T. C.

NECMETTİN ERBAKAN ÜNİVERSİTESİ

SAĞLIK BİLİMLERİ ENSTİTÜSÜ

KURUMLARDA BİLGİ GÜVENLİĞİ YÖNETİMİ: HASTANE BİLGİ SİSTEMLERİ ÜZERİNDE BİR ARAŞTIRMA

HACER ÖZGE KURT

YÜKSEK LİSANS TEZİ

SAĞLIK YÖNETİMİ ANABİLİM DALI

TEZ DANIŞMANI

Doç. Dr. Yusuf Yalçın İLERİ

KONYA 2019

T. C.

NECMETTİN ERBAKAN ÜNİVERSİTESİ

SAĞLIK BİLİMLERİ ENSTİTÜSÜ

KURUMLARDA BİLGİ GÜVENLİĞİ YÖNETİMİ: HASTANE BİLGİ SİSTEMLERİ ÜZERİNDE BİR ARAŞTIRMA

HACER ÖZGE KURT

YÜKSEK LİSANS TEZİ

SAĞLIK YÖNETİMİ ANABİLİM DALI

TEZ DANIŞMANI

Doç. Dr. Yusuf Yalçın İLERİ

KONYA 2019

TEZ ONAY SAYFASI

Necmettin Erbakan Üniversitesi Sağlık Bilimleri Enstitüsü Sağlık Yönetimi Anabilim Dalı Yüksek Lisans Öğrencisi HACER ÖZGE KURT'un "Kurumlarda Bilgi Güvenliği Yönetimi: Hastane Bilgi Sistemleri Üzerinde Bir Araştırma" başlıklı tezi tarafımızdan incelenmiş; amaç, kapsam ve kalite yönünden Yüksek Lisans Tezi olarak kabul edilmiştir.

Konya/18../06../2019

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

Jüri Üyesi
Prof Dr. Rifat İRAZ
Selçuk Üniversitesi
.....

Jüri Üyesi
Doç. Dr. Ş. Didem KAYA
Necmettin Erbakan Üniversitesi
.....

Yukarıdaki tez, Necmettin Erbakan Üniversitesi Sağlık Bilimleri Enstitüsü Yönetim Kurulunun 01/08/2019 tarih ve 16../09.. Sayılı kararı ile onaylanmıştır.

Prof. Dr. Kısmet Esra
NURULLAHOĞLU ATALIK
Enstitü Müdürü
.....

APPROVAL

We certify that we have read this dissertation entitled "Information Security Management In Institutions: A Research On Hospital Information Systems" by "Hacer Özge KURT" that in our opinion it is fully adequate, in scope and quality, as dissertation for the degree of Master of Science in the Department of "Healthcare Management", Institute of Health Sciences, University of Necmettin Erbakan Konya, Turkey /18.06/2019

Principal Advisor
Assoc. Prof. Yusuf Yalçın İLERİ
Necmettin Erbakan University
.....

Examination Committee Member
Prof Dr. Rifat İRAZ
Selçuk University
.....

Examination Committee Member
Assoc. Prof. Ş. Didem KAYA
Necmettin Erbakan University
.....

This thesis has approved for the University of Necmettin Erbakan Institute of Health Sciences.

Prof. Dr. Kısmet Esra NURULLAHOĞLU ATALIK
Director of Institute of Health Sciences
.....

BEYANAT

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

18/06/2019

Hacer Özge KURT

turnitin

Ödevler Öğrenciler Not Defteri Kütüphaneler Takvim Tartışma Tercihler

GÖRÜNTÜLENİYOR: ANASAYFA > HACER ÖZGE KURT > KURUMLARDA BİLGİ GÜVENLİĞİ YÖNETİMİ

Bu sayfa hakkında

Bu sizin odev kutunuzdur. Bir yazılı ödevi görüntülemek için yazılı ödevin başlığını seçin. Bir Benzerlik Raporunu görüntülemek için yazılı ödevin benzerlik sutunundaki Benzerlik Raporu ikonunu seçin. Tıklanabilir durumda olmayan bir ikon Benzerlik Raporunun henüz oluşturulmadığını gösterir.

KURUMLARDA BİLGİ GÜVENLİĞİ YÖNETİMİ

GELEN KUTUSU | GÖRÜNTÜLENİYOR: YENİ ÖDEVLER ▼

Dosyayı Gönder

Çevrimiçi Derecelendirme Raporu | Ödev ayarlarını düzenle | E-posta bildirmeyenler

YAZAR	BAŞLIK	BENZERLİK	PUANLA	CEVAP	DOSYA	ODEV NUMARASI	TARİH
Hacer Özge Kurt	KURUMLARDA BİLGİ GÜVENLİĞİ YÖNETİMİ_HAS.	%23	--	--		1130791419	15-May-2019

Doç.Dr. Yusuf Yılan

TEŞEKKÜR

Yüksek lisans eğitimimin, tez çalışmamın ve sosyal hayatımın her aşamasında ışık olan, yol gösteren, destekleyen, cesaretlendiren ve en önemlisi bana farklı pencerelerden bakmayı öğreten kıymetli danışmanım Doç. Dr. Yusuf Yalçın İLERİ' ye,

Tez yazım sürecimde bilgisini paylaşıp destekçi olan değerli hocam Prof. Dr. Ramazan Erdem'e, yüksek lisans eğitimim boyunca bilgi ve tecrübelerinden istifade ettiğim Doç. Dr. Şerife Didem Kaya' ya, Arş. Gör. Muazez Demir'e ve Arş. Gör. Dilek Kocabaş başta olmak üzere SDÜ Sağlık Yönetimi bölümü hocalarına,

Hayatım boyunca her zaman yanımda olan, bugünlere gelmemi sağlayan, sevgi ve desteklerini her daim hissettiğim aileme, yanımda olup, bana ve çalışmama katkı sağlayan arkadaşlarıma sonsuz teşekkürlerimi sunarım.

Hacer Özge KURT

Konya, 2019

İÇİNDEKİLER

İç Kapak……*i*
Tez Onay Sayfası ..... *ii*
Approval ..... *iii*
Beyanat ..... *iv*
Benzerlik Oranı ..... *v*
Teşekkür ..... *vi*
İçindekiler ..... *vii*
Kısaltmalar Listesi ..... *x*
Şekiller Listesi ..... *xi*
Tablolar Listesi ..... *xii*
Özet ..... *xiii*
Abstract ..... *xiv*
1.GİRİŞ ve AMAÇ 1
2. GENEL BİLGİLER 3
2.1. Hasta Bilgilerinin Gizliliği *3*
2.1.1.Kişisel Bilgilerin Gizliliği Prensibinin Temeli *3*
2.1.2. Hasta İle Hekim Arasındaki İlişkinin Hukuki Niteliği *5*
2.1.3. Hekimin Hastanın Bilgilerini Saklama Yükümlülüğü *8*
2.1.3.1. Kavram *8*
2.1.3.2.Tıp Etiği Yönünden Uluslararası Düzenlemeler *9*
2.1.3.3. Hekimin Hastanın Bilgilerini Saklama Yükümlülüğü İle İlgili Özel Düzenlemeler *11*
2.1.3.4. Hasta Bilgilerinin Gizliliğine Yönelik Diğer Mevzuat Düzenlemeleri *14*
2.1.3.5. Kişisel Nitelikli Verilerin Otomatik İşleme Tabi Tutulması *20*
2.1.3.6. Hasta Bilgilerinin Gizliliği Prensibinin İhlalinin Sonuçları *21*
2.1.3.7. Verileri Hukuka Aykırı Olarak Verme\Ele Geçirme *26*
2.2. Bilgi Sistemleri ve Güvenliği *28*
2.2.1.2. Bilgi Sistemi *28*
2.2.1.3. Bilgi Sistemlerinin Sınıflandırılması *29*
2.2.1.4. Veri İşleme Sistemleri *29*
2.2.1.5. Ofis Otomasyon Sistemleri *30*
2.2.1.6. Karar Destek Sistemleri *30*
2.2.1.7. Yönetim Bilgi Sistemleri *30*
2.2.1.8. Üst Yönetim Bilgi Sistemleri *31*

2.2.2. Bilgi Yönetimi *31*
2.2.3. Bilgi Güvenliği *33*
2.2.3.1.Bilgi Güvenliği Yönetimi *35*
2.2.3.2.Türkiye'de ve Dünyada Bilgi Güvenliği *38*
2.2.3.3.Kurumsal Bilgi Güvenliği Hafızasının Oluşturulması *40*
2.2.3.4.Bilgi Güvenliğini Etkileyen Faktörler *40*
2.2.3.5.Bilgi Güvenliği Sağlama Araçları *44*
2.2.3.6.Bilgi Güvenliği Standartları *44*
2.3. Hastane Bilgi Yönetim Sistemleri *48*
2.3.1. Hastane Yönetim Bilgi Sistemlerinin Amacı *49*
2.3.2. Hastane Bilgi Yönetim Sistemlerinin Tarihsel Gelişimi *50*
2.3.3. Hastane Yönetim Bilgi Sisteminde Olması Gereken Temel Özellikler *51*
2.3.4. Hastane Bilgi Yönetim Sistemlerini Oluşturan Temel Bileşenler *53*
2.3.4.1. Klinik Bilgi Sistemleri *53*
2.3.4.2. Yönetimsel ve Finansal Bilgi Sistemleri *54*
2.3.4.3. Stratejik Karar Destek Sistemleri *55*
2.3.5. Hastane Bilgi Yönetim Sistemlerinin Kullanım Alanları *57*
2.3.6. Hastane Bilgi Yönetim Sistemlerinde Bilgi Güvenliği *58*
2.3.6.1. Hbys Bilgi Güvenliğinin Hukuki Dayanakları *59*
2.3.6.2. Hbys'de Bilgi Güvenliği Önlemleri *59*
2.3.6.3. Veri Güvenliği Açısından Tehditler *59*
2.3.6.4. Bilgi Güvenliği Önlemleri Ve Kimlik Doğrulama *60*
2.4. Konu İle İlgili Yapılmış Önceki Çalışmalar *63*
3. GEREÇ ve YÖNTEM **64**
3.1. Araştırmanın Amacı ve Önemi *64*
3.2. Araştırma Evreninin Belirlenmesi Ve Örneklemi *64*
3.3. Veri Toplama Yöntemi *65*
3.3.1. Boyutların Psikometrik Özellikleri *65*
3.4. Anket Formunun Hazırlanması *67*
3.5. Analiz ve Yöntem *68*
3.6. Araştırmanın Etik Boyutu *68*
3.7. Araştırmanın Sınırlılıkları *68*
3.8. Araştırmanın Soruları *69*
4.BULGULAR **70**
4.1. Katılımcıların Demografik Değişkenlere Göre Dağılımı *70*

4.2. Elde Edilen Verilerin Analizi ve Bulguların Değerlendirilmesi 71

4.3. Boyutların Demografik Değişkenlere Göre Karşılaştırılması 74

4.3.1. Erişim ve Yetkilendirme Boyutunun Demografik Değişkenlere Göre Karşılaştırması 74

4.3.2. Güvenlik Uygulamaları Boyutunun Demografik Değişkenlere Göre Karşılaştırması 76

4.3.3. Hizmet Sunumu Boyutunun Demografik Değişkenlere Göre Karşılaştırması . 79

4.3.4.Örgütsel Güvenlik Boyutunun Demografik Değişkenlere Göre Karşılaştırması 81

