.1016/j.dss.2013.10.011

Dimitrov, D. V. (2016). Medical internet of things and big data in healthcare. Healthcare informatics research, 22(3), 156-163. http://dx.doi.org/10.4258/hir.2016.22.3.156

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. Computers & Security, 92, 101747.

DLA Piper. GDPR Data Breach Survey 2022, Https://iapp.Org/Resources/Article/Dla-Piper-Gdpr-Data-Breach-Survey/

DPA. Data Protection And The EU https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/overview-data-protection-and-the-eu/

Donaldson, M.S., Corrigan, J.M., Kohn, L.T. To Err Is Human, Institute of Medicine. (2000). To Err Is Human: Building A Safer Health System. Washington, DC: The National Academies Press.2000. Https://Nap.Nationalacademies.Org/Catalog/9728/To-Err-İs-Human-Building-A-Safer-Health-System, ERİŞİM Tarihi: 10.11.2022

Dzazali, S., Sulaiman, A., & Zolait, A. H. (2009). Information security landscape and maturity level: Case study of Malaysian Public Service (MPS) organizations. Government Information Quarterly, 26(4), 584-593. https://doi.org/10.1016/j.giq.2009.04.004

Eloff, M. M., & von Solms, S. H. (2000). Information security management: a hierarchical framework for various approaches. Computers & Security, 19(3), 243-256. https://doi.org/10.1016/S0167-4048(00)88613-7

Eichler, H. G., Bloechl-Daum, B., Broich, K., Kyrle, P. A., Oderkirk, J., Rasi, G., ... & Paris, V. (2019). Data rich, information poor: can we use electronic health records to create a learning healthcare system for pharmaceuticals?. Clinical Pharmacology & Therapeutics, 105(4), 912-922. https://ascpt.onlinelibrary.wiley.com/doi/full/10.1002/cpt.1226

Enisa [Webpage On The Internet] *Risk Management/Risk Assessment European Union Agency for Network And Information Security (ENISA)* 2005–2014. [Accessed March 11, 2014]. [Cited May 11, 2014]. Available From: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management.

Enisa (European Network And Information Security Agency), "Risk Management /Risk Assessment " (Available On-Line At http://www.enisa.europa.eu/rmra)

Epfl. Internet Of Things. Connected Medical & Health Devices and Connected Vehicles. Workshop Report. Lausanne: EPFL International Risk Governance Center; 2017. P. 6–29. Erişim Tarihi: 11.10.2022

Esatoğlu, A.E., Köksal, A.(2010). Sağlık hizmetlerinde bilgi yönetimi. İkinci Baskı, Ankara: Anadolu Üniversitesi Uzaktan Eğitim Yayınları.

Floyd, T., Grieco, M., & Reid, E. F. (2016, September). Mining hospital data breach records: Cyber threats to us hospitals. In 2016 IEEE Conference on Intelligence and Security Informatics (ISI) (pp. 43-48). IEEE. https://ieeexplore.ieee.org/abstract/document/7745441 DOI: 10.1109/ISI.2016.7745441

Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martinez-Caro, E., & Chinnaswamy, A. (2023). Resilience in healthcare systems: Cyber security and digital transformation. Technovation, 121, 102583. https://doi.org/10.1016/j.technovation.2022.102583

Gillies, A. (2011), "Improving the quality of information security management systems with ISO27000", The TQM Journal, Vol. 23 No. 4, pp. 367-376. https://doi.org/10.1108/17542731111139455

Glazer, R. (1993). Measuring the value of information: The information-intensive organization. IBM Systems Journal, 32(1), 99-110. DOI: 10.1147/sj.321.0099

GDPR. What is GDPR, The EU's New Data Protection Law?, Https://Gdpr.Eu/Faq/, Erişim Tarihi: 11.11.2022

Gordon, W. J., Fairhall, A., & Landman, A. (2017). Threats to information security—public health implications. The New England Journal of Medicine, 377(8), 707-709. https://www.saudemaispublica.com/uploads/9/8/9/4/98944468/356355652-nejmp1707212.pdf

Gonzalez, J. J., & Sawicka, A. (2002, October). A framework for human factors in information security. In Wseas international conference on information security, Rio de Janeiro (pp. 448-187).

Greaves, F., Joshi, I., Campbell, M., Roberts, S., Patel, N., & Powell, J. (2018). What is an appropriate level of evidence for a digital health intervention?. The Lancet, 392(10165), 2665-2667. doı:https://doi.org/10.1016/s0140-6736(18)33129-5

Fahey, R. A., & Hino, A. (2020). COVID-19, digital privacy, and the social limits on data-focused public health responses. International Journal of Information Management, 55, 102181. https://doi.org/10.1016/j.ijinfomgt.2020.102181

Freeman, E. H. (2007). Holistic information security: ISO 27001 and due care. Information Systems Security, 16(5), 291-294.https://doi.org/10.1080/10658980701746478

Fortune. This Big U.S. Health Insurer Just Got Hacked, https://fortune.com/2015/09/10/hack-health-insurer-bluecross/, erişim tarihi: 120.11.2022

Furnell, S., Heyburn, H., Whitehead, A., & Shah, J. N. (2020). Understanding the full cost of cyber security breaches. Computer fraud & security, 2020(12), 6-12. https://doi.org/10.1016/S1361-3723(20)30127-5

Hamdan, R. A. Z. A. K. (2018). Human factors for IoT services utilization for health information exchange. Journal of Theoretical and Applied Information Technology, 96(8), 2095-2105.

Hammoda, B., & Durst, S. (2022). A taxonomy of knowledge risks for healthcare organizations. VINE Journal of Information and Knowledge Management Systems.https://doi.org/10.1108/vjıkms-07-2021-0114

Hamidovic, H., & Kabil, J. (2011). An Introduction to Information Security Management in Health Care Organizations. ISACA Journal, 5, 2-3.

Habertük, (2022). Türkiye'deki Veri İhlallerinden 25 Milyondan Fazla Kişi Etkilendi, https://www.haberturk.com/turkiyedeki-veri-ihlallerinden-25-milyondan-fazla-kisi-etkilendi-3316727-teknoloji. Erişim Tairih. 01.11.2022

Haux, R. (2006). Health information systems–past, present, future. International journal of medical informatics, 75(3-4), 268-281. https://doi.org/10.1016/j.ijmedinf.2005.08.002

Hippa. Health Information Privacy, Https://www.Hhs.Gov/Hipaa/İndex.Html Erişim Tarihi: 12.10.2022

Hipaajournal. Healthcare Data Breach Statistics. https://www.hipaajournal.com/healthcare-data-breach-statistics/. Erişim Taihi: 09.10.2022

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. Decision Sciences, 43(4), 615-660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

Huang, C. D., Behara, R. S., & Goo, J. (2014). Optimal information security investment in a Healthcare Information Exchange: An economic analysis. Decision Support Systems, 61, 1-11. https://doi.org/10.1016/j.dss.2013.10.011

Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. Heliyon, 7(3), e06522. https://doi.org/10.1016/j.heliyon.2021.e06522

Humphreys, T. (2006). State-of-the-art information security management systems with ISO/IEC 27001: 2005. ISO Management Systems, 6(1), 15-18.

Humphreys, E.(2008). Information Security Management Standards: Compliance, Governance And Risk Management. *İnformation Security Technical Report*. 2008;*13*(4), 247-255. https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/info_security.pdf

IBM, 2021, X-Force Threat Intelligence Index , Https://Www.Cert.Hu/Sites/Default/Files/Xforce_Threat_İntelligence_İndex_2021_90037390usen.Pdf, Erişim Tarihi: 25.11.2022

IBM 2022, Cost Of a Data Breach 2022, Https://Www.Ibm.Com/Reports/Data-Breach, Erişim Tarihi: 25.11.2022

ICO, International Commission Office, Your Data Matters, Https://İco.Org.Uk/Your-Data-Matters/, Erişim Tarihi: 12.09.2022

ISO 27001 Definition: What is ISO 27001?, Https://Www.itgovernance.Co.Uk/iso27001erişim Tarihi: 19.04.2021

ISO.org. Health informatics — Information Security Management İn Health Using ISO/IEC 27002. https://www.iso.org/obp/ui/#iso:std:iso:27799:ed-2:v1:en. Erişim Tarihi: 07.06.2022.

ISO, International Standards Organization. (2004). ISO/IEC TR 13335-1:2004 Guidelines to The Man- Agement Of Information Technology Security (GMITS). Part1: Concepts And Models For IT Security. ISO/IEC, JTC 1, SC27, WG 1.

Ionescu, R. C., Ceauşu, I., & Ilie, C. (2018, January). Considerations on the implementation steps for an information security management system. In Proceedings of the International Conference on Business Excellence (Vol. 12, No. 1, pp. 476-485). https://doi.org/10.2478/picbe-2018-0043

Ioannidis, C., Pym, D., & Williams, J. (2016). Is public co-ordination of investment in information security desirable?. Journal of Information Security, 7, 60-80. https://publications.aston.ac.uk/id/eprint/29603/ https://doi.org/10.4236/jis.2016.72005

İleri, Y. Y. (2016). Örgütlerde bilgi güvenliği yönetimi, kurumsal entegrasyon süreci ve örnek bir uygulama. Anadolu Üniversitesi Sosyal Bilimler Dergisi, 17(4), 55-72. https://doi.org/10.18037/ausbd.417372

İleri, Y. Y. (2018). Sağlık Yönetim Bilişim Sistemleri. Çizgi Kitabevi. S. 32 Konya

Jara, A. J., Zamora-Izquierdo, M. A., & Skarmeta, A. F. (2013). Interconnection framework for mHealth and remote monitoring based on the internet of things. IEEE Journal on Selected Areas in Communications, 31(9), 47-65. https://ieeexplore.ieee.org/abstract/document/6585881

Jigna H. J., Tanwar, S., Tyagi, S., & Kumar, N. (2019). Securing electronics healthcare records in Healthcare 4.0 : A biometric-based approach. Computers & Electrical Engineering, 76, 398–410. doi:10.1016/j.compeleceng.2019.04

Kaiser, F. K., Wiens, M., & Schultmann, F. (2021). Use of digital healthcare solutions for care delivery during a pandemic-chances and (cyber) risks referring to the example of the COVID-19 pandemic. Health and Technology, 11, 1125-1137. https://link.springer.com/article/10.1007/s12553-021-00541-x

Kara, B., İleri, Y. Y. (2022). Covid-19 Pandemi Sürecinde Kullanılan Güncel Sağlık Bilişim Uygulamaları ve Yenilikçi Teknolojiler: İnsanlığa Katkıları ve Temel Kaygılar. Sağlık ve Toplum, 32(1), 33-52.

Kayrak, M.(2012). Bilgi Kriterleri Çerçevesinde Bilişim Teknolojileri Denetimi. Sayıştay Dergisi. (87), 143-167.

Keckley, P. H., Coughlin, S., & Gupta, S. (2011). Issue brief: privacy and security in health care: a fresh look. Deloitte Center for Health Solutions. Retrieved from http://www. deloitte. com/assets/Dcom-UnitedStates/Local% 20Assets/Documents/Health% 20Reform% 20Issues% 20Briefs/US _CHS_PrivacyandSecurityinHealthCare_022111. pdf.

Kessler, S. R., Pindek, S., Kleinman, G., Andel, S. A., & Spector, P. E. (2020). Information security climate and the assessment of information security risk among healthcare employees. Health informatics journal, 26(1), 461-473. DOI: 10.1177/1460458219832048

Kılıç, A.P.(2014) Hastane Bilgi Yönetim Sisteminin Bilgi Güvenliği Açısından Değerlendirilmesi. (Doktora Tezi). Marmara Üniversitesi Sağlık Bilimleri Enstitüsü.

Kılıç, B. (2019) ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Açısından Türkiye' De Hukuk Bürolarında Bilgi Güvenliği Yönetimi Yüksek Lisans Tezi Gazi Üniversitesi Bilişim Enstitüsü Adli Bilişim Ana Bilim Dalı.

Kumar, A., Kumar, R., & Sodhi, S. S. (2022). A novel privacy preserving blockchain based secure storage framework for electronic health records. Journal of Information and Optimization Sciences, 43(3), 549-570. https://doi.org/10.1080/02522667.2022.2042092

Kurt, S.G. (2019). Bilgi Güvenliğinin Bilgi İşlem Çalışanları Tarafından Değerlendirilmesi–Sağlık Sektöründe Bir Çalışma Yüksek Lisans Tezi Marmara Üniversitesi. Yöktez

Kruger, H. A., Drevin, L., Flowerday, S., & Steyn, T. (2011, August). An assessment of the role of cultural factors in information security awareness. In 2011 Information Security for South Africa (pp. 1-7). IEEE.

Kowalski, E., Cappelli, D., & Moore, A. (2008). Insider threat study: Illicit cyber activity in the information technology and telecommunications sector. carnegıe-mellon unıv pıttsburgh pa software engıneerıng ınst.

Kişisel Verilerin Korunması Kanunu (KVVK), Resmî Gazete Tarihi: 07.04.2016 Resmî Gazete Sayısı: 29677, https://www.mevzuat.gov.tr/

Larson, D. B., Magnus, D. C., Lungren, M. P., Shah, N. H., & Langlotz, C. P. (2020). Ethics of using and sharing clinical imaging data for artificial intelligence: a proposed framework. Radiology, 295(3), 675-682. https://doi.org/10.1148/radiol.2020192536

Liginlal, D., Sim, I., & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. computers & security, 28(3-4), 215-228. https://doi.org/10.1016/j.cose.2008.11.003

Lubis, M., Fauzi, R., Liandani, P., & Lubis, A. R. (2020, July). Information security awareness (ISA) towards the intention to comply and demographic factors: statistical correspondence analysis. In Proceedings of the 8th International Conference on Computer and Communications Management (pp. 79-84).

Luna, R., Rhine, E., Myhra, M., Sullivan, R., & Kruse, C. S. (2016). Cyber threats to health information systems: A systematic review. Technology and Health Care, 24(1), 1-9. https://content.iospress.com/articles/technology-and-health-care/thc1102. DOI: 10.3233/THC-151102

Malliouris, D., & Simpson, A. C. (2020, July). Underlying and consequential costs of cyber security breaches: Changes in systematic risk. Workshop on the Economics of Information Security.. https://weis2020.econinfosec.org/wp-content/uploads/sites/8/2020/06/weis20-final14.pdf

Maarop, N., Thamadharan, K., Samy, G. N., Zainuddin, N. M. M., Azmi, A., Yusop, O. M., & Azizan, A. (2016). Information security management system implementation success factors: a review. Advanced Science Letters, 22(10), 3023-3026. DOI: https://doi.org/10.1166/asl.2016.8005

Management System Standards. Https://Www.iso.Org/Management-System-Standards.Html, Erişim Tarihi: 20.04.2021

Marttin, V., & Pehlivan, İ. (2010). ISO 27001: 2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir Đnceleme. Mühendislik Bilimleri ve Tasarım Dergisi, 1(1), 49-56.

McFadzean, E., Ezingeard, J. N., & Birchall, D. (2006). Anchoring information security governance research: sociological groundings and future directions. Journal of Information System Security, 2(3), 3-48. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=851f26460feea37fb1c3bab1b1942d6a5bc91c74

McLeod, A., ve Dolezel, D. (2018). Cyber-analytics: Modeling factors associated with healthcare data breaches. Decision Support Systems, 108, 57-68. https://doi.org/10.1016/j.dss.2018.02.007

Mcy, K. Perspectives On Transforming Cybersecurity. Mckinsey Glob. Inst.2019; 32, 1-128. https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx

Mehraeen, E., Ayatollahi, H., & Ahmadi, M. (2014). A study of information security in Hospital Information Systems. Health Information Management, 10(6), 779-788.

Meier, C., A. Fitzgerald MC, Smith JM. Ehealth: Extending, Enhancing, And Evolving Health Care. Annual Review Of Biomedical Engineering.2013;15, 359-382. https://him.mui.ac.ir/him/index.php/him/article/view/468/article_11238.html?lang=en

Meral, S., & BÜLBÜL, H. İ. (2022). Kamu Kurumlarının Bilgi Güvenliği Politikalarının Kurumsal Bilgi Güvenliğinin Sağlanması Açısından Etkinliğinin Analiz Edilmesi. Gazi University Journal of Science Part C: Design and Technology, 10(2), 314-329.

Mete, H. (2010). ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi' Nin Bilgi İşlem Merkezlerinde Uygulanması. (Yayınlanmamış Yüksek Lisans Tezi).Sakarya Üniversitesi Sosyal Bilimler Enstitüsü. Sakarya

Milicevic, D. & Goeken, M., (2010). Konzepte der Informationssicherheit in Standards am Beispiel ISO 27001. In: Fähnrich, K.-P. & Franczyk, B. (Hrsg.), INFORMATIK 2010. Service Science – Neue Perspektiven für die Informatik. Band 2. Bonn: Gesellschaft für Informatik e.V.. (S. 305-310).

Mitnick, K., Simon, W. (2022) The Art Of Deception: Controlling The Human Element of Security. Wiley Publishing.

Muthuppalaniappan, M., & Stevenson, K. (2021). Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. International Journal for Quality in Health Care, 33(1), mzaa117. https://doi.org/10.1093/intqhc/mzaa117

Murphy, G. F., Hanken, M. A., & Waters, K. A. (1999). Electronic health records: changing the vision. (No Title).

Nadiminti, R., Mukhopadhyay, T., & Kriebel, C. H. (1996). Risk aversion and the value of information. Decision Support Systems, 16(3), 241-254. https://doi.org/10.1016/0167-9236(95)00023-2

Narayana Samy, G., Ahmad, R., & Ismail, Z. (2010). Security threats categories in healthcare information systems. Health informatics journal, 16(3), 201-209. DOI: 10.1177/1460458210377468

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors, 21(15), 5119.

OAIC, What Is Health Information?2022, Https://www.Oaic.Gov.Au/Privacy/Health-İnformation/What-İs-Health-İnformation

Patterson, T. (2003). Holistic security: why doing more can cost you less and lower your risk. Computer Fraud & Security, 2003(6), 13-15.