4.3.5.Güvenlik Politikaları Boyutunun Demografik Değişkenlere Göre Karşılaştırması 84

4.4. Ankete Katılan Bireylere Yönelik İfadeler 87

5. TARTIŞMA ve SONUÇ 93

KAYNAKLAR 100

EKLER 107

Ek- A Etik Kurul Onay Yazısı 107

Ek- B Araştırma İzni 110

Ek- C Anket Formu 111

KISALTMALAR LİSTESİ

ÇKYS : Çekirdek Kaynak Yönetim Sistemi

İKY : İnsan Kaynakları Yönetimi

İKYS : İnsan Kaynakları Yönetim Sistemi

IOM : Institute of Medicine

KDS : Karar Destek Sistemi

MKYS : Malzeme Kaynak Yönetim Sistemi

PKI : Private Key Infrastructure (Açık Anahtar Alt Yapısı)

SBMT : Sağlık Bakanlığı Merkez Teşkilatı

SKYS : Özel Sağlık Kuruluşları Yönetim Sistemi

TSİM : Temel Sağlık İstatistikleri Modülü

YBS : Yönetim Bilgi Sistemleri

YTS : Yatırım Takip Sistemi

VPN : Virtual Private Network (Sanal Özel Ağ)

SS : Standart Sapma

$\overline{X}$: Aritmetik Ortalama

ŞEKİLLER LİSTESİ

Şekil 1: Sağlık Bilgi Sistemlerinin Tarihsel Gelişimi *50*

Şekil 2: Hastane Bilgi Yönetim Sistemleri Modüler Yapısı Örneği *52*

Şekil 3: Sağlık Bakanlığı Çekirdek Kaynak Yönetim Sistemi Bileşenleri *56*

Şekil 4: Çekirdek Kaynak Yönetim Sistemi İletişim Ağı Mimarisi *57*

TABLOLAR LİSTESİ

Tablo 3.3.1. Boyutların Psikometrik Özellikleri *66*
Tablo 4.2. Katılımcıların Bilgi Güvenliği Sorularına Verdikleri Cevaplara İlişkin Puanların Dağılımı *71*
Tablo 4.3.1. Erişim ve Yetkilendirme Boyutunun Demografik Değişkenlere Göre Karşılaştırması *74*
Tablo 4.3.2. Güvenlik Uygulamaları Boyutunun Demografik Değişkenlere Göre Karşılaştırması *76*
Tablo 4.3.3. Hizmet Sunumu Boyutunun Demografik Değişkenlere Göre Karşılaştırması *79*
Tablo 4.3.4. Örgütsel Güvenlik Boyutunun Demografik Değişkenlere Göre Karşılaştırması *81*
Tablo 4.3.5. Güvenlik Politikaları Boyutunun Demografik Değişkenlere Göre Karşılaştırması *84*
Tablo 4.4.2. Araştırmaya Katılan Tıbbi ve İdari Birim Çalışanlarının HBYS Kullanımları *88*
Tablo 4.4.3. Araştırmaya Katılan Tıbbi ve İdari Birim Çalışanlarına Göre HBYS Kullanımında Erişim Denetimi *89*
Tablo 4.4.4. Araştırmada Tıbbi ve İdari Birim Çalışanlarının Bilgi Güvenliği Uygulamaları *89*
Tablo 4.4.5. Araştırmaya Katılan Tıbbi ve İdari Birim Çalışanlarına Göre Bilgi Güvenliği Kazalarının Duyurulma ve Farkındalık Sağlama Yöntemleri *91*

ÖZET

T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

Kurumlarda Bilgi Güvenliği Yönetimi: Hastane Bilgi Sistemleri Üzerinde Bir Araştırma

Hacer Özge KURT
Sağlık Yönetimi Anabilim Dalı
YÜKSEK LİSANS TEZİ / KONYA 2019

Bilgi teknolojilerinde yaşanan hızlı değişim ve gelişmeler sonucunda yazılı ortamda kayıtlı olan sistemlerden, sağlık hizmetlerini maliyet-etkin bir biçimde sağlayan ve yeni servisler açısından fırsatlar yaratan bilgi sistemlerine geçiş süreci yaşanmaktadır. Bu bağlamda bilgi sistemlerinin en kayda değer faydalarından biri de bilgiyi çok daha kolay erişilebilir hale getirmesi ve bunun sonucunda çok daha hızlı ve kaliteli sağlık hizmeti verilmesidir. Bu çalışmada sağlık alanında çalışanların veri gizliliği, bilgi güvenliği ve hastaların kayıtlara ulaşımı konularında mesleki bilgi ve farkındalıklarına yönelik betimsel ve nicel veriler sunmak amaçlanmıştır. Çalışma kapsamında bilgi güvenliği konusundaki tutumların tespiti amacıyla Isparta merkezinde bulunan Süleyman Demirel Üniversitesi Araştırma ve Uygulama Hastanesi'nin çalışanlarına anket uygulanmış, anket sorularına verilen cevaplar SPSS 24.0 İstatistik paket programı ile analiz edilerek elde edilen bulgular tartışılmıştır.

Araştırmada, üniversite hastanesinde çalışan mevcut kişilere tanımlayıcı sorular, HBYS ile ilgili sorular ve bilgi güvenliği yönetimi ölçeğinin yer aldığı anket formu uygulanmıştır. Ayrıca bireylerin bilgi güvenliğine ilişkin memnuniyetleri tespit edilmeye çalışılmıştır. Çalışmanın evreni 1265 kişi olup, formülle belirlenen kişi sayısına basit tesadüfi örneklem yöntemi kullanılarak ulaşılmaya çalışılmıştır. Araştırma kapsamında 317 anket analize alınmıştır. Verilerin analizinde; ortalama, standart sapma, t ve ANOVA testi analizinden yararlanılmıştır. Erişim ve yetkilendirme, güvenlik uygulamaları, hizmet sunumu, örgütsel güvenlik ve güvenlik politikaları olmak üzere bu beş boyut demografik değişkenlere göre farklılık gösterip göstermediğinin tespiti yapılmıştır. Gruplar arasında fark tespit edildiği durumlarda ise farkın kaynağını anlayabilmek amacıyla Post-Hoc testlerinden "Tukey testi" kullanılmıştır. Anketin ikinci bölümündeki çoktan seçmeli sorulara frekans analizi uygulanmıştır.

Araştırma sonucunda tıbbi ve idari birimlerin ortak olarak hasta ve sosyal güvence bilgilerine ulaşabildikleri tespit edilmiştir. Ayrıca grupların, bilgi işlem yetkilendirmelerinden benzer olduğu sonucuna ulaşılmıştır. Bireylerin bilgi güvenliğinde güvenlik uygulamaları boyutundan (3,00) orta derecede, erişim ve yetkilendirme (3,64), örgütsel güvenlik (3,43), güvenlik politikaları (3,24) ve hizmet sunumu (3,65) boyutlarından iyi düzeyde memnun oldukları sonucuna varılmıştır. Buradan çalışanları hizmet sunumunda HBYS şartlarının iyi olduğu, yetkililerin erişim ve yetkilendirilme noktasında çalışanları memnun ettikleri ve örgütsel güvenlik hakkında bilgilendirme yaptıkları tespit edilmiş.

Anahtar Kelimeler: Bilgi güvenliği; Hastane bilgi yönetim sistemleri; Sağlık kurumları.

ABSTRACT

REPUBLIC of TURKEY

NECMETTİN ERBAKAN UNIVERSITY

HEALTH SCIENCES INSTITUTE

Information Security Management In Institutions: A Research On Hospital Information Systems

Hacer Özge Kurt

Health Management Department

MASTER'S THESIS / KONYA 2019

As a result of rapid changes and developments in information technologies, there is a transition process from information systems registered in written environment to information systems that provide health services-cost effectively and create opportunities for new services. In this context, one of the most valuable benefits of information system is to make information much easier to accessand, as a result, to provide faster and better quality health care. In this study, it is aimed to present descriptive and quantitative data about occupational knowledge and awareness in the field of data confidentiality, information security and access of health care worker store cords of patients. Within the scope of the study, a question naire was applied to the employees of Süleyman Demirel University Research and Application Hospital located in the center of Isparta in order to determine the attitudes related to information security and the findings obtained by analyzing the answers to the questionnaires were analyzed with SPSS 24.0 statistical package program.

A questionnaire including descriptive questions, HIS related questions and information security management scale was applied to the current people working in the university hospital. In addition, satisfaction of individuals about information security has been tried to be determined. The population of the study is 1265 people and it is tried to be reached by using simple random sampling method. In the scope of the research, 317 questionnaires were taken for analysis. In the analysis of data; mean, standard deviation, t and ANOVA tests were used. Access and authorization, security practices, service delivery, organizational security and security policies have been determined to determine whether these five dimensions differ according to demographic variables. In the cases where there is a difference between the groups, the concept Tukey test from the Post-Hoc tests was used to understand the source of the difference. Frequency analysis was applied to the multiple-choice questions in the second part of the questionnaire.

As a result of the research, it has been determined that medical and administrative units have access to patient and social security information jointly. In addition, it was concluded that the groups were similar to the information processing authorization. It has been concluded that individuals are well satisfied with the dimensions of security practices in information security (3,00), access and authorization (3,64), organizational security (3,43), security policies (3,24) and service delivery (3,65). Here, it is determined that the employees are satisfied with the HBYS conditions in the provision of services and that the employees are satisfied with the employees at the point of access and authorization, and they inform about the organizational security.

Keywords: Healthcare institutions; Hospital information management systems; Information security.

1. GİRİŞ ve AMAÇ

Bilgi teknolojilerinde yaşanan hızlı değişim ve gelişmeler sonucunda yazılı ortamda kayıtlı olan sistemlerden, sağlık hizmetlerini maliyet-etkin bir biçimde sağlayan ve yeni servisler açısından fırsatlar yaratan bilgi sistemlerine geçiş süreci yaşanmaktadır. Bu bağlamda bilgi sistemlerinin en kayda değer faydalarından biri de bilgiyi çok daha kolay erişilebilir hale getirmesi ve bunun sonucunda çok daha hızlı ve kaliteli sağlık hizmeti verilmesidir.

Hastalar polikliniklerden kamu ya da özel hastanelere birçok sağlık kurumunda bakım görebilmekte ve hizmet alabilmektedir. Bakım ve tedavi aşamasında hastaya ait kan örneklerinden röntgenine kadar hastalara ilişkin birçok bilgi elde edilmektedir. Araştırmada bilgiler kurumların bünyelerinde muhafaza edilmektedir. Diğer taraftan, anılan bilgiler farklı kurumlarla da paylaşılmaktadır. Bu kapsamda sigorta kurumlarından eczanelere birçok noktada hasta bilgileri kişiler tarafından erişilebilmektedir. Bu erişimler yapılırken verinin bu yeni ortamdaki güvenliği ve gizliliği de dikkate alınması gereken önemli bir konudur. Kişisel veri saklayan bilgi sistemleri, ilgili politikalar, kurallar, prosedürler ve düzenlemelerle uyumlu olması amacıyla bilgi güvenliği ve gizliliği ile alakalı hususların etkin bir biçimde ele alması gereklidir.