Park, C. S., Jang, S., & Park, Y. (2010). A study of effect of Information Security Management System [ISMS] certification on organization performance. IJCSNS International Journal of Computer Science and Network Security, 10(3), 10-21. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=39d2ebb23620785b968f369bdd1e76a11a67ac59

Parasuraman, R., & Riley, V. (1997). Humans and automation: Use, misuse, disuse, abuse. Human factors, 39(2), 230-253. https://doi.org/10.1518/001872097778543886

Pavlov, G., Karakaneva, J.(2011) Information Security Management System İn Organization. Trakia Journal Of Sciences. 9(4), 20-25. http://www.uni-sz.bg/tsj/Vol9N4_2011/J.Karakaneva.pdf

Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: guidelines for effective information security management. CRC press.

Petersilge, C. A. (2020). The enterprise imaging value proposition. Journal of Digital Imaging, 33(1), 37-48.Https://Doi.Org/10.1007/S10278-019-00293-1

Pick, E. Importance Of Data Security in Healthcare, https://insightscare.com/importance-data-security-healthcare/, Erişim Tarihi: 19.04.2021

Pieters, W.(2011) The (social) construction of ınformation security. The Information Society. 27(5), 326–335. Doi:10.1080/01972243.2011.607038

Pituch, K. A., & Stevens, J. P. (2015). Applied multivariate statistics for the social sciences: Analyses with SAS and IBM's SPSS. Routledge.

Pıdeda. Fair information principles, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

Proença, D., & Borbinha, J. (2018). Information security management systems-a maturity model based on ISO/IEC 27001. In Business Information Systems: 21st International Conference, BIS 2018, Berlin, Germany, July 18-20, 2018, Proceedings 21 (pp. 102-114). Springer International Publishing.

Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. Journal of Management Information Systems, 32(4), 179-214.https://Doi.Org/10.1080/07421222.2015.1138374

Razaque, A., Amsaad, F., Jaro Khan, M., Hariri, S., Chen, S., Siting, C., & Ji, X. (2019). Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain. IEEE Access, 7, 168774-168797. [8888271]. https://doi.org/10.1109/ACCESS.2019.2950849

Reisman, M. (2017). EHRs: the challenge of making electronic data usable and interoperable. Pharmacy and Therapeutics, 42(9), 572.

Resmî Gazete. 2016. Kişisel Verilerin Korunması Kanunu, Sayı: 29677 Mükerrer.

Ricciardi, W. (2019). Assessing the impact of digital transformation of health services: Opinion by the Expert Panel on Effective Ways of Investing in Health (EXPH). European Journal of Public Health, 29(Supplement_4), ckz185-769.https://op.europa.eu/en/publication-detail/-/publication/83d00a4a-2b53-11e9-8d04-01aa75ed71a1/language-en, Erişim Tarihi: 27.11.2022

RM Studio. The Standard For ISMS, Https://www.Riskmanagementstudio.Com/İso-İec-27001/, Erişim Tarihi: 10.11.2022

RSI Security. What's The Dıfference Between Hıpaa and Pıpeda for Healthcare Organızatıons?https://blog.rsisecurity.com/whats-the-difference-between-hipaa-and-pipeda-for-healthcare-organizations/ 2020, Erişim Tarihi: 09.10.2022

Roberts, S. J. (2014). The necessity of information security in the vulnerable pharmaceutical industry. Journal of Information Security, 5(04), 147. DOI:10.4236/jis.2014.54014

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. Heliyon. https://www.cell.com/heliyon/pdf/S2405-8440(23)01441-X.pdf

Safa, N. S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. Journal of information security and applications, 40, 247-257.

Sağıroğlu, Ş., Alkan, M. (2018) Siber Güvenlik Ve Savunma. Grafiker Yayınları. Ankara.

Sheikhpour, R., & Modiri, N. (2012). A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. Indian journal of science and technology, 5(2), 2170-2176.

Schmit, C., Sunshine, G., Pepin, D., Ramanathan, T., Menon, A., & Penn, M. (2017). Transitioning from paper to digital: state statutory and regulatory frameworks for health information technology. Public Health Reports, 132(5), 585-592.

Scott, M., & Wingfield, N. (2017). Hacking attack has security experts scrambling to contain fallout. New York Times, 13.

Secundo, G., Toma, A., Schiuma, G., & Passiante, G. (2019). Knowledge transfer in open innovation: A classification framework for healthcare ecosystems. *Business Process Management Journal*, *25*(1), 144-163.Https://Doi.Org/10.1108/BPMJ-06-2017-0173

Securityscorecard, Top 25 Cybersecurity Frameworks To Consider, 2021, Https://Securityscorecard.Com/Blog/Top-Cybersecurity-Frameworks-To-Consider, Erişim Tarihi: 08.09.2022

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020, May). Healthcare data breaches: insights and implications. In Healthcare (Vol. 8, No. 2, p. 133). MDPI.Https://Doi.Org/10.3390/Healthcare8020133

Shen, C., Zhang, H., Feng, D., Cao, Z., & Huang, J. (2007). Survey of information security. Science in China Series F: Information Sciences, 50(3), 273-298.Https://Doi.Org/10.1007/S11432-007-0037-2

Shojaie, B., Federrath, H., & Saberi, I. (2014, September). Evaluating the effectiveness of ISO 27001: 2013 based on Annex A. In 2014 Ninth International Conference on Availability, Reliability and Security (pp. 259-264). IEEE. DOI: 10.1109/ARES.2014.41

Sheikhpour, R., & Modiri, N. (2012). A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management. Indian journal of science and technology, 5(2), 2170-2176.

Silva, M. M., de Gusmão, A. P. H., Poleto, T., e Silva, L. C., & Costa, A. P. C. S. (2014). A multidimensional approach to information security risk management using FMEA and fuzzy theory. International Journal of Information Management, 34(6), 733-740.

Singh, A., & Chatterjee, K. (2019). Security and privacy issues of electronic healthcare system: a survey. Journal of Information and Optimization Sciences, 40(8), 1709-1729.

Sidhu, S. Information Security in The Healthcare System.2018. Https://Scholarworks.Calstate.Edu/Downloads/2r36v037p?Locale=En, Erişim TARİGİ: 05.11.2022

Speed, A. E., Woo, B. L., Kouhestani, C. G., Stubbs, J. J., & Birch, G. C. (2018, October). Human factors in security. In 2018 International Carnahan Conference on Security Technology (ICCST) (pp. 1-5). IEEE.

Sulleyman, A. (2017). NHS cyber attack: why stolen medical information is so much more valuable than financial data. Independent (2017).http://www. independent.co.uk/life-style/gadgets-and-tech/news/nhs-cyber-attack-medical- data-records-stolen-why-so-valuable-to-sell-financial-a7733171.html .

Sönmez, F. Ö., Hankin, C., & Malacaria, P. (2022). Decision support for healthcare cyber security. Computers & Security, 122, 102865.

Statista, 2022a, Worldwide Information Security Services Spending From 2017 To 2023, https://www.statista.com/statistics/217362/worldwide-it-security-spending/#:~:text=ın%202022%2c%20the%20security%20service,exceed%2076%20billion%20u.s.%20dollars

Statisca, 2022:Largest Fines Issued for General Data Protection Regulation (GDPR) Violations, https://www.statista.com/statistics/1133337/largest-fines-issued-gdpr/

Stoll, M., Felderer, M., & Breu, R. (2013). Information management for holistic, collaborative information security management. In Emerging Trends in Computing, Informatics, Systems Sciences, and Engineering (pp. 211-224). Springer New York.

Stankovic, J. A. (2016). Research directions for cyber physical systems in wireless and mobile healthcare. ACM Transactions on Cyber-Physical Systems, 1(1), 1-12.

Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). Information security policies in the UK healthcare sector: a critical evaluation. Information Systems Journal, 22(1), 77-94. https://doi.org/10.1111/j.1365-2575.2011.00378.x

Sveiby, K. E. (1997). The new organizational wealth: Managing & measuring knowledge-based assets. Berrett-Koehler Publishers.

Şen, Ş., & Yerlikaya, T. (2013). ISO 27001 Kurumsal Bilgi Güvenliği Standardı. MA, U. Çağlayan, E. Derman, A. Özgit, M. Topakcı, R. Uyar, O. Oral, Ş. Akbunar, TF Kasalak, E. Sezgin, F, Yücel, H. Akar, & U. Ercan (Eds.). XV. Akademik Bilişim Konferansı, 677, 681.

Offner, K. L., Sitnikova, E., Joiner, K., & MacIntyre, C. R. (2020). Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation. Intelligence and National Security, 35(4), 556-585.

Omri, N., Al Masry, Z., Mairot, N., Giampiccolo, S., & Zerhouni, N. (2021). X-PHM: Prognostics and health management knowledge-based framework for SME. Procedia CIRP, 104, 1595-1600.

Ossborne, C. Data Breach Forces Medical Debt Collector AMCA to File for Bankruptcy Protection, https://www.zdnet.com/article/medical-debt-collector-amca-files-for-bankruptcy-protection-after-data-breach/, erişim tarihi: 15.10.2022

Özaslan, G. (2019). Bilgi güvenliği ve mahremiyetin korunmasına yönelik eğitimin etkilerinin değerlendirilmesi: Bir özel hastane uygulaması (Doctoral dissertation, Marmara Universitesi (Turkey)).

Özdemir, A., Uluyol, Ç. (2021). Kamu kurum ve kuruluşlarında bilgi güvenliği farkındalığı. Türkiye Sosyal Araştırmalar Dergisi.25(3), 649-666.

Özbilgin, D., Mustafa, Ö. ISO 27001 Bilgi Güvenliği Yönetim Sistemi ve Ağ Yönetimi Politikası.

Öner, F. (2014). Sağlık Bilişimi, Türkiyede sağlık bilgi enformasyon sistemleri ve dijital hastaneler. Beykent Üniversitesi Sosyal Bilimler Enstitüsü İşletme Yönetimi Anabilim Dalı Hastane Ve Sağlık Kurumları Yönetimi Bilim Dalı.

Tonta, Y. (1999) Bilgi toplumu ve bilgi teknolojisi. Türk kütüphaneciliği. Https://Core.Ac.Uk/Download/Pdf/11881658.Pdf. Erişim Tarihi 19.10.2022

Tuygun, M. (2019). Iso27001 Bilgi Güvenliği Yönetim Sistemi Standardının Kamu Kurumlarına Uygulanabilirliğinin Araştırılması: Ankara İli Örneği. Gazi Üniversitesi Bilişim Sistemleri Anabilim Dalı Yüksek Lisans Tezi Haziran. 2019

Yıldız, R. (2022). ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri Gereksinimlerinin Veri Tabanı Sistemlerinde Uygulanması. Gazi Üniversitesi Bilişim Sistemleri Anabilim Dalı Yüksek Lisans Tezi. 2022.

Yılmaz, H. (2014) TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması Ve Bilgi Güvenliği Risk Analizi. KİDDER Kamu İç Denetçileri Derneği.15.1: 45-59.

Yılmaz, H. (2014). TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması Ve Bilgi Güvenliği Risk Analizi. KİDDER Kamu İç Denetçileri Derneği. 15.1: 45-59.

Yıldırım, E., Y, Akalp, G., Aytac, S., Bayram, N. (2011). Factors Influencing Information Security Management in Small-And Medium-Sized Enterprises: A Case Study From Turkey. International Journal Of Information Management. 31(4), 360-365. DOI:10.1016/j.ijinfomgt.2010.10.006

Yusof, M. M., Kuljis, J., Papazafeiropoulou, A., & Stergioulas, L. K. (2008). An evaluation framework for Health Information Systems: human, organization and technology-fit factors (HOT-fit). International journal of medical informatics, 77(6), 386-398.

Vaishnav, R., Panditi, M. D. D., Dhiman, V., Aarthy, C. C. J., Kumari, Y. S., & Mohiddin, M. K. (2022). Data security in healthcare management analysis and future prospects. Materials Today: Proceedings, 51, 2202-2206. https://doi.org/10.1016/j.matpr.2021.11.280

Verizon, 2022 Data Breach Investigations Report https://www.verizon.com/business/resources/reports/dbir/2022/master-guide/, 2022, erişim tarihi: 10.12.2022

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. The journal of strategic information systems, 28(2), 118-144, ISSN 0963-8687,

Von Solms, B. (2001) Information Security—A Multidimensional Discipline. Computers & Security, 20, 504-508.https://doi.org/10.1016/S0167-4048(01)00608-3

Von Solms, R. (1999). Information security management: why standards are important. Information Management & Computer Security, 7(1), 50-58. https://doi.org/10.1108/09685229910255223

Vora, J., Italiya, P., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., & Hsiao, K. F. (2018, July). Ensuring privacy and security in e-health records. In 2018 International conference on computer, information and telecommunication systems (CITS) (pp. 1-5). IEEE.Doi:10.1109/Cits.2018.8440164

Vroom, C., Solms, V. (2004). R. Towards Information Security Behavioural Compliance. Computers & Security.23(3), 191-198.

Qader, A. A., Zhang, J., Ashraf, S. F., Syed, N., Omhand, K., & Nazir, M. (2022). Capabilities and opportunities: Linking knowledge management practices of textile-based SMEs on sustainable entrepreneurship and organizational performance in China. Sustainability, 14(4), 2219.Https://Doi.Org/10.3390/Su14042219

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. Computers & Security, 55, 81-99.

Zhang, Z. K., Cho, M. C. Y., Wang, C. W., Hsu, C. W., Chen, C. K., & Shieh, S. (2014, November). IoT security: ongoing challenges and research opportunities. In 2014 IEEE 7th international conference on service-oriented computing and applications (pp. 230-234). IEEE.

Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). Frontiers in Digital Health, 135.

Wegen, B. V., & Hoog, R. D. (1996). Measuring the economic value of information systems. Journal of Information Technology, 11(3), 247-260

White Paper Healthcare, I. T. Health Information at Risk: Successful Strategies for Healthcare Security And Privacy., 2011, https://www.intel.eu/content/dam/www/public/us/en/documents/white-papers/strategies-for-healthcare-security-and-privacy-paper.pdf. Erişim Tarihi: 09.10.2022

WHO, 2021a, World Health Organisation (WHO) on Primary Health Care. Available Online: https://www.who.int/docs/default-source/primary-health-care-conference/digital-technologies.pdf?sfvrsn=3efc47e0_2. (accessed on 16 july 2021)

WHO, 2021b, World Health Organisation (WHO), Global Strategy on Digital Health 2020-2025, https://apps.who.int/iris/bitstream/handle/10665/344249/9789240020924-eng.pdf

WHO, Overview, Https://Www.Who.int/Activities/Integrating-Rehabilitation-into-Health-Systems/Information

Wolff, J., & Lehr, W. (2017). Degrees of ignorance about the costs of data breaches: What policymakers can and can't do about the lack of good empirical data. Available at SSRN 2943867.

8.EKLER

EK-1 Etik Kurul İzni

T.C.

NECMETTİN ERBAKAN ÜNİVERSİTESİ

SAĞLIK BİLİMLERİ BİLİMSEL ARAŞTIRMALAR ETİK KURULU

Sayı : 13-74 01.09.2021

Sayın Doç. Dr. Yusuf Yalçın İLERİ

Sorumlu araştırmacı olarak yürüteceğiniz "ISO/IEC 27001 Kapsamında Bilgi Güvenliği Yönetim Farkındalığının Değerlendirilmesi: Ankara İli Sağlık Kurumları Bilgi İşlem Birimi Çalışanları Örneği" başlıklı proje ile ilgili kurulumuza yaptığınız etik kurul başvurusu görüşüldü. Kurulumuzun 01.09.2021 tarih ve 2021/13-74 sayılı kararıyla, çalışmanın bilimsel etik açıdan uygun olduğuna karar verildi.

Not: Çalışma ile ilgili gerekli izin ve yasal sorumluluk araştırmacıya aittir.
Yardımcı Araştırmacılar : Yükseklisans Öğrencisi Hadis SOSYAL

EK-2 Kurum İzinleri

ANKARA İL SAĞLIK MÜDÜRLÜĞÜ - ANKARA EĞİTİM VE TESCİL BİRİMİ
31/01/2022 17:14 - E-90739940 - 799 - 193
00157942208

T.C.
ANKARA VALİLİĞİ
İl Sağlık Müdürlüğü

Sayı : E-90739940-799
Konu : Hadis SOYSAL
(Tez Çalışması)

DESTEK HİZMETLERİ BAŞKANLIĞINA

İlgi a) 11/11/2021 tarih ve 152109768 barkodlu yazınız.
b) 12/11/2021 tarih ve 152172259 barkodlu yazımız.

İlgi (a)'da kayıtlı yazı ile Başkanlığı'nızda çalışan ve Necmettin Erbakan Üniversitesi Sağlık Yönetimi anabilim dalı yüksek lisans öğrencisi Hadis SOYSAL'ın "ISO/IEC 27001 Kapsamında Bilgi Güvenliği Yönetim Farkındalığının Değerlendirilmesi Ankara İli Sağlık Kurumları Bilgi İşlem Birimi Çalışanları" konulu tez çalışmasını Müdürlüğümüz Bilgi İşlem Birimi koordinasyonunda ekli listedeki hastanelerde bilgi işlemden sorumlu yöneticiler ile bilgi işlem biriminde çalışan teknik personel için akademi.asm.gov.tr üzerinden online olarak yapılmasına yönelik gerekli izin talebi yazısı ilgili hastanelere ilgi(b)'de kayıtlı yazı ile gönderilmiştir.

Söz konusu çalışma sonucunun Bakanlığımızın bilgisi dışında ilan edilmemesi, başka bir amaçla kullanılmaması, başka makam ve kişilere verilmemesi ve bir örneğinin Müdürlüğümüze gönderilmesi kaydıyla, ilgili kurumda yapılması hususunda, ilgili Hastane Yöneticilikleri'nin cevabi yazısı ekte gönderilmektedir.

Bilgilerinizi ve gereğini arz ederim.