Bilgi güvenliği sağlık hizmetlerinde kritik bir önem taşımaktadır. Sağlık personeli, yöneticileri ve sağlık hizmetlerinden yararlananlar da bilgi güvenliği sürecinde önemli rol ve haklara sahiptirler. Tıbbi ya da idari birim çalışanı olmak ve HBYS eğitimi almak, bilgi güvenliği ile ilişkili önemli faktörlerdendir. Bilgi güvenliğinin tüm çalışanlar için ve özellikle yöneticiler için oldukça kritik olması nedeni ile bilgi güvenliği politikaları geliştirmek ve bunları kurumdaki tüm çalışanlar ile paylaşmak gerekmektedir. Sağlık sistemleri için yapılan bu uygulamaların yönetim perspektifinden amacı hizmetin sunumunu, verimliliğini ve etkinliğini artırmaktır. Tıbbi hizmetler ve idari hizmetlerin elektronik ortama taşınabilirliği, sağlık politikaları bakımından önemlidir. Bilgi güvenliğinin tüm boyutları birbirleri ile ilişkili olduğu için bunların uygun şekilde değerlendirilmesi oldukça önemlidir. Biri olmadan diğerinin olamayacağı göz ardı edilmemelidir.

Çalışma üç bölüm olarak planlanmıştır. Çalışmanın ilk bölümünde hasta bilgilerinin mahremiyetinin önemine değinilmiş ve yasal çerçeve çizerek daha

anlaşılır kılınması amacıyla ilgili dünyada ve Türkiye'de yasal düzenlemelere yer verilmiştir. Çalışmanın devamında hasta bilgilerinin gizliliği ve güvenliğine ilişkin tanımlamalar yapılmış, yasal düzenlemeler açıklanmış ve problemler muhtemel ihlaller sonucunda yaşanabilecek sorunlar ortaya konmuştur. Aynı bölümde bilgi sistemleri ve bilgi güvenliği konusunda kavramlar açıklanmış, kullanılan sistemler açıklanmıştır. Bilgi yönetimi ve bilgi güvenliği konuları incelenmiş ve hastane bilgi yönetim sistemlerinde bilgi güvenliği açıklanmıştır. Ayrıca bilgi sistemlerinin önemi, bilgi güvenliğinin dünyada ve ülkemizdeki yeri, kurumsal bilgi güvenliği hafızasının oluşturulması, bilgi güvenliğini etkileyen faktörler gibi konular işlenmiştir.

Çalışmanın son bölümde çalışanların bilgi güvenliğine ilişkin tutumları tespit edilmeye çalışılmıştır. Çalışmanın amacı, yöntemi, hipotezleri açıklanmıştır. Çalışmanın verileri SPSS 24.0 paket programında Frekans Analizi, Bağımsız Gruplar t-testi ve ANOVA testi kullanılarak analiz edilmiş ve elde edilen bulgulara yer verilmiştir. Son olarak araştırmanın bulguları tartışılmış, bulgular ışığında sonuçlar ortaya konmuş ve bu sonuçlara yönelik öneriler sunulmuştur.

Bu çalışmada, günümüzde gittikçe önemi artan bilgi güvenliği yönetimi ve teknolojik gelişmeleri uyum sağlamak, gerekli tedbirleri alabilmek ve alanındaki her türlü bilgi ve beceriyi doğru aktarabilmek için HBYS eğitimi, çalışanlar açısından önemli bir yere sahiptir. Çünkü hasta bilgilerinin doğru şekilde sisteme aktarılmasıyla birlikte, iletilmesi ve yetkili kişilerce kullanımının sağlanması kurumun hizmet sunumunda sağlık sektöründe ilgili oldukça önemli etkiye sahiptir. Bu çalışma, çalışanların arz edilen hızla hizmet veriliyorken HBYS 'nin doğru ve etkili kullanımı ile hasta mahremiyetine uygun bilgi güvenliğinin sağlanabiliyor olduğunu tespit etmek, çalışanların bilgi güvenliği açısından HBYS'yi değerlendirmenin ortaya konması açısından önemli görülmüştür. Bu çalışma sonucunda çalışanların vermiş olduğu cevaplar neticesine göre bilgi güvenliğinde yetersiz kalınması durumunda; HBYS'de iyileştirmeler ve geliştirmeler yapılmasının gerekli olacağı düşünülmektedir. Ayrıca bu çalışma, bu alanda yapılacak olan yeni çalışmaları besleyeceği için hem literatür hem de eğitim açısından önemli bir yere sahip olacağı düşünülmektedir.

2. GENEL BİLGİLER

2.1. Hasta Bilgilerinin Gizliliği

Kişisel bilgi kavramı, birçok açıdan korunması öncelikli olan haklardan biridir. Bu bağlamda kişisel bilgilerin bireylerin doğrudan bir şekilde özgürlükleriyle ilgili olduğu gerçeği akıldan çıkarılmamalıdır. İkincisi ise bu hakkın korunması gerekliğidir. Bununla birlikte kişisel verilerin gizliliği bireylerin özel hayatlarını da ilgilendirdiğinden saklı tutulmasının gerekliği bir başka açıdan da ortaya çıkmaktadır. Bu açıdan, kişisel bilgi kavramı uluslararası normlarda ve iç hukukta en önemli konuların başında gelmektedir (Er 2008).

2.1.1.Kişisel Bilgilerin Gizliliği Prensibinin Temeli

Özel hayatın gizliliğine dair birçok hukuki düzenlemede görülmektedir. Bu düzenlemelerden en öne çıkanı İnsan Hakları Evrensel Bildirgesi'dir. Bu bildirgenin 12. Maddesi özel hayatın gizliliğini düzenlemektedir. İlgili maddeye göre "kimsenin özel yaşamına, ailesine konutuna ya da haberleşmesine keyfi olarak karışılamaz, şeref ve adına saldırılamaz. Herkesin bu gibi karışma ve saldırılara karşı yasa tarafından korunmaya hakkı vardır". Bu düzenleme özel hayatın gizliliğini evrensel olarak koruma altına almaktadır (Erdem 2008).

Kişisel bilgilerin gizliliği konusunda yapılan bir diğer uluslararası düzenleme ise İnsan Haklarının ve Temel Özgürlüklerinin Korunmasına dair 1950 yılında yürürlüğe giren sözleşmedir. Bu sözleşme 20 Mart 1950'de Roma'da imzalanmıştır. Sözleşme, Türkiye'de 18 Mayıs 1954'de onaylanmıştır. Avrupa İnsan Hakları Sözleşmesi'nin 8. Maddesi de özel hayatın gizliliğini düzenlemektedir.

Avrupa İnsan Hakları Sözleşmesi'ne göre kişisel bilgilerin korunması, özel hayatın gizliliği kanunun içerisinde düzenlenmiştir. Ancak bu düzenlemelere rağmen kişisel bilgilerin saklandığı ya da depolandığı da bilinmektedir. Bu tarz ihlaller ise bu hakkın hukuki olarak korunmasını zorunlu kılmaktadır (Erdem ve ark. 2004).

AİHS'nin 8. maddesi aynen şu şekildedir;

“Herkes özel ve aile hayatına, konutuna ve haberleşmesine saygı gösterilmesi hakkına sahiptir. Bu hakkın kullanılmasına bir kamu otoritesinin müdahalesi, ancak ulusal güvenlik, kamu emniyeti, ülkenin ekonomik refahı, dirlik ve düzenin korunması, suç işlenmesinin önlenmesi, sağlığın veya ahlakın veya başkalarının hak ve özgürlüklerinin korunması için, demokratik bir toplumda, zorunlu olan ölçüde ve yasayla öngörülmüş olmak koşuluyla söz konusu olabilir.”

Özel hayatın gizliliğine dair hukuki tasarruflarda bulunabilecek bir diğer kurum ise Avrupa İnsan Hakları Mahkemesi’dir. AİHM ise bu hakkın yasal bir dayanak olmaksızın ihlal edilmesini onaylamamaktadır. Ancak özel durumlarda bu hak askıya alınabilmektedir. Bu bağlamda AİHM elde edilen kişisel bilgilerin de ancak amacına uygun biçiminde kullanılması gerekliğini belirtmektedir. Toplanan kişisel veriler amacı dışında kullanıldığında ise bir başka hak ihlal edilmektedir. Bu durum hukuki süreç usul yönüyle de sorunlu bir hal almaktadır (Erdem 2008).

Türk Hukuku’nda ise kişisel bilgilerin korunması 82 Anayasası ile gündeme gelmiştir.1982 anayasasının 20. Maddesi bu durumu düzenlemektedir. Bu maddeye göre “Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz”.

Anayasanın 20. maddesinin ikinci fıkrasına göre de milli güvenlik, kamu düzeni, suç işlenmesinin önlenmesi, genel sağlık ve genel ahlakın korunması veya başkalarının hak ve özgürlüklerinin korunması sebeplerinden biri veya birkaçına bağlı olarak, usulüne göre verilmiş hakim kararı olmadıkça; yine bu sebeplere bağlı olarak gecikmesinde sakınca bulunan hallerde de kanunla yetkili kılınmış merciin yazılı emri bulunmadıkça; kimsenin üstü, özel kağıtları ve eşyası aranamaz ve bunlara el konulamaz.

Hukuki düzenlemelerin bir diğer ayağını ise mevzuat hükümleri oluşturmaktadır. Bu mevzuatların başında kişilerin haklarını koruyan medeni kanunun 23. ve 25. maddeleri gelmektedir. Birçok farklı açıdan İsviçre hukukunda etkilen Türk hukuk sisteminin bu maddeler özelinde İsviçre hukukundan etkilendiği görülmektedir. Nitekim kişisel haklar ayrı ayrı değerlendirilmekten daha çok genel olarak takdir yetkisi hakime bırakılmıştır. Bununla birlikte kişisel bilgilerin gizliliğine yönelik kanunlar geniş başlıklar halinde düzenlenmiştir.

Kişisel hakların gizliliği konusunda değinilmesi gereken kavramlardan biri "gizlilik alanı" kavramıdır. Gizlilik alanı ise bir kişinin kendi şahsi bilgilerinin saklandığı alandır. Bu alanı bireyler belirler. Gizlilik alanı genellikle üçüncü kişilerden saklanan alandır ya da sadece bilgi sahibinin istediği kişilerle paylaşılmasıdır. Gizlilik alanına kişinin bilinmesini istemediği tüm belge ya da dokümanlar girmektedir. Ayrıca bu gizlilik alanı bireyin şahsi bilgi ve sırlarını içermektedir. Burada sır kavramının tanımı da önem arz etmektedir. Sır öncelikle kişisel bir durumdur ve ilgili konu her neyse onun sır değeri olup olmadığına dairi fikri bireyin kendisi verir. Bu durumda sır kişinin iradesine bağlıdır ve iradenin ise iki farklı yönü bulunmaktadır. Öncelikle herhangi bir durumun suç unsuru teşkil edip etmediği ya da kimlere karşı sır oluşturabileceğidir. İkinci yönü ise sır olarak kalacak konun bireyin yararına olup olmadığı gerçekliğidir (Dural 1995).