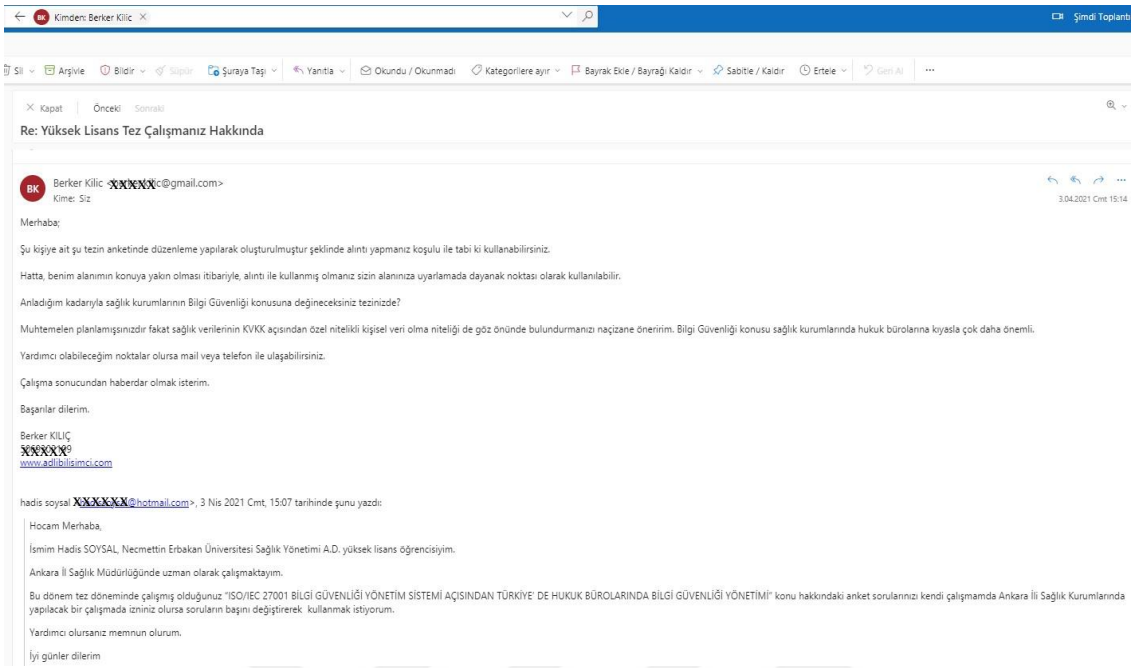
Doç. Dr. Özgür Ömer YILDIZ
Başkan Yardımcısı

Ek: Yazı (27 sayfa)

Bu belge, güvenli elektronik imza ile imzalanmıştır.
Belge Doğrulama Kodu: a9ff2a76-bba2-4d01-8c0a-71e10705399ff Belge Doğrulama Adresi: https://www.turkiye.gov.tr/saglik-bakanligi-ebys

Emrah Mahallesi Gülhane Kampüsü NO:87 Keçiören ANKARA
Bilgi için: Elif AL
Telefon: Faks No:
DİYETİSYEN
e-Posta: elif.uyar@saglik.gov.tr İnternet Adresi: Sağlık Hizmetleri Başkanlığı Eğitim ve Tescil Birimi
Telefon No: (0 312) 306 36 22

EK -3 Anket Kullanım İzni



Kimden: Berker Kilic

Şimdi Toplantı

Sil | Arşivle | Bildir | Süpür | Şuraya Taşı | Yanıtla | Okundu / Okunmadı | Kategorilere ayır | Bayrak Ekle / Bayrağı Kaldır | Sabitle / Kaldır | Ertele | Geri Al | ...

Kapat | Önceki | Sonraki

Re: Yüksek Lisans Tez Çalışmanız Hakkında

BK Berker Kilic <XXXXXic@gmail.com>
Kime: Siz
3.04.2021 Cmt 15:14

Merhaba;

Şu kişiye ait şu tezin anketinde düzenleme yapılarak oluşturulmuştur şeklinde alıntı yapmanız koşulu ile tabi ki kullanabilirsiniz.

Hatta, benim alanımın konuya yakın olması itibariyle, alıntı ile kullanmış olmanız sizin alanınıza uyarlamada dayanak noktası olarak kullanılabilir.

Anladığım kadarıyla sağlık kurumlarının Bilgi Güvenliği konusuna değineceksiniz tezinizde?

Muhtemelen planlamışsınızdır fakat sağlık verilerinin KVKK açısından özel nitelikli kişisel veri olma niteliği de göz önünde bulundurmanızı naçizane öneririm. Bilgi Güvenliği konusu sağlık kurumlarında hukuk bürolarına kıyasla çok daha önemli.

Yardımcı olabileceğim noktalar olursa mail veya telefon ile ulaşabilirsiniz.

Çalışma sonucundan haberdar olmak isterim.

Başarılar dilerim.

Berker KILIÇ
XXXXX9
www.adlibilisimci.com

hadis soysal XXXXXX@hotmail.com>, 3 Nis 2021 Cmt, 15:07 tarihinde şunu yazdı:

> Hocam Merhaba,
>
> İsmim Hadis SOYSAL, Necmettin Erbakan Üniversitesi Sağlık Yönetimi A.D. yüksek lisans öğrencisiyim.
>
> Ankara İl Sağlık Müdürlüğünde uzman olarak çalışmaktayım.
>
> Bu dönem tez döneminde çalışmış olduğunuz "ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ AÇISINDAN TÜRKİYE' DE HUKUK BÜROLARINDA BİLGİ GÜVENLİĞİ YÖNETİMİ" konu hakkındaki anket sorularınızı kendi çalışmamda Ankara İli Sağlık Kurumlarında yapılacak bir çalışmada izniniz olursa soruların başını değiştirerek kullanmak istiyorum.
>
> Yardımcı olursanız memnun olurum.
>
> İyi günler dilerim

EK-4. Anket Formu

ANKET FORMU

Bilgi güvenliği sağlık hizmeti veren kurumlar açısından büyük önem taşımaktadır. Bu araştırmaya katılmayı kabul ederseniz bilgi güvenliğine yönelik anket sorularını cevaplamanız istenecektir. Necmettin Erbakan Üniversitesi Sağlık Bilimleri Enstitüsü ve Ankara İl Sağlık Müdürlüğü onayı ile gerçekleştirilen bu çalışma bir bilimsel araştırma niteliğinde olup size ait olan bilgiler araştırma grubu dışındaki kişilerle paylaşılmayacaktır.

Çalışma Doç. Dr. Yusuf Yalçın İLERİ'nin danışmanlığında yüksek lisans öğrencisi ve Ankara İl Sağlık Müdürlüğü kurum personeli Hadis SOYSAL tarafından yürütülmektedir. (İletişim: xxxxxxxxx@saglik.gov.tr)

Çalışmanın amacına ulaşması sizlerin değerli katılımlarına bağlıdır. Bu nedenle soruları dikkatli okumanız ve cevaplamanız büyük önem taşımaktadır.

BÖLÜM -1-Kişisel Bilgiler

1. Çalışmakta Olduğunuz Sağlık Kuruluşu:……..

2. Çalışmakta olduğunuz Birim:…….....

3. En son mezun olduğunuz okul: ( )Lise ( )Yüksekokul

( )Lisans ( )Yüksek Lisans ve üzeri

4. Ünvanınız:……

5. Yaşınız: [ ] 18-25 [ ] 26-33 [ ] 34-41

[ ] 42-49 [ ] 50 -57 [ ] 58-65

6. Cinsiyetiniz: ( )Erkek ( )Kadın

7. Medeni haliniz: ( )Evli ( )Evli Değil

8. Aylık geliriniz: ( )4000 TL ve altı ( )4001-6000 TL

( )6001-8000 TL ( )8001 TL ve üstü

9. Kurumda çalışma süreniz: ( ) 0-1 yıl arası ( ) 1-5 yıl arası ( ) 5-10 yıl arası

( ) 10-15 yıl arası ( ) 15-20 yıl arası ( ) 20 yıl ve üzeri

BÖLÜM 2: BİLGİ GÜVENLİĞİ POLİTİKALARI

	EVET	HAYIR	KISMEN
1.Çalıştığınız sağlık tesisinde yönetimi tarafından bilgi güvenliği konusunda yasal düzenlemelerle uyumlu, paydaşlara yönelik yazılı bir yönlendirme/bilgilendirme yapıldı mı?			
2. Bilgi güvenliği politika dokümanı hazırlandı mı?			
3. Bilgi güvenliği politika dokümanı yönetim tarafından onaylandı mı?			
4. Bilgi güvenliği yönetim politika dokümanı çalışanlara ve paydaşlara bildirildi mi?			
5. Bilgi güvenliği yönetim politika dokümanı belirli aralıklarla uygunluğu ve doğruluğu açısından gözden geçiriliyor mu?			

BÖLÜM 3: BİLGİ GÜVENLİĞİ ORGANİZASYONU

	EVET	HAYIR	KISMEN
1. Çalıştığınız sağlık tesisinde yerine getirilmesinde, bilgi güvenliği sorumluları belirlenerek bilgi güvenliği kapsamında, ilgili kamu kurumları ve STK' lar gibi taraflarla bilgi alışverişinde bulunuldu mu?			
2. Çalıştığınız sağlık tesisinde bilgi güvenliği sorumlulukları tanımlandı mı?			
3. Çalıştığınız sağlık tesisinde bilgi güvenliği rollerinin tahsisinde görevler ve sorumluluklar arasındaki çelişkiler giderildi mi?			
4. Çalıştığınız sağlık tesisinde bilgi güvenliği ile ilgili yetkilendirilmemiş görevler temizlendi veya gereksiz yetkilendirmeler giderildi mi?			
5. Çalıştığınız sağlık tesisinde bilgi güvenliği kapsamında değerlendirilmesinde müdürlük veya bakanlıkla iletişim kuruldu mu?			
6. Çalıştığınız sağlık tesisinde bilgi güvenliği kapsamında değerlendirilmesinde özel ilgi grupları veya derneklerle iletişim kuruldu mu?			
7. Çalıştığınız sağlık tesisinde bilgi güvenliği kapsamında değerlendirilmesinde profesyonel yardım alındı mı?			
8. Çalıştığınız sağlık tesisinde hizmetler sunulurken, hizmetin türüne bakılmaksızın bilgi güvenliğine dikkat ediliyor mu?			
9.Çalıştığınız sağlık tesisinde personelin, mevcut ağ sistemine kişisel bilgisayarı, mobil cihazları gibi araç gereçlerle bağlanmasında belirlenmiş kurallar/standartlar mevcut mu?			
10. Çalıştığınız sağlık tesisinde personelin, kendi mobil cihazlarını ağ sistemine bağlanması nedeniyle ortaya çıkabilecek risklere karşı alınan güvenlik tedbirleri mevcut mu?			

BÖLÜM 4: İNSAN KAYNAKLARI GÜVENLİĞİ

	EVET	HAYIR	KISMEN
1. Çalıştığınız sağlık tesisinde çalışanları ile yapılan sözleşmelerde, kişilere bilgi güvenliği sorumlulukları bildiriliyor mu?			
2. Çalıştığınız sağlık tesisindenun mal ve hizmet aldığı kişi ve kurumlara, bilgi güvenliği sorumlulukları bildiriliyor mu?			
3. Çalıştığınız sağlık tesis personeli görevi gereği hizmetlerin yerine getirilmesinde bilgi güvenliği prosedürlerine uymamaları durumunda karşılaşacakları sorumluluklar hakkında yazılı olarak bilgilendiriliyor mu?			
4. Çalıştığınız sağlık tesis personeline bilgi güvenliği prosedürleri ile ilgili bir iç eğitim verildi mi?			
5. Çalıştığınız sağlık tesis personeline bilgi güvenliği konusunda bir dış eğitim alması sağlandı mı?			
6. Çalıştığınız sağlık tesisi personeline yönelik bilgi güvenliği prosedürlerini ihlal etmeleri durumunda uygulanacak bildirilmiş bir yaptırım mevcut mu?			
7. Çalıştığınız sağlık tesisi mal ve hizmet satın aldığı kişi ve kurumlara yönelik bilgi güvenliği prosedürlerini ihlal etmeleri durumunda uygulanacak kendilerine bildirilmiş bir yaptırım mevcut mu?			
8. Çalışanların işten çıkarılması veya ürün/hizmet alınan yüklenicilerle çalışmanın sonlandırılması durumunda, sonrasında ortaya çıkabilecek olası bilgi güvenliği zaafiyetlerine karşı tedbirler alınıyor mu?			
9. Çalıştığınız sağlık tesisinde çalışanların işten ayrılmaları veya görevlerinin değişmesi durumunda bilgi güvenliği sorumluluklarının devam ettiğine ilişkin bilgilendirme yapılıyor mu?			
10. Çalıştığınız sağlık tesisinden mal ve hizmet aldığı kişi ve kurumlara, çalışmalarının sonlandırılması veya değişmesi durumunda bilgi güvenliğine ilişkin sorumluluklarının devam ettiğine ilişkin bilgilendirme yapılıyor mu?			

BÖLÜM 5: VARLIK YÖNETİMİ

	EVET	HAYIR	KISMEN
1.Çalıştığınız sağlık tesisinde hizmetlerinde kullanılan bilişim teknolojileri ekipmanına ait durum ve sahiplikleri de kapsayan bir envanter çalışması yapıldı mı?			
2. Çalıştığınız sağlık tesis hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarının tamamı kayıt altında tutuluyor mu?			
3. Çalıştığınız sağlık tesis hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarının tamamının kullanımına dair belirlenmiş kurallar var mı?			
4. Çalıştığınız sağlık tesis personelin işten ayrılmaları durumunda, sağlık tesisi tarafından kendilerine sağlanan bilgi işlem ekipmanlarını ne şekilde iade edeceklerine ilişkin belirlenmiş kurallar mevcut mu?			
5.Çalıştığınız sağlık tesisinde yerine getirilmesinde ihtiyaç duyulan veya Çalıştığınız sağlık tesisinde gerçekleştirilmesi esnasında üretilen dijital bilginin sınıflandırılması, etiketlenmesi ve korunmasına ilişkin yöntemler/standartlar mevcut mu?			
6. Çalıştığınız sağlık tesisinde yerine getirilmesinde ihtiyaç duyulan veya sağlık tesisinde gerçekleştirilmesi esnasında üretilen dijital bilgi yasal şartlara göre sınıflandırılıyor mu?			
7. Çalıştığınız sağlık tesisinde yerine getirilmesinde ihtiyaç duyulan veya sağlık tesisinde gerçekleştirilmesi esnasında üretilen dijital *bilgi değerine/kritikliğine* göre sınıflandırılıyor mu?			
8. Çalıştığınız sağlık tesisinde yerine getirilmesinde ihtiyaç duyulan veya sağlık tesisinde gerçekleştirilmesi esnasında üretilen dijital bilgi yetkisiz ifşa edilebilirliğine göre sınıflandırılıyor mu?			
9. Çalıştığınız sağlık tesisinde yerine getirilmesinde ihtiyaç duyulan veya sağlık tesisinde gerçekleştirilmesi esnasında üretilen dijital değiştirilmeye karşı hassasiyetine göre sınıflandırılıyor mu?			
10. Çalıştığınız sağlık tesisinde yerine getirilmesinde ihtiyaç duyulan veya sağlık tesisinde gerçekleştirilmesi esnasında üretilen dijital bilginin sınıflandırılmasına ilişkin kullanılan belirli bir prosedür mevcut mu?			
11. Çalıştığınız sağlık tesisinde yerine getirilmesinde ihtiyaç duyulan veya sağlık tesisinde gerçekleştirilmesi esnasında üretilen dijital bilginin kullanımına ilişkin sınıflandırma düzeni ile örtüşen bir etiketleme sistemi mevcut mu?			
12.Çalıştığınız sağlık tesisinde yerine getirilmesinde, depolanmış dijital bilgiyi koruma, bilgiye erişim, bilgiyi güncelleme, bilgiyi silme, bilgiyi yok etme işlemlerine ilişkin standartlar mevcut mu?			
13. Çalıştığınız sağlık tesisinde yerine getirilmesinde veya üretilen dijital bilginin depolama birimlerine kaydedilirken bilgi sınıflandırma prosedürlerine uyuluyor mu?			
14. Çalıştığınız sağlık tesisinde yerine getirilmesinde veya üretilen dijital bilginin geçmişte depolanmış olduğu birimler güvenli bir şekilde yok ediliyor mu?			
15. Çalıştığınız sağlık tesisinde yerine getirilmesinde veya üretilen dijital bilginin depolama birimlerine kaydedilirken yetkisiz erişime karşı tedbir alınıyor mu?			
16. Çalıştığınız sağlık tesisinde yerine getirilmesinde veya üretilen dijital bilgi depolama birimlerine kaydedilirken kötüye kullanıma karşı tedbir alınıyor mu?			
17. Çalıştığınız sağlık tesisinde yerine veya üretilen dijital bilgi depolama birimlerine kaydedilirken bozulmaya karşı tedbir alınıyor mu?			

BÖLÜM 6: ERİŞİM KONTROLÜ

	EVET	HAYIR	KISMEN
1.Çalıştığınız sağlık tesisinde hizmetlerin yerine getiren ağ kullanıcılarının yaptıkları iş çerçevesinde ağ hizmetlerine erişimlerini düzenleyici kurallar/standartlar mevcut mudur?			
2. Çalıştığınız sağlık tesisinde kullanıcılar için iş ve bilgi güvenliği temelinde hazırlanmış yazılı bir erişim kontrol politikası mevcut mu?			
3. Çalıştığınız sağlık tesisisinde kullanılar için ağ kullanıcılarının yönetimi için tanımlanmış yetkiler doğrultusunda kullanıcı erişim politikaları uygulanıyor mu?			
4. Çalıştığınız sağlık tesisisinde ağ kullanıcıları için gerekli durumlarda verilen ayrıcalıklı yetkilerin tahsis edilmesi, kısıtlanması ve kontrolü gerçekleştiriliyor mu?			
5. Çalıştığınız sağlık tesisinde hizmetlerini yerine getiren ağ kullanıcılarının, ağ kaynakları üzerindeki haklarının belirlenmesi ve hak atamalarının yapılması konularında yazılı standartlar mevcut mu?			
6. Çalıştığınız sağlık tesisi hizmetlerini yerine getirmede sistemler ve hizmetlere erişim hakları verilirken uyulacak kullanıcı erişim kuralları mevcut mu?			
7. Çalıştığınız sağlık tesis hizmetlerini yerine getiren kullanıcılara verilen erişim haklarının tahsisi ve kısıtlanması düzenli olarak kontrol ediliyor mu?			
8. Çalıştığınız sağlık tesis hizmetlerinde kullanılan bilişim teknolojileri ekipmanlarına erişim hakları düzenli aralıklarla gözden geçiriliyor mu?			
9. Çalıştığınız sağlık tesis hizmetlerini yerine getiren çalışanların ve mal/hizmet alınan dış tarafların sahip olduğu bilgi işleme olanaklarına erişim yetkileri sözleşmeleri/anlaşmaları sona erdiğinde kaldırılıyor mu?			
10.Çalıştığınız sağlık tesisinde hizmetlerini yerine getiren kullanıcılar, sahip oldukları erişim ve kullanım kimliklerini korumaları konusunda bilgilendirildi mi?			
11. Çalıştığınız sağlık tesisi hizmetlerini yerine getiren çalışanların, bilgi işleme olanaklarına erişmede kullandıkları gizli kimlik doğrulama bilgilerini kullanmalarında uymaları gereken kurallar mevcut mu?			
12. Çalıştığınız sağlık tesisi hizmetlerini yerine getiren çalışanların, bilgi işleme olanaklarına kullanımda kullandıkları gizli kimlik doğrulama bilgilerini kullanmalarında uymaları gereken kurallar mevcut mu?			
13.Çalıştığınız sağlık tesisinde çalışanları tarafından kullanılan sistem açılış, bağlantı ve uygulama şifreleri kullanıcının ihtiyacı olan yetkilerle orantılı olarak seviyelendirirdi mi?			
14. Çalıştığınız sağlık tesis hizmetlerinde kullanılan bilgi işleme olanaklarının kullanımı, erişim kontrol kuralları ile kısıtlanıyor mu?			
15. Çalıştığınız sağlık tesis hizmetlerinde kullanılan bilgi işleme olanaklarına erişim esnasında, şart koşulan durumlarda güvenli oturum açma kontrolleri mevcut mu?			
16. Çalıştığınız sağlık tesis hizmetlerinde kullanılan bilgi işleme olanaklarına erişmede kullanılan parola yönetim sistemi güvenilir parolalar kullanmayı zorunlu hale getiriyor mu?			