"Sır" olgusuna bir de hukuki literatür açısından bakılması gerekmektedir. Hukuki anlamda sır, bir kişinin herkesçe bilinmeyen yönlerini ve açıklandığında o kişiyi küçük düşürecek durumları ifade etmektedir. Bu bağlamda sırrın açıklanmaması sırrın sahibinin yararına olan bir durumdur. Ancak bir olay ya da durum herkes tarafında bilinirse sır olma özelliğini kaybeder. Tıbbi olarak bir hastanın özel durumunu öğrenen doktor o kişinin sırrını da öğrenmiş olmaktadır. Bu sır doğrudan hasta üzerinde öğrenilmiş olabileceği gibi yakınları aracılığıyla da öğrenilebilir (Yıldırım 2007). Bununla birlikte herhangi bir sohbet esnasında öğrenilebilecek konular ilgili kişinin sırrı olarak kabul görmemektedir. Ancak, herkesin bildiği konular veya herhangi bir kişi tarafından kolayca öğrenilebilecek hususlar, sohbet, dedikodu vb. yollarla edinilen bilgiler sır olarak kabul edilemez (Er 2008).

2.1.2. Hasta ile Hekim Arasındaki İlişkinin Hukuki Niteliği

Sadece hasta ile hekim arasındaki ilişkinin niteliğini içeren özel bir düzenleme bulunmamaktadır. Tedavi sözleşmesi diye ifade edebileceğimiz bu sözleşme hukuki olarak borçlar hukukuna dayanmaktadır. Bununla birlikte ifade edilen sözleşmenin, hem konuları hem de diğer boyutlarının hukukla olan bağının tartışmalı olarak devam ettiğini de söylemeliyiz. Gelinen noktada hasta ile hekim arasında yapılan gizlilik sözleşmelerinin hangi hukuk kanunlarına göre düzenleneceği bir sorun olarak devam etmektedir (Akartepe 2007).

Özdemir (2004)'e göre hekimlik sözleşmesi, hem doktora he de hastaya yükümlülükler yükleyen ayrıca kanunla da koruma altına alınan bir tür sağlık anlaşmasıdır. Hasta hekim arasındaki bu sözleşme ile birlikte hekim, hasta için gerekli tedaviyi uygulamayı da kabul etmektedir. Ancak bu tedavi, uygulamasında tıbbın kabul ettiği genel kabulleri de uygulamayı yapmak zorundadırlar (Akartepe 2007). Hekim-hasta arasında tesisi edilen bu sözleşmenin en öne çıkan niteliği doğru tedavinin uygulanması zorunluluğudur. Bununla beraber, sonucun garanti edilmesi mümkün değildir (Sarıtaş 2005).

Tüm bu unsurlar göz önüne alındığında, literatür incelendiğinde varılan netice itibariyle; hekim ile hasta sözleşmesinin Borçlar Kanunu'nda yer alan adi vekalet hükümlerine bağlı olduğu görülmektedir. Bu sözleşme bir tedaviyi gerektirdiğinden bir fiili de zorunlu kılmaktadır. BK'nın 386. Maddesine göre yapılan bu tedavi bir iştir. Daha önce ifade edilen vekâlet sözleşmesi hukuki fiille ile birlikte maddi bir işi de içerebilmektedir (Sarıtaş 2005; Akartepe 2007). Ayrıca iki taraf arasında yapılan bu sözleşme ile birlikte hekim hastaya yönelik tedaviyi uygulamayı da kabul etmektedir. Bu bağlamda aynı kanun kapsamında sözleşmenin her iki ucundaki taraflar için bir sözleşmeye bağlılık ödevi de bulunmaktadır (Öztürkler 2003).

Bu bağlamda hekim tarafından hastanın bilgilendirilmesi, tedavinin anlatılması ve bilgilerin saklanması da aynı sözleşmenin kapsamındadır.

Hekim ile hasta arasında oluşan bu akitte hekimin sözleşmeye olan bağlılığına yönelik özel bir madde bulunmasa da vekâlet anlaşması bu sadakati de zorunlu kılmaktadır. Ortaya konan bu bağlılık, tedavi bittikten sonra da özel bilgilerin korunmasını esas almaktadır (Tandoğan 1985).

Yukarıda da tanımı yapılan hasta-doktor sözleşmesi içeriğinden dolayı bir tür iş görme sözleşmesi de olarak da adlandırılabilir. Nitekim doktorun herhangi bir hatası ciddi bir yıkım da neden olabilmektedir. Bu bağlamda hekimin hem sözleşme gereği açısından hem de etik kurallar bakımından dikkat etmesi gereken kurallar bulunmaktadır. Bu bağlamda hekimin etik kurallara da riayet etmesi bir zorunluluk olarak görülmektedir. Hekimlerin hastalarına karşı olan görevleri tüm sağlık kontrollerini kapsarken, bununla birlikte zararı olabilecek şeylerden korumayı da içermektedir. Bu durumda bir hekim doktorluk görevini yerine getirirken, hastanın hem fiziksel sağlığını hem de psikolojik olarak sağlığını korumakla yükümlüdür.

Sonuç olarak tedavi sırasında öğrenilen tüm bilgiler saklı tutulmalıdır (İpekyüz 2006). Hastanın hekime olan güveni bu bilgilerin saklı tutulmasında yatmaktadır. Bu durumda hekim dürüst kalmalı ve hastanın güvenini sarsmamalıdır (Sarıtaş 2005). Eğer bu güvenin sarsılmasına yönelik herhangi bir tutum ya da davranış olursa hastanın bu durumu ifade etmesi ve kendisini bu fikre doğru iten davranışları anlatması yeterlidir. Ancak bu durum yine de bir ispat da gerektirmektedir. Böyle bir olayda hekime düşen ise aksi yönde beyan geliştirmektir.

Yukarıda belirtilen durumların somut olarak yaşandığı durumlar da söz konusudur. Nitekim bu bağlamda Yargıtay'ın aldığı kararlar bulunmaktadır. Bu kararlar Yargıtay 13. Hukuk Dairesi'nin 04.03.1994 tarihli 1994/8557-2138 sayılı ve 25.04.2002 tarihli 2002/2589-4560 sayılı kararlarında da mevcuttur. Bu kararlardan özetle şunları çıkartabilir:

"genel olarak bir vekil öncelikle yapılan işin özeninden sorumludur. Elbette ulaşılması istenen sonuç da önemlidir, ancak yapılan işlemlerdeki özen daha önemlidir. Ayrıca bu kurallar hem vekilin hem de işçinin sorumluluğunu düzenler (BK m. 390/II). Özenle davranmak sadece işçilere has bir durum değildir. Vekilinde özen sorumluluğu bulunmaktadır (BK m. 321/I). Bu bağlamda hekimler kendi alalarındaki tedaviye yönelik tüm kusurlardan sorumludurlar. Gelinen noktada hekimlerin sorumlulukları geniş olduğundan hastanın zarar görmemesine son derece dikkat etmeleri gerekmektedir.

Bu kararlar neticesinde; hekimin meslek kurallarına aykırı davranmasının, kusurun varlığı konusunda bir karine oluşturduğu teyit edilmektedir.

Vekilin bu kurallara aykırı davranması, maddi ve manevi tazminatla sorumlu tutulma sonucunu doğurur. Doktoruna güvenen müvekkili, mesleki bir iş gören vekilinden, yaptığı işte hassasiyet göstermesini beklemek hakkına sahiptir. BK m. 390 uyarınca akdi sorumluluğu düzenleyen BK m. 96 ve müteakip maddeleri; vekilin kusurlu olarak akdi ihlal ile hastaya zarar verme ve gizli sırlarını açıklaması halinde hukuki sorumluluğu doğacaktır (Öztürkler 2003).

Son olarak vurgulanması gereken bir diğer önemli husus da; vekilin sadakat borcunun sadece iş görme süresince devam etmeyip sürekli özelliğini koruyan bir borç olmasıdır. Yani iş görme süreci bitse bile devam eden bir yükümlülüktür. Akit

ilişkisi hakkında Borçlar Hukuku çerçevesinde hükümlerin mevcut olması ve bununla hastanın özel yaşamının korunmaya çalışılması konunun hassasiyetini gösteren başka bir unsur olarak karşımıza çıkmaktadır (Gürkan 2004).

2.1.3. Hekimin Hastanın Bilgilerini Saklama Yükümlülüğü

Bu konuda Borçlar Kanununda özel bir düzenleme bulunmamaktadır. Bununla beraber, sadakat yükümlülüğünün bir sonucu olan güven ilişkisinin gereği olarak hekim, hastasına ait öğrenmiş olduğu sırları saklamakla sorumludur. Tıbbi literatürde sır ise saklı kalması hastanın menfaatine olan her şeyi kapsamaktadır (Ayan 1991).

Hekim sağlık hizmeti verirken etik ilkelere bağlamında da sır saklama yükümlülüğü bulunmaktadır. Bu yükümlüğün en önemli yanını doktorun hastaya dair bilgileri üçüncü şahıslara açmaması oluşturmaktadır. Nitekim hekim-hasta ilişkisinde güven en önemli değişkenlerdendir. Güven duygusu doktorun gizlilik olgusuna dayanmaktadır. Sonuç olarak doktorlar hasta ile ilgili tespit ettikleri tüm detayları ve özel bilgileri başkaları ile paylaşmamalıdır (Özkan 2008).

Bu ayrıca tüm doktorlar için hastaların özel hayatlarına saygı duymalarını da gerektirmektedir. Bir hastanın en temel hakkı; özel hayatına dair bilgilerin her türlü hakkını ve ulaşımını kendi isteğine bağlı olarak denetlemesidir. Çünkü hasta tedavisi boyunca kendisiyle ilgili bilgileri doktora söylemek durumdadır. Ayrıca bu bilgilerle beraber tedavi sırasında oluşan yeni bilgiler de hem kurumla hem de doktorla paylaşılmaktadır. Tedavi sürecinde oluşan bu yeni bilgilerde kurum tarafından aynı titizlikte saklanmalıdır (Sert 2008).

2.1.3.1. Kavram

Hekimler için “meslek sırrı” kavramı bu gibi kişinin yaşama alanına giren mesleklerde kaçınılmaz bir zorunluluk haline gelmektedir. Aksi durumda sır sahibinin mahrem bilgileri aleniyet kazanacağından hekimin hukuki sorumluluğu doğacaktır (Hancı 2006).

Sırrın sınırını açıklandığı takdirde kişilere zarar veren her şey oluşturmaktadır. Bedensel özellikler, hastalık bulguları, psikolojik bozukluklar, toplumundan dışlanmalar, maddi sorunlara neden olan her türlü durum, (evli

olmayan birinin çocuk doğurması, intihar çabası, kürtaj vb.) her şey sırdır (Hatırnaz 2009). Hastayla doktor arasında kalması gerek iktisadi konularda sır olarak yorumlanabilmektedir (Ayan 1991).