BÖLÜM 7: KRİPTOGRAFİ

	EVET	HAYIR	KISMEN
1. Çalıştığınız sağlık tesisinde yerine getirilmesinde kullanılan ve bu hizmetler sonrasında üretilen bilginin gizliliği, bilginin aslına uygunluğu ve bilginin bütünlüğünü sağlama amacı ile şifreleme işlemlerinden faydalanılıyor mu?			
2. Çalıştığınız sağlık tesisi şifrelenmesinde kullanılan kriptografik anahtarların kullanımına ilişkin kurallar mevcut mu?			
3. Çalıştığınız sağlık tesisi şifrelenmesinde kullanılan kriptografik anahtarların yaşam sürelerine ilişkin kurallar mevcut mu?			

BÖLÜM 8: FİZİKSEL VE ÇEVRESEL GÜVENLİK

	EVET	HAYIR	KISMEN
1. Çalıştığınız sağlık tesis ortamında fiziksel ve elektronik sistemler (kamera ve alarm sistemleri gibi) ile yetkisiz erişimlere karşı koruma tedbirleri mevcut mudur?			
2. Çalıştığınız sağlık tesis ortamında hassas ve kritik bilgilerin bulunduğu ortamlar genel kullanıma açık alanlardan ayrılmış mı?			
3. Çalıştığınız sağlık tesis ortamında hassas ve kritik bilgilerin bulunduğu ortamlara genel kullanıma açık alanlardan geçişte kullanılan güvenlik kontrolleri belirlenmiş mi?			
4. Çalıştığınız sağlık tesis ortamının ve çevresinin fiziksel güvenliğini sağlamak için bir güvenlik tasarımı yapıldı mı?			
5. Çalıştığınız sağlık tesis ortamında genel kullanıma açık olmayan alanlarda çalışanlar için tanımlanmış iş süreçleri mevcut mu?			
6. Yetkisiz kişilerin çalıştığınız sağlık tesisinde bulunabildiği sekreterlik, bekleme alanları benzeri alanlarda güvenlik zaafiyetlerine karşı kontrol ediliyor mu?			
7.Çalıştığınız sağlık tesisinde hizmetlerinde kullanılan bilişim teknolojileri varlıklarının kaybedilmesi, hasar görmesi, çalınması veya ele geçirilmesi gibi durumlara karşı, Çalıştığınız sağlık tesisinde sürekliliğini sağlamaya yönelik tedbirler mevcut mu?			
8. Çalıştığınız sağlık tesis hizmetlerinde kullanılan bilişim teknolojileri araçları çevresel tehditlerden kaynaklanan riskleri azaltacak şekilde konumlandırıldı mı?			
9. Çalıştığınız sağlık tesis hizmetlerinde kullanılan bilişim teknolojileri araçları yetkisiz erişim fırsatlarından kaynaklanan riskleri azaltacak şekilde konumlandırıldı mı?			
10. Çalıştığınız sağlık tesis hizmetlerinde kullanılan bilişim teknolojileri araçlarını destekleyici altyapı sebepli enerji kesintilerine karşı tedbirler alındı mı?			
11. Çalıştığınız sağlık tesis hizmetlerinde kullanılan bilişim teknolojileri araçlarını destekleyici ağ alt yapısı sebepli Internet bağlantı kesintilerine karşı tedbirler alındı mı?			
12. Çalıştığınız sağlık tesisi hizmetlerinde kullanılan, depolama ortamı içeren bilişim teknolojileri araçlarının yok edilecek olması durumunda kayıtlı hassas bilgilerin ve lisanslı yazılımların kaldırılmasına ilişkin belirlenmiş kurallara uyuluyor mu?			
13. Çalıştığınız sağlık tesisi hizmetlerinde artık ihtiyaç duyulmayan ve sahipliği olmayan bilişim teknolojileri ekipmanının korunması için alınmış tedbirler mevcut mu?			
14. Çalıştığınız sağlık tesisi hizmetlerinde kağıt ve taşınabilir depolama ortamlarının düzenli olmasını sağlamak üzere temiz masa politikası uygulanıyor mu?			

BÖLÜM 9: İŞLEM GÜVENLİĞİ

	EVET	HAYIR	KISMEN
1. Çalıştığınız sağlık tesis hizmetlerinde bilişim sistemleri ekipmanları aracılığı ile yerine getirilen işlemler yazılı hale getirildi mi?			
2. Çalıştığınız sağlık tesisinde doğru ve güvenli şekilde gerçekleştirilmesine yönelik ilgili iş süreçleri ve bilgi işleme olanakları hakkında çalışanlara yazılı bilgilendirme yapıldı mı?			
3. Çalıştığınız sağlık tesis hizmetlerinde kullanılan bilişim sistemleri ekipmanlarında bilgi güvenliğini etkileyen yeni kurulum işlemleri kontrol ediliyor mu?			
4. Çalıştığınız sağlık tesis hizmetlerinde veri girişi, veri işleme, depolama, yedekleme, arşivleme yetkisiz erişim veya bilişim sistemleri ekipmanlarındaki değişiklik risklerinin azaltılması için birbirinden ayrıldı mı?			
5. Çalıştığınız sağlık tesis hizmetlerinde kullanılan bilişim sistemleri ekipmanlarını kötücül yazılımlardan korunması için tedbirler alınıyor mu?			
6. Çalıştığınız sağlık tesis hizmetlerinde kullanılan veya hizmetler esnasında üretilen bilginin yedeklemesi yapılıyor mu?			
7. Çalıştığınız sağlık tesis hizmetlerinde kullanılan veya hizmetler esnasında üretlen bilginin yedekleri harici bir bilişim sistemi ekipmanı üzerinde mi yapılıyor?			
8. Çalıştığınız sağlık tesis hizmetlerinde kullanılan veya hizmetler esnasında üretilen bilginin yedekleri düzenli olarak test ediliyor mu?			
9. Çalıştığınız sağlık tesis hizmetlerinde kullanılan bilişim sistemleri ekipmanlarının düzenli olarak sistem yedekleri (imajları) alınıyor mu?			
10. Yedekleme işlemleri için çalışanlara duyurulmuş yedekleme kuralları mevcut mu?			
11. Çalıştığınız sağlık tesisinde yerine getirilmesi esnasında bilişim sistemleri ekipmanları üzerindeki kullanıcı işlemleri olay aktiviteleri kaydediliyor ve düzenli olarak gözden geçiriliyor mu?			
12. Çalıştığınız sağlık tesisinde yerine getirilmesi esnasında bilişim sistemleri ekipmanları üzerindeki bilgi güvenliği aktiviteleri kaydediliyor ve düzenli olarak gözden geçiriliyor mu?			
13. Çalıştığınız sağlık tesisinde hizmetlerinde kullanılan bilişim teknolojileri ekipmanları ve ağ alt yapısınına yapılacak yazılımsal eklemeler (yazılım güncellemeleri ve yamaları gibi) için bir kurulum kontrolü standardı mevcut mu?			
14.Çalıştığınız sağlık tesisinde hizmetlerinde kullanılan bilişim teknolojileri varlıklarında olası teknik zaafiyetlere karşı tespit ve tedbir alma kapsamında uygulanan standartlar mevcut mu?			
15. Çalıştığınız sağlık tesisinde yerine getirilmesinde kullanılan bilişim teknolojileri ekipmanlarının teknik açıklıkları nedeniyle ne tür zaafiyetlerin ortaya çıkabileceği biliniyor mu?			
16. Çalıştığınız sağlık tesisinde yerine getirilmesinde kullanılan bilişim teknolojileri ekipmanlarının teknik açıklıklarına karşı tedbirler alınıyor mu?			
17. Çalıştığınız sağlık tesisinde yerine getirilmesinde kullanılan bilişim teknolojileri ekipmanlarına kullanıcıları tarafından yazılım kurulumuna dair oluşturulmuş kurallar mevcut mu?			
18.Çalıştığınız sağlık tesisinde hizmetlerinde kullanılan bilişim teknolojileri varlıkları üzerinde yapılan bilişim güvenliğine yönelik çalışmalar, hizmetlerin yavaşlamasına veya aksamasına sebep olacak nitelikte mi?			
19. Çalıştığınız sağlık tesisinde hizmetlerinde kullanılan bilişim teknolojileri ekipmanları üzerinde zorunlu olarak gerçekleştirilen donanımsal ve yazılımsal tetkik işlemlerinin sağlık tesis hizmetlerinde asgari kesintiye neden olacak çekilde planlanması yapılıyor mu?			

BÖLÜM 10: HABERLEŞME GÜVENLİĞİ

	EVET	HAYIR	KISMEN
1.Çalıştığınız sağlık tesisinde hizmetlerinde kullanılan ağ alt yapısında olası teknik zaafiyetlere karşı tespit ve tedbir alma kapsamında uygulanan standartlar mevcut mu?			
2. Çalıştığınız sağlık tesisinde hizmetlerinde kullanılan veya hizmetler sonrasında ortaya çıkan veriyi korumak amacı ile birden fazla alt ağ kurulumu yapıldı mı?			
3. Çalıştığınız sağlık tesisinde hizmetlerinde kullanılan ağ alt yapısının güvenliğinin tesisi amacı ile belirlenmiş yetkin bir ağ sorumlusu var mı?			
4. Çalıştığınız sağlık tesisinde hizmetlerinde kullanılan ağ alt yapısının güvenliğinin tesisi amacı ile yetkin bir kişi/kurumdan hizmet alımı gerçekleştiriliyor mu?			
5. Çalıştığınız sağlık tesisinde hizmetlerinde kullanılan veya hizmetleri neticesinde üretilen bilginin sağlık tesisi dışına çeşitli yollarla transferinde uyulması gereken güvenlikkuralları mevcut mu?			
6. Çalıştığınız sağlık tesis hizmetlerinde mal/hizmet alınan firmalar, hizmetlerinde kullanılan veya hizmetleri sonrasında ortaya çıkarılan bilgileri ifşa etmemeleri konusunda yazılı bir sözleşme ile bağlayıcı hale getiriliyor mu?			

BÖLÜM 11: SİSTEM TEMİNİ, GELİŞTİRME VE BAKIMI

1. Çalıştığınız sağlık tesisinde hizmetleri içerisinde kullanıcıların aldatılarak veya teknik zaafiyetlerin kullanılması ile ortaya çıkabilecek saldırılara karşı bilgi güvenliği tedbirleri alınıyor mu?	EVET	HAYIR	KISMEN
2. Çalıştığınız sağlık tesisinde hizmetlerinde kullanılan veya hizmetleri sonrasında üretilen bilgiyi, ağ üzerinde transfer edilirken yanlış yönlendirmeye ve kopyalamaya karşı korumak için tedbirler alınıyor mu?			
3.Çalıştığınız sağlık tesisinde gerçekleştirilmesi süreçleri içerisinde entegre bir bilgi güvenliği yaşam döngüsü belirlenmiş veuygulanıyor mu?			
4. Çalıştığınız sağlık tesisinde gerçekleştirilmesinde uygulanan bilgi güvenliği yaşam döngüsü çalışanları kapsıyor mu?			
5. Çalıştığınız sağlık tesisinde gerçekleştirilmesinde uygulanan bilgi güvenliği yaşam döngüsü bilişim teknolojileri ekipmanını kapsıyor mu?			
6. Çalıştığınız sağlık tesis hizmetlerinde kullanılan bilişim sistemlerinde yapılan değişiklikler için belirlenmiş kurallar mevcut mu?			
7. Çalıştığınız sağlık tesisinde yerine getirilmesinde kullanılan kritik uygulamaların güncellemeler sonrasında mevcut bilişim sistemleri ile uyumluluğu test edildi mi?			
8. Çalıştığınız sağlık tesisinde gerçekleştirilmesinde, donanımsal ve yazılımsal değişiklikleri sonrasında belirlenmiş bir kabul prosedürü uygulanıyor mu?			
9. Çalıştığınız sağlık tesisinde gerçekleştirilmesinde, donanımsal ve yazılımsal değişiklikleri sonrasında sistem güvenliği testleri için belirlenmiş test süreçleri mevcut mu?			
10.Çalıştığınız sağlık tesisinde hizmetleri iş süreçleri içerisinde, bilgi güvenliği zaafiyetlerinin tespitine yönelik test/tatbikat çalışması yapıldı mı?			
11. Çalıştığınız sağlık tesisinde gerçekleştirilmesinde, donanımsal/yazılımsal değişiklikler ve bakım/onarım hizmeti sonrasında sistem güvenliği testlerinde kullanılan test verisi düzenli olarak kontrol ediliyor mu?			

BÖLÜM 12: TEDARİKÇİ İLİŞKİLERİ

	EVET	HAYIR	KISMEN
1.Ürün/hizmet satın alınan tedarikçilere karşı kritik verileri korumak için belirlenmiş standart ve kurllar mevcut mu?			
2. Ürün/hizmet satın alınan tedarikçilerin Çalıştığınız sağlık tesis hizmetlerinde kullanılmak üzere yeni bilişim teknolojileri alt yapı bileşenleri temininde tedarik zincirinden kaynaklı ne tür zaafiyetler ortaya çıkabileceği yazılı hale getirildi mi?			
3. Ürün/hizmet satın alınan tedarikçilerle Çalıştığınız sağlık tesisinde arasında bilgi güvenliği ve hizmet kalitesi konularını kapsayan yazılı bir sözleşme var mı?			
4. Ürün/hizmet satın alınan tedarikçiler ile yapılan çalışmalar kayıt altına alınıyor mu?			
5. Ürün/hizmet satın alınan tedarikçiler ile yapılan çalışmalar kapsamında tedarikçinin iş süreçleri yetkinliği izleniyor/ölçülüyor mu?			

BÖLÜM 13: BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ

	EVET	HAYIR	KISMEN
1. Bilgi güvenliği ihlali olaylarını tespit ve en aza indirgeme amaçlı, tedbir, tespit, kanıt toplama, iyileştirme, raporlama işlemlerini kapsayan prosedürler/standartlar mevcut mu?			
2. Çalıştığınız sağlık tesisinde çalışmaları kapsamında ortaya çıkan bir bilgi güvenliği ihlali durumunda konuyla ilgilenecek bir sorumlu belirlendi mi?			
3. Çalıştığınız sağlık tesisinde çalışmaları kapsamında ortaya çıkan bir bilgi güvenliği ihlali durumunda ilgilenecek sorumlunun izleyeceği süreçler belirlendi mi?			
4. Çalıştığınız sağlık tesisinde, çalışanlarından sistemler veya hizmetlerde gözlenen/şüphelenilen bir bilgi güvenliği zaafiyeti olması durumunda bunu bildirmeleri istendi mi?			
5. Bilgi güvenliği ihlali gerçekleşmesi durumunda uygulanacak yazılı bir planlama ve uygulama mevcut mu?			
6. Bilgi güvenliği ihlali gerçekleşmesi durumunda uygulanacak yazılı planlama uygulanıyor mu?			

BÖLÜM 14: İŞ SÜREKLİLİĞİNİN BİLGİ GÜVENLİĞİ HUSUSLARI

	EVET	HAYIR	KISMEN
1.Bilgi güvenliği sürekliliğini sağlamak üzere, Çalıştığınız sağlık tesisinde bilgi güvenliği olağan iş süreçlerinden birisi haline getirildi mi?			
2. Bir kriz/doğal afet benzeri durumlarda bilgi güvenliği yönetimini ve bilgi güvenliği yönetiminin sürekliliğini sağlamaya yönelik alınan tedbirler mevcut mu?			
3. Çalıştığınız sağlık tesis hizmetlerinde kullanılan bilişim teknolojileri ekipmanının ve donanımının yeterliliği ve verimliliği konusunda çalışma yapıldı mı?			
4. Çalıştığınız sağlık tesis hizmetlerinde kullanılan yazılımların yeterliliği ve verimliliği konusunda çalışma yapıldı mı?			

BÖLÜM 15: UYUM

	EVET	HAYIR	KISMEN
1. Çalıştığınız sağlık tesisinde hizmet gerçekleştirilmesinde, bilişim güvenliği konusunda yasal zorunluluklara uyuluyor mu?			
2. Çalıştığınız sağlık tesisinde hizmetler esnasında üretilen bilgiler kaybedilmeye karşı uygun şekilde yasa veya sözleşmelerden doğan şartlar kullanılarak korunuyor mu?			
3. Çalıştığınız sağlık tesisinde hizmetler esnasında üretilen bilgiler yetkisiz yayımlamaya karşı uygun şekilde yasa veya sözleşmelerden doğan şartlar kullanılarak korunuyor mu?			
4. Çalıştığınız sağlık tesis bilgi güvenliği sistemleri belirli aralıklarla bağımsız şekilde inceleniyor/denetleniyor mu?			
5. Çalıştığınız sağlık tesisinde bilgi güvenliği sisteminin bilgi güvenliği standartları ile uyumluluğu düzenli şekilde gözden geçiriliyor mu?			