Sır saklamanın hekimliğin tarihsel bir görevi olduğu kendini Hipokrat Andında da göstermektedir. Nitekim Hipokrat Yemini' nde de hekim hasta ilişkisindeki gizliliğe dikkat çekilmektedir.

Tarihsel süreç incelendiğinde hasta doktor ilişkisine yönelik Roma döneminde de vesikalar bulunmaktadır. Justinien Kanunları, Cassiodore ve Vespasien bu konunun diğer örneklerini oluşturmaktadır. Ancak bu konudaki ilk düzenlemeyi 1810 yılındaki Fransa Ceza Kanunu oluşturmaktadır (Sert 2008).

Hastanın rızası olmaksızın sır niteliği taşıyan hasta bilgilerinin hasta dışındaki ortamlarda üçüncü şahıslara söylenmesi gizlilik hakkının ihlal edilmesidir. Ancak ülkemizde bu tarz bir ihlale yönelik yaptırım yoktur. Bu konudaki hukuki boşluk Türk Ceza Kanunu'nun 24 vd. maddeler ile çözümlenmeye çalışılmıştır.

2.1.3.2.Tıp Etiği Yönünden Uluslararası Düzenlemeler

Tıp etiği çerçevesinde hareket etmesi hastaya yönelik uygulamaları açısından hekim için önem taşıyan ilk kavramdır.

Dünya Hekimler Birliği'nin aldığı kararlar birçok kurumu ilgilendirdiği gibi Türk Tabipler Birliği'ni de ilgilendirmektedir. Nitekim Dünya Hekimler Birliği'nin kararları tüm tıp çevrelerinde etkili olmaktadır.

Dünya Hekimler Birliği'nin mesleki bağlılık yemini adıyla anılan sözleşmesinde de "bana verilmiş olan sırlara, hastanın ölümünden sonra bile saygı göstereceğim*"* ifadesine yer verilmiştir. Aynı ifade dünya hekimler birliğin 1949 yılındaki 3. Genel Kurulunda da gündeme gelmiştir. Bu kurulda kabul edilen Uluslararası Tıbbi Etik Kodunda "hekim hastanın ölümünden sonra bile, hasta hakkında bildiği her şey ile ilgili bütün gizliliği sürdürecektir." İfadesine yer verilmiştir (Sert 2008).

Dünya Hekimler Birliği'nin kongrelerde bu konuda belli başlı aldığı kararlar şöyle özetlenebilir:

● Hekim hasta hakkında bildiği her şeyle ilgili hastanın ölümünden sonra bile gizliliği sürdürecektir (Hancı 2006).

● Hekimler hastaların özel bilgilerini hasta ölse dahi gizli tutmak durumundadırlar. Hastanın hekimden tüm özel ve tıbbi bilgilerin gizliliğine saygı duyulmasını bekleme hakkı vardır. Ancak bu bilgilerin gizli tutulmasının da istisnaları bulunmaktadır. Nitekim aynı yerde yaşayan akrabaları bu riskleri öğrenmek durumundadır. Ancak yine de hastaya ait olan bilgiler kanun çerçevesinde üçüncü şahıslara verilebilir. Bununla birlikte sağlık personeli kendi arasında bu bilgileri tedavinin doğru yapılabilmesi adına paylaşılabilir (Sert 2004).

● Dünya Sağlık Örgütü Avrupa Bürosu (World Health Organization 1994) tarafından hazırlanmış olan Avrupa'da Hasta Haklarının Geliştirilmesi Bildirgesi'nin "Mahremiyet ve Özel Hayat" başlıklı 4. maddesinin konu ile ilgili hükümleri şu şekildedir;

1. hastaya ait olan her türlü bilgi (tedavi süreci, tanısı ya da prognozu ve bireye ait diğer tüm bilgiler) hasta ölse dahi üçüncü kişilerle paylaşılmamalıdır.

2. hastaların kişisel bilgiler iki durumda paylaşılabilir. Bunlardan birincisi hastanın kendi rızası alınmasıdır. Diğeri ise yasal sorunlar olduğunda mahkemenin talep etmesidir.

3. hastaya dair bilgilerin korunması hukuki ve kurumsal usule göre yapılmalıdır.

4. Sağlık kurumlarına başvuran hastalar, özellikle sağlık personelinin kişisel bakımlarını veya muayene ve tedavilerini yapacağı durumda kurumların özel hayatlarının korunmasını sağlayan fiziksel özelliklere sahip olmasını bekleme hakkına sahiptirler (Hatun 1999).

Hastanın kimliğine ait tüm bilgiler korunmalıdır. Bu bilgiler tanıya yönelik de olsa, prognozda olsa kişinin ölümüne kadar korunmalıdır. Bu bilgilerin korunması usulüne uygun yapılmalıdır (Şükrü 1992).

Hasta Haklarına İlişkin Avrupa Statüsü 'nün (Roma - Kasım 2002) "hastalara ait 14 hak" başlıklı II. Bölümünün "özel ve gizlilik hakkı" başlıklı 6. maddesine göre

de; bireyin sağlık durumuna veya ona uygulanan tıbbi/cerrahi tedaviye ilişkin bilgi ve veriler gizli olmalı ve öyle muhafaza edilmelidir. Bununla birlikte hasta tedavi sırasında oluşabilecek yeni durumların saklanmasını da yeniden talep edebilmektedir. Ayrıca hasta, yapılan ziyaretlerinde gizli tutulmasını isteyebilmektedir. Tedavi sırasında yapılan her türlü tıbbi müdahalede de bireylerin onayının alınması önem kazanan bir diğer konudur (Hakeri 2007).

2.1.3.3. Hekimin Hastanın Bilgilerini Saklama Yükümlülüğü ile İlgili Özel Düzenlemeler

Hasta hakkındaki bilgi ve kayıtlar kamu ya da özel sağlık kurum ve kuruluşları tarafından düzgün bir biçimde tutulmak, bir dosya halinde saklanmakla zorundadır. Dosyada, hastanın bireysel bilgileri, yapılan tetkik ve tahlillerin sonuçları, tanı, hastalığın gelişimi, tedavinin seçimi, uygulanması, hastalığın seyri ve iyileşmesi gibi konular bilgiler bulunur (Er 2008).

Tıbbi kayıtların tutulma zorunluluğu konusu hakkındaki mevzuata genel hatlarıyla değinecek olursak aşağıdaki düzenlemeler karşımıza çıkabilmektedir.

Sağlık Hizmetlerinin Sosyalleştirilmesi Hakkında Kanun'un 10. maddesinde "sağlık ocakları ve evlerinin, her türlü koruyucu hekimlik hizmetleri ile hastaların muayene ve tedavisinin yanı sıra, sağlık ocağına kayıtlı şahısların sağlık sicillerini tutmakla mükellef oldukları aktarılmaktadır. Ayakta Teşhis Ve Tedavi Yapılan Özel Sağlık Kuruluşları Hakkında Yönetmeliği'nin 17. Maddesinde de sağlık çalışanlarının hastalarının bilgilerini kayıt etmekle sorumlu oldukları görülmektedir. 27. Madde ise hastanelere gelen hastaların bilgilerin nasıl düzenlenmesi gerektiğini, tıbbi konuların nasıl uygulandığını, gözlemleri ve tüm evrakların nasıl tasnif edilmesi gerektiğini düzenlemektedir.

Yataklı Tedavi Kurumları İşletme Yönetmeliği'nin 12. Maddesinde de polikliniğe gelen insanların tüm sağlık işlemlerinin (acil, adli vakalar vs.) ayrıca başvuru saatlerinin de kaydedilmesini içermektedir. Özel Hastaneler Yönetmeliği'nde de hastaneye başvurun kişilerin tüm bilgilerinin 21 yıl süreyle saklı tutulması gerekliği belirtilmiştir.

Aynı şekilde Acil Sağlık Hizmetleri Yönetmeliği'nin 8. maddesinde de resmi ve özel sağlık kurumlarına bağlı olarak çalışan hastanelerin acil bölümlerinin de kayıt tutması zorunlu hale getirilmiştir.

Özel Hastaneler Tüzüğü'nün "hasta dosyaları ve iç hizmet yönergesi" başlıklı 29. maddesi ve Tababet ve Şuabatı Tarzı İcrasına Dair Kanun'un 72. Maddesi uyarınca da hem kamu kurumlarının hem de özel kurumların gerek danışma için gelenleri gerekse de tedavi amaçlı gelenleri kayıt altında tutmaları kanuni olarak bir yükümlülüktür.

Bununla beraber uygulamada karşılaşılan önemli sorun, bu tıbbi kayıtların tutulmaması, saklanmaması veya mahkemelere gönderilmemesi ya da silinti ve eklentilerle gönderilmesi durumlarıdır. 657 sayılı Devlet Memurları Kanunu'nun 125. maddesi ile Yükseköğretim Kurumları Yönetici, Öğretim Elemanı ve Memurları Disiplin Yönetmeliği'nin 5 ve 8. maddeleri kapsamında idari cezayı getiren tıbbi dosyalardaki kayıtların tutulmaması, eksik tutulması veya saklanmaması konusunda belki de en ciddi yaptırım Türk Ceza Kanunu'nun 257. maddesi kapsamında görevin kötüye kullanılması olarak karşımıza çıkmaktadır (Akyıldız 2008).

Aynı zamanda doktorların herhangi bir hastayla ilgili kayıtları mahkeme istediği takdirde mahkemeye bildirme zorunluluğu bulunmaktadır. Bu durum ceza muhakemesinin 332. Maddesinde belirtilmektedir. Bu maddeye göre mahkeme bir hastanın evraklarını istediğinde 10 gün içinde göndermesi gereklidir. Gönderilmediği takdirde sebepleri mahkeme ile paylaşılmalıdır.

● Hasta Hakları Yönetmeliği Yönünden Hasta Bilgileri: Hastaneye gelen tüm hastaların tedavi amaçlı bilgileri ve özel kimlik bilgileri bireysel olarak kişiye aittir. Hasta mahremiyeti, ancak hastaya ait bilgilerin gizli tutulması ile mümkün olabilecektir (Özkan ve Akyıldız 2008).

Hastaların özel bilgilerinin korunması bir zorunluluk olsa da mahkeme istediği takdirde bu gizlilik bozulabilir. Gizliliğin bozulmasını ön gören maddeler 5/f de belirtilmektedir. Ayrıca 21. Madde de hastaların özel hayatlarının düzenlendiği görülmektedir. Hastanın mahremiyetine saygı gösterilmesi gerekliği, teşhisin ve tanının da diğer insanlarla paylaşılmaması gerekliği ifade edilmektedir. 23. Madde de ise hasta bilgilerinin hukuk tarafından müsaade edilen haller dışında

paylaşılmamasını ön görmektedir. Ayrıca bu haller dışındaki hak ihlalleri cezai yaptırımları olmaktadır (Hancı 2006; Savaş 2007; Sert 2008).

Yasa aksini öngörmediği ve emretmediği müddetçe sağlık personelleri hastaya dair bilgileri kimseyle paylaşamazlar. Akademik çalışmalar için de kullanılan hasta bilgileri hastanın rızası alınmadan araştırma ya da eğitim amaçlı çalışmalarda da yine hastanın rızası olmaksızın hiçbir bilgi açıklanmamalıdır. Hastadan izin alınmak şartıyla her zaman hastanın kimlik bilgileri açıklanabilir, araştırma ve eğitim amacıyla yapılan çalışmalarda da kullanılabilir. Fakat tersi durum mümkün değildir. Hukuki prosedürlere uymadan yapılan her türlü hasta özel bilgisinin paylaşımı hukuki başka sorunları oluşturabilir. Nitekim bilgisi paylaşılan hasta hukuki yollarla hakkını arayarak sağlık personeli hakkında suç duyurusunda bulunabilir (Özkan ve Akyıldız 2008).

Ölüm durumu dahi bu kapsam dışında değildir. Öyle ki; tıbbi eğitim verilen sağlık kurum ve kuruluşlarında, tedavi ile doğrudan ilgili olmayanların tıbbi müdahale sırasında bulunması gerekli ise; bu konu hakkında önceden veya tedavi sırasında hastanın ayrıca rızası alınır (Yıldırım 2007). Yine bu yönetmeliğin 2. Maddesi, hasta bilgilerinin sağlık haklarından faydalanma hakkı olan herkesi kapsamaktadır.

Bu yönetmelikle bağlantılı olarak Yataklı Tedavi Kurumları İşletme Yönetmeliği'nin 7. Maddesinde de, poliklinik muayenelerinde gizlilik prensiplerine riayetin esas olacağı, halkın gelenek ve ahlak kurallarına saygı gösterileceği, muayene esnasında poliklinik odasında tıp ve yardımcı tıp meslekleri personelinden başka kimsenin bulunamayacağı, ancak hasta isterse ailesinden biri veya bir yakını bulunabileceği hükme bağlanmış durumdadır.

● Türk Tabipler Birliği Hekimlik Meslek Etiği Kuralları: Hekimlik Meslek Etik Kurallarının 9. maddesi hasta bilgilerini saklama yükümlülüğünü düzenler. Buna göre "doktorlar tedavi sırasında ya da tedavi öncesinde hastasında öğrendiği özel bilgileri özel haller dışında kimseyle paylaşamaz. Hastanın ölümü dahi bu gizliliği ortadan kaldırmamaktadır. Ancak hastanın izni alınarak bilgiler paylaşılabilir. Özellikle diğer insanların sağlıklarının tehlikeye girmesi durumunda mevcut hastanın da kişilik haklarına dikkat edilerek bilgilerin paylaşımı yapılabilmektedir. Yasal durumlarda beyanına başvurulan hekimler meslek sırlarını

açıklamaya yönelik durumlar söz konusu olursa bu tanıklıklardan çekilebilirler (Hancı 2006).

Aynı düzenlemenin 31. maddesine göre, doktorlar hastaların tüm bilgilerini gizli tutmalıdır. Ancak dosya üzerinde belirlemeler yapılırken hekim, hastasının kimlik bilgilerini araştırma için kullanabilir.

Sonuç olarak, mevzuatta hasta bilgilerinin gizliliğine yönelik düzenlemeler bulunmakla birlikte, bu prensibin ihlali halinde maddi hukuk ve ceza hukuku düzenlemelerinde ne tarz bir yaptırımın uygulanacağı hakkında özel bir düzenleme bulunmamaktadır.

2.1.3.4. Hasta Bilgilerinin Gizliliğine Yönelik Diğer Mevzuat Düzenlemeleri

Medeni kanunda hukuken sadece üç durum yapılan müdahaleyi kanuna aykırılıktan kurtaracaktır. MK m. 24/II' ye göre bunlar aşağıdaki gibidir;

● Açıklamanın kişinin rızası ile yapılması, İsviçre Ceza Kanunu'na benzer bir yaklaşım gösteren 5237 sayılı Yeni Türk Ceza Kanunu'nun 26. maddesinin ikinci fıkrasına göre korunan hukuki yararın kişinin iç dünyasına müdahalesiz bir yaşam olması ve sır sahibinin açıklanmasına rıza göstermesi halinde meslek sırrının açıklanabileceği belirtilmiştir (Ayan 1991; Sert 2004).

Kanunda kural olarak rızanın şekli konusunda bir şekil şartı öngörülmemişse de, rızanın ispatlanması açısından yazılı şekilde alınmasında fayda bulunacağı açıktır (Erman 2003).

Bu bağlamda rıza, hak ihlalinden sonra onaylama ya da önceden verilecek bir izin şeklinde olabilir. Bu bağlamda verilerin alınması sırasında bu verilerin ileride belli amaçlarla kullanılmasına hukuki bir engel olmaması için hastadan yazılı bir izin alınabilir. Ancak bu şartla alınan bilgilerin 3. şahıslara aktarılması hukuka aykırılık teşkil etmez.

Bununla beraber, kişi hakları mutlak hak niteliğinde olduğundan baştaki amacın aşılması halinde hastanın rızası ortadan kalkmış olacağından, bu kullanımın hukuken yaptırımının olacağı unutulmamalıdır. Hatta hasta tarafından rızanın sonradan geri alınması halinde, bu konuda yetkilendirilmiş kişi ya da kurumun geri

alma nedeniyle uğrayacağı zararlarını tazmin ile yükümlü olacağı da düşünülmelidir. Son olarak, verilen rızanın geçerli olabilmesi için MK m. 23 anlamında hukuka ve ahlaka aykırı bir biçimde verilmemiş olması gereklidir (Dural 1995).

Bazı durumlarda hasta istese bile sağlık personeli tarafından hastanın zarar görebileceğinin öngörüldüğü hallerde sırrın açıklanmaması gerekir. Burada sağlık personeli tarafından yararlılık ve zarar vermeme ilkeleri çerçevesinde hareket edilmelidir. Açıklamanın yapılması halinde ise sadece rıza çerçevesindeki haller hakkında açıklama yapılmalıdır. Bununla ilgili Tıbbi Hizmetlerin Kötü Uygulanmasından Doğan Sorumluluk (Malpraktis) Kanun Tasarısı'nın 10. maddesinin dördüncü fıkrası ile getirilen düzenlemede hastaya ait sırrın açıklanması için hastanın yazılı izni aranmış fakat adli vakalar, bildirimi zorunlu hastalıkların varlığı halinde yapılacak açıklamayı yükümlülüğün ihlali saymamıştır. Buna göre, sırrın sahibi hastanın serbest iradesine dayanan açık veya örtülü rızası ile yapılacak açıklamalar hukuka uygundur. Fakat açıklamanın zararlı sonuçlar doğuracağı öngörülen durumlarda konuşulmaması daha yerinde bir davranış olacaktır (Karasu 2009).

Ayrıca Kişisel Verilerin Korunması Hakkında Kanun Tasarısı'nın 6. maddesine göre, kişisel veriler kişinin açık rızasıyla işlenebilir. Kanunun öngördüğü bir zorunluluğun mevcudiyeti durumunda; ilgili kişinin rızasını açıklayamayacak durumda olması halinde; kendisinin veya başkasının hayatını veya beden bütünlüğünü korumak amacıyla, kişisel verilerin işlenmesi durumunda verilerin işlenmesi hukuka uygun olacaktır (Hakeri 2007).

● Üstün bir kamu yararının bulunması, hastanın hastalığı bulaşıcı ve önemli problemler ortaya çıkarma ihtimali olan enfeksiyon hastalıkları gibi toplumu ciddi bir şekilde tehdit edebilecek mahiyette olur ve ortaya tıbbi ve yasal bir sorumluluk çıkmış olacaksa; bu haller "Üstün nitelikteki bir kamu yararı da kişilik hakkına yapılan müdahale" sınıfına gireceğinden bu bilgilerin gerektiği kadarının ilgili kişi ve kurumlara aktarılması hukuka aykırılığı ortadan kaldırır.

Örneğin; cinsel yolla bulaşan bir hastalığı olan kimse, kendi onayı alınarak (onlarda da hastalık meydana gelme olasılığı bulunduğundan) ilişkide bulunduğu diğer kişilere haber verilmelidir. Bu işlemler yapılırken de gizlilik kurallarına en yüksek şekilde özen gösterilmelidir (Sütlaş 2000).

AIDS hastası bir kişi ile ilgili Alman Federal Mahkeme kararına konu olan bir olaya göre; hasta öncelikle psikolojik destek almak istemiştir. Hastaneye bu istekle gelen AIDS hastası psikologdan ailesine ve karısına bu sorunu açmamasını söylemiştir. Ancak bu hasta iki yıl kadar sonra ölmüştür. Bu durumda doktor, ölen kişinin eşine durumu anlatmıştır. Olayı öğrenen eş hemen test yaptırmış ve o da AIDS olduğunu öğrenmiştir. Daha sonra olay mahkemeye taşınmıştır. Mahkeme ise olayın eşe daha önce anlatılması gerekliğini hükmetmiştir. Çünkü mahkemeye göre burada özel ve üstün denilebilecek bir yara vardır (Yıldırım 2007).

Aynı konuyla ilgili Avrupa İnsan Hakları Mahkemesi 25.02.1997 tarih ve 22009/93 sayılı Finlandiya'ya karşı Z kararında (Doğru 2002; Erdem ve ark. 2004); mahkeme tıbbi verilerin ceza muhakemesinde kullanılmasını sözleşmenin ihlali olarak nitelememiştir. Burada ifade edilen konu ise özetle şu şekildedir:

Mahkemeye taşınan konunun sahipleri X ve Y boşanmıştır. Davanın her iki tarafı da HIV virüsü taşıyıcısıdırlar. Y ye yönelik daha önceden bir dava açılmıştır. Bu dava ise cinsel suçtan dolayı açılmıştır. Bu yargılama esnasında başvurun kişi daha sonra tanıklıktan çekilmiştir. Gelinen noktada savcı başvurucunun doktorları ile görüşmüştür. Bu bağlamda başvurucun sağlık dosyası ev bilgileri mahkemeye dosyasına eklenmiştir. Mahkeme basından gizli bir şekilde yürütülmüştür. Ancak buna rağmen yine basına yansımıştır. Başvurucunun isteği nedeniyle karar 10 yıl süre ile gizli tutulmuştur. Kamuoyuna sadece kısa karar hakkında bilgi verilmiştir.

Avrupa İnsan Hakları Mahkemesi kararında;

Bu dava dosyasında başvuran kişinin doktorunun da dinlenilmesinin bir sebebi başvurucunun kendisinin tanıklıktan çekilmesi olmuştur. Y'nin yargılanmasında özel hayatın gizliliğine dikkat edilmiştir. Ancak diğer yandan yüksek bir kamu yararı olduğundan Y'nin hastalığının başlangıcı araştırılmıştır. Bu bağlamda Avrupa insan hakları sözleşmesinin 8. Maddesi ihlal edilmemiştir.

Bu dava özelinde tıbbi belgelere el konmasında yüksek kamu yararı göz önünde bulundurulmuştur. Ayrıca elde edilen belgelerin kötüye kullanılmasının da önüne geçilmeye çalışmıştır.

Ancak dava dosyasının 10 yıl süre ile kısıtlanması başvurucunun faydasını yeterince ön görmemiştir. 10 yıl sonra da olsa bu bilgilerin kamuoyuna açılmasının

doğrudan kamu yararına olmadığına hükmedilmiştir. Ayrıca bu durumun özel hayata orantısız müdahale olarak kabul edilmiştir. Sonuç olarak başvuran kişinin HIV virüsü taşıması ve bunu açıklanması 8. Maddenin ihlaline neden olmaktadır, tespitlerinde bulunmuştur.

● Kanunun verdiği yetki; kamu görevlileri ve kurumlarının, kamu hukukunu düzenleyen hükümlerden kaynaklanan yetkilerini kullanırken, bir kimsenin kişilik hakkına ihlal ederlerse, sahip oldukları yetki hukuka aykırılığı ortadan kaldırır (Dural 1995).

Umumi Hıfzıssıhha Kanunu'nun 57, 97, 104, 113 ve 114. maddeleri bulaşıcı hastalıkların ihbarını öngörmektedir. Bu kanunda olduğu gibi toplum sağlığını tehlikeye düşüren belirli hastalıkların açıklanmasını zorunludur (Hancı 2006). İlgili maddeler uyarınca ihbarı zorunlu bulaşıcı hastalıkları bildirme yükümlülüğü hukuka aykırılığı oradan kaldırır (Sert 2008). Aynı kanunun 282. maddesine göre, kanundaki zorunluluklara uymayanlar hakkında, kanunda ayrıca bir ceza hükmü gösterilmediği ve fiilleri Türk Ceza Kanununda daha ağır bir cezayı gerektirmediği takdirde, idari yaptırım uygulanacaktır. Ayrıca, fiilin işleniş şekli ve niteliğine göre failin suça vasıta kıldığı meslek ve sanatın yedi günden üç aya kadar tatiline aynı süre kadar işyerinin kapatılmasına da hükmedilebilir.

Umumi Hıfzıssıhha Kanunu'nda düzenlenmeyen bazı hastalıklar da Sağlık Bakanı onayıyla bu listeye eklenebilmektedir. Örneğin AIDS hastalığı da 07.10.1985 tarih ve 3765 sayılı bakanlık makamı onayı ile ihbarı mecburi hastalıklar arasına alınmıştır (Hakeri 2007).

Örneğin Avusturya'da 1986 tarihli bir AIDS Yasasına göre; hastanın isminin açıklanması konusunda hekim için bir yükümlülük getirmemektedir. Zorunluluk sadece hastalığa ilişkin ölüm vakaları söz konusu olduğunda hastanın ad ve soyadının sadece baş harfleri, doğum tarihi, hastanın cinsiyetine ve önemli klinik verilere ilişkin bilgiler içermektedir. Almanya'da ise 2001 yılında bazı enfeksiyonlar için Enfeksiyonlara Karşı Koruma Kanunu çıkartılmıştır. Bu kanunda yine Avusturya'da olduğu gibi anonim bir bildirim yükümlülüğü getirilmiştir. Sadece, hepatit gibi bazı virüsler söz konusu olduğunda istisnalara yer verilmiştir. Hepatit gibi bazı tehlikeli virüsler söz konusu olduğunda, hastanın isminin bildirilmesi mümkündür. Bunun dışındaki durumlarda hastanın ismi gizli tutulur. Bildirim, hekim

tarafından yerel Sağlık Müdürlüğüne ve Berlin'deki Robert Koh Enstitüsü'ne yapılır. Buradaki amaç hastaya gerekli yardımın yapılmasını sağlamak, enstitüye yapılan bildirimin amacı ise AIDS hastalarının sayısına ilişkin ülke genelinde bilgilere ulaşabilmektir (Erdem 2004).

Bildirimler ile ilgili ülkemizde Ceza Muhakemesi Kanunu'nun 159/1. maddesi bir bildirim yükümlülüğünü öngörmektedir. Bu hükme göre, bir ölümün doğal nedenlerden meydana gelmediği kuşkusunu doğuracak bir durumun varlığı *veya* ölünün kimliğinin belirlenememesi halinde, sağlık veya cenaze işleriyle görevli kişiler, durumu derhal Cumhuriyet Başsavcılığına bildirmekle yükümlüdürler.

Yine Ceza Muhakemesi Kanunu 87. maddesine göre, ölümünden hemen önceki hastalığında öleni tedavi etmiş olan hekimin otopsi sırasında hazır bulunması ve hastalığın seyri hakkında bilgi vermesinin istenebileceği öngörüldüğünden, bu durumda hekimin hastalığın seyri hakkında verdiği bilgiler hukuka aykırı olmayacaktır.

Ayrıca, CMK m. 161/4 gereğince; kamu görevlileri bakımından yürütülmekte olan soruşturma kapsamında ihtiyaç duyulan bilgi ve belgeleri talep eden Cumhuriyet savcısına vakit geçirmeksizin temin etmek yükümlülüğü bulunmakta olup, konu hakkında bilgilendirme de hukuka aykırılık taşımayacaktır. Burada sadece kamu görevlilerine yönelik bilgiler düzenleme kapsamındadır. Fakat CMK m. 332/1'de gerek suçların soruşturma gerekse kovuşturması sırasında, Cumhuriyet Savcısı, hâkim veya mahkeme tarafından yazılı olarak istenen bilgilere on gün içinde cevap verme zorunluluğu öngörüldüğünden; Cumhuriyet Savcısı, hakim veya mahkemenin talebi karşısında, kamu veya özel sağlık kurumları ve burada görevli sağlık görevlileri, ceza soruşturması ve kovuşturması ile ilgili hastanın kişisel verilerine ilişkin açıklamalarından dolayı TCK'nin 136. maddesinde yer alan "verileri hukuka aykırı olarak verme" suçundan dolayı sorumlu tutulmayacaktır (Yokuş 2008).

Özel Hastaneler Tüzüğü'nün 32. maddesi de güvenlik makamlarına bildirme mecburiyetini düzenlemektedir. Durumundan kuşku duyulan ve kimliği belli olmayan hastalarla, adli olaylar güvenlik makamlarına derhal bildirilecektir. Aynı tüzüğün 40. maddesinde de, "bildirilmesi zorunlu hastalığa yakalanmış olanlardan

iyileşmeden çıkanlarla, bulaşıcı hastalık taşıyıcıları ile gidecekleri yerler, sorumlu müdürlerce ilgili makamlara bildirilir" hükmü yer almaktadır.

Aynı doğrultuda Yataklı Tedavi Kurumları İşletme Yönetmeliği'nin 86. maddesinde de "adli ihbar işlemleri" düzenlenmiştir. Buralarda muayene ve tedavi edilen vakaların, Türk Ceza Kanunundaki ilgili maddenin müstesna kıldığı haller dışında gecikmeksizin Cumhuriyet Başsavcılığına haber verilmesi zorunludur.

Kişisel ve özel nitelikteki bilgiler hariç olmak üzere Devlet İstatistik Enstitüsünün, DİE Kanunu uyarınca istatistikî ya da toplum sağlığına yönelik hususlar hakkında hasta kayıtlarını isteme imkânı vardır.

İsveç'te, Anne-Marie Andersson, psikiyatrisi tarafından Sosyal Hizmetler Kurumu'na bilgisi ve rızası olmaksızın kişisel verilerinin açıklanmasının 8. maddede garanti edilen özel hayatın gizliliğini ihlal ettiği iddiasıyla 11 Şubat 1992'de AİHM komisyonuna başvurmuştur. Buna göre; başvurucunun psikiyatrisi tarafından hastanın oğlu hakkında Sosyal Hizmetler Kurumunca koruma tedbiri alınmasını sağlamak üzere yaptığı bildirimin hak ihlali olduğu savunulmuştur. Fakat Komisyon başvurucunun verilerin açıklanmasının özel hayata saygı hakkına müdahale olduğu konusundaki şikâyetini, İsveç Sosyal Hizmetler Kanununda "sağlık ve ahlak" ile "başkalarının hak ve özgürlüklerini koruma" meşru amacına uygun bulmuştur. Komisyon, başvurucuya daha önce önlem hakkında bilgi verildiğini ve söz konusu bilginin kamuya açıklanmadığını ve gizliliğine uyulduğunu tespit etmiştir. Başvurucunun iddiasının aksine Sosyal Hizmetlerin müdahalenin gerekliliğini değerlendirirken sadece oğlu hakkında değil, kendisi hakkında da bilgi sahibi olması gerekmektedir. Psikiyatrisin, sosyal hizmetlerin soruşturmasında hangi verinin önem taşıdığını değerlendirme konusunda geniş bir takdir yetkisine sahip olup, ilgiliyi sosyal hizmetlere bilgi verilmeden önce haberdar etme yükümlülüğü bulunmamaktadır. Komisyon bu nedenlerle, tıbbi verilerinin açıklanması hususunun sözleşmenin 8. maddesinin ihlali hususundaki iddiayı kabul edilebilir bulmamıştır (Yokuş 2008).

Kişisel verilerin korunması hakkında kanun tasarısı ve bu tasarının dayanağı niteliğindeki sözleşme ve kanunlara bakıldığında ise Türkiye'de 1995 yılından itibaren konu üzerinde durulmasına rağmen henüz bir yasa çıkarılamamıştır. Çalışmalar sadece yasa maddeleri şeklinde düzenlenip yürürlüğe konmamıştır. Diğer

bir açıdan ise yapılan düzenlemeler Anayasa ile ilişkilendirilmesiyle birlikte kişisel verilerin korunması konusuna temel atılmış ve bu durum pozitif bir gelişme olarak değerlendirilebilir (Dülger 2015).

Bireylerin kişilik haklarının korunmasına ilişkin kişisel nitelikteki verilerin otomatik işleme tabi tutulması hakkında kanun tasarısını hazırlamak için ilk komisyon 14 Eylül 1995 tarihinde kurulmuştur (Sert 2008). Ancak bu komisyon çalışmalarını tamamlayamamış, 18 Eylül 2000 tarihinde tekrar oluşturulmuştur. Neticede burada meydana gelen "Kişisel Verilerin Korunması Hakkında Kanun Tasarısı" bakanlıklar ile ilgili kamu kurum ve kuruluşlarının görüşlerine gönderilmiş, en son 09.11.2005 tarihinde Başbakanlığa sevk edilmiş, ancak hala kanunlaşmamıştır.

28 Ocak 1981 tarihinde ülkemizin de imzaladığı Kişisel Nitelikli Verilerin Otomatik İşleme Tabi Tutulması Karşısında Kişilerin Korunmasına Dair 28 Ocak 1981 Tarihli Avrupa Konseyi (Strasbourg) 108. No.lu Sözleşmesi ve Kişisel Verilerin İşlenmesinde Gerçek Kişilerin Korunması Yönergesi, konuyla ilgili kanun tasarısını dayanağını teşkil etmektedir (Başalp 2004).

2.1.3.5. Kişisel Nitelikli Verilerin Otomatik İşleme Tabi Tutulması

Yukarıdaki sözleşmenin kapsamı izah edilirken; sözleşmede korunacağı taahhüt edilen kişisel bilgilerin, belirli bir kişiye ilişkin olan veya belirli bir kişiye ilişkin olduğu belirlenebilen bütün bilgiler olduğu, kişinin özel, toplumsal ve resmi yaşamına, ailesine, öğrenimine, işine, görevine vb. ilişkin bilgilerin bu kapsamda olduğu, bu bilgilerden kişinin inancı, sağlığı, cinsel yaşamı, etnik kökeni, dini, siyasal görüşlerine ilişkin bilgilerin özel nitelikleri dolayısıyla "duyarlı" bilgiler olarak daha ciddi koruma önlemlerine tabi tutulması, toplanan verilerin doğruluğunun kontrol edilmesi, bunun verilerin toplanış amacı ve temel hak özgürlüklere aykırı olmaması, toplanma amacının hangi amaçla olduğunun başlangıçta tüm ilgililere bildirilmesi, kişinin kimliğini kanıtlamak koşulu ile kendi kişisel verileri hakkında ne tür işlemlerin yapıldığı, istemesi halinde ve bir örneğin kendisine temin edilmesi, bu prensipleri terk etme hakkının sadece temel hak ve özgürlüklere uygun olmak kaydı ve ulusal güvenlik, kamu düzeni, halk sağlığı koruması amaçları ile ilgili kamu görevlilerine verilebileceği, aynı çerçevede istatistiki veya bilimsel amaçlara hizmet eden durumlarda kişilik hakkının ihlal

edilmemesi koşulu ile bu verilerin korunmasına sınırlandırma getirebileceği konuları düzenlenmiştir.

Sözleşme'nin giriş kısmında özetle, Avrupa Konseyi'nin hedefinin, her şeyden önce insan hakları ve temel hakların ön planda olduğunun bilincinde olarak, üye ülkeler arasında sıkı ilişkileri gerçekleştirmek olduğunu, giderek yaygınlaşan sınır aşırı otomatik işleme tabi tutulan kişisel veri trafiği karşısında, her insanın hakları ve temel özgürlüklerinin korunması, her şeyden evvel kişilik alanına dikkat edilmesi, aynı zamanda Devletlerin sınırlarıyla kayıtlı olmaksızın bilgilenme özgürlüğünün güçlendirilmesi gerektiği ve kişilik alanın dikkate alınması ve halklar arasındaki özgür bilgi değişimi temel değerlerinin hayata geçirilmesinin kabulü vurgulanmıştır.

Sözleşmenin 10. maddesi taraf devletlere, iç hukuk mevzuatında, Sözleşmede yer alan veri korunmasına ilişkin ilkelerin yerine getirilmesi için gerekli yaptırımları ve hukuksal araçları oluşturmak yükümlülüğü getirmekte; 13. Madde ise taraf devletlere sözleşmenin hayata geçirilmesi, ihlallerin önlenmesi ve verilerin korunması hususunda, mevzuat ve uygulamayı geliştirmek için işbirliği ve karşılıklı yardım yükümlülüğünü getirir (conventions.coe.int).

2.1.3.6. Hasta Bilgilerinin Gizliliği Prensibinin İhlalinin Sonuçları

Ceza hukuku yönünden incelendiğinde hekimlik mesleği diğer mesleklerden farklı olarak kişilerin özel hayatları ile ilgili olabilmektedir. Dolayısıyla bu özel bilgilerin saklanması kişilerin özel hayatlarının gizliliği hususunda önem arz etmektedir. Bu bilgilerin üçüncü şahıslarla paylaşılması hekimin hukuki yaptırımlara maruz kalmasına neden olabilir.

Bu çerçevede, bazı ceza kanunlarında da hekimin sorumlulukları ilgili kurallar bulunmakla birlikte, hekim ile ilgili tıp mesleğini ifa ederken işleyebileceği çeşitli suçlar, genellikle sağlık kanunlarında düzenlenir. Fakat çeşitli ülkelerin ceza kanunlarında hekimin durumu mahiyetleri icabı hekimler tarafından daha kolaylıkla işlenebilen bazı suçlarla ilgili ayrıca düzenlemelere de rastlanmaktadır (Bayraktar 1972).

Konuyla ilgili 5237 sayılı Türk Ceza Kanunu'nda hekimlerin cezai sorumluluğu olabilecek belli başlı maddeler;

● Özel Hayatın Gizliliğini İhlal 134. Madde;

(1) Kişilerin özel hayatının gizliliğini ihlâl eden kimse, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır. Gizliliğin görüntü veya seslerin kayda alınması suretiyle ihlâl edilmesi halinde, cezanın alt sınırı bir yıldan az olamaz.

(2) Kişilerin özel hayatına ilişkin görüntü veya sesleri ifşa eden kimse, bir yıldan üç yıla kadar hapis cezası ile cezalandırılır. Fiilin basın ve yayın yoluyla işlenmesi halinde, ceza yarı oranında artırılır.

Hüküm ile gerekçede, başkaları tarafından görülmesi mümkün olmayan bir özel yaşam olayının gizli yaşam alanına girerek veya başka suretle saptanması ve kaydedilmesinin cezalandırılmasının amaçlandığı ifade edilmektedir (Meran 2004).

"Özel hayat" kişinin kendine özgü yaşayışı, yaşam tarzı, kendisini ilgilendiren tutum ve davranışları kapsayıp, bunun ihlali, bu mahremiyeti bozmak, sakatlamak ve zarara uğratmaktır. Bir kimsenin evinin gizlice gözetlenmesi bu suç için örnektir (Arslan 2004).

Özel hayatın mahremiyetine dair gizlilik hakkı birçok hukuki sözleşmede de vurgulandığı üzere en temel insani haklardandır. Başkaları tarafından bilinmesi halinde kişinin moral değerlerini bozacak bilgilerin üçüncü şahıslarla paylaşılması bu hakkın ihlalini oluşturmaktadır (Parlar ve Hatipoğlu 2008). Özel hayatın korunmasına yönelik uluslararası düzenlemelere örnek olarak 04.11.1948 tarihli Avrupa İnsan Hakları ve Ana Hürriyetlerini Korumaya Dair Sözleşme (m.8), 10.12.1948 tarihli BM İnsan Hakları Evrensel Beyannamesi (m.12), 16.11.1966 tarihli Medeni ve Siyasal İlişkin Milletlerarası Sözleşme (m.17), BM'in 1989 tarihli Çocuk Haklarına Dair Sözleşmesi (m.11), Avrupa Konseyi'nin 1993 tarihli Avrupa Sınır Ötesi Televizyon Sözleşmesi (m.7) gösterilebilir. Bu düzenlemeler vasıtasıyla özel hayatın gizliliği, insan hak ve hürriyetlerinin kapsamına dâhil olmuştur (Özbek 2008).

İnsanların özel hayatlarının çeşitli şekillerle izlenmeye çalışılması ya da kaydedilmesi suç olarak tanımlanmış hatta bu durum ağırlaştırıcı neden olarak vurgulanmıştır. Kişinin başkalarının görmesini ve bilmesini istemediği, özel alanlarında geçen faaliyetlerinin izinsiz görüntülenmesi ayrı, ifşa edilmesi ayrı suçlar

olarak belirlenmiştir. Ayrıca kişinin bu gizli alanına girilmesi ve rahatsız edilmesi de bu suç kapsamındadır (Malkoç 2007).

Birinci fıkradaki suçun unsuru failin başka bir kişinin yaşam alanına girerek veya başka suretle başkaları tarafından görülmesi mümkün olmayan bir özel yaşam olayını saptaması ve kaydetmesidir. Dolayısıyla özel yaşamın gizliliğine müdahale oluşturan her türlü davranış bu suçu oluşturur. İkinci fıkradaki suçun maddi unsuru ise bu görüntü veya seslerin ifşa edilmesidir. Ancak, ifşa eyleminden söz edilebilmesi için, yalnızca ses veya görüntülerin değil bunun ilgili olduğu kişi veya kişilerin de açıklaması gerekir. Bu ifşa, açık veya örtülü, yazılı veya sözlü olabilir. Ses veya görüntülerin bir kişiye açıklanması dahi yeterlidir (Parlar ve Hatipoğlu 2008).

Bu bağlamda, bir hekimin meslek icabı öğrendiği bir sırrın gizliliğini bozmaması gerekmektedir. Eğer, hekim sırrı hukuka uygun bir neden olmaksızın başkalarına bildirecek olursa, özel hayatın gizliliğini ihlal etmiş olur. Doktoruna eşcinsel olduğunu söyleyen bir danışanın bilgilerinin doktor tarafından gizli tutulmalıdır. Doktor bu bilgiyi paylaştığında gizliliği ihlal etmiş demektir. Bununla birlikte bu bilginin paylaşımı kişiyi toplum içerisinde küçük düşürmesine bakılmaksızın ihlal yapılmış demektir. Bu bağlamda önemli olan ilgili bilginin saklı tutulmasıdır (Şen 2006).

Rıza, şahıs tarafından belirli bir konuda hukuka aykırı davranışa yetki verilmesidir. Kişinin rıza göstermesi ile birlikte, açık olarak belirli bir eylemin işlenebileceğine izin vermiş sayılacaktır. Bu rıza beyanının açık olması şart olmayıp, beyan zımni de olabilir. Dolayısıyla, sırrın açıklanmasına rıza gösterildiği takdirde, YTCK' nin 26/2. maddesinde düzenlenen "mağdurun rızası" adlı hukuka uygunluk sebebi gündeme gelir. Bu sebeple, failin rıza beyanı sınırları içerisinde hareket etmesi koşulu ile fiil suç teşkil etmeyecektir. Ayrıca rıza beyanında bulunacak kişinin bu beyanı vermeye yetkili olması gerekmektedir. Rıza beyanının geçerli olabilmesi, rızanın konusunun mağdur yönünden tasarruf edilebilir nitelikte olmasıyla ilintilidir (Donay 1978).

Örneğin hekim hastanın beyanı yahut kendi incelemesi sonucu hastada AIDS hastalığının bulunduğunu öğrense normalde sır niteliği taşıyan bu hususun başkalarına açıklanmaması gerekir. Ancak hekimin bir görevi de bu tarz toplum

sağlığını olumsuz etkileyebilecek bulaşıcı hastalıkların yayılmasını önlemek olduğundan, özel hayatın gizliliğini ihlal etmek veya hakaret etmek amacı taşımayacak şekilde hastalığın kanunda belirtilen yetkililere haber verilmesi ya da örneğin AIDS hastasının yanına gelen eşine mağdurun hastalığı hakkında bilgi verilmesi hukuka aykırılık taşımayacaktır (Şen 2006).

TCK'nin 134. maddesinde tanımlanan bu suçun manevi unsuru bakımından genel kast yeterlidir. Suçun olası kastla işlenmesi de mümkündür. Failin suçu hangi saikle işlediği önem taşımaz. Suçun taksirle işlenmesi mümkün değildir (Özbek 2008).

Adli Yargı İlk Derece Mahkemeleri ile Bölge Adliye Mahkemelerinin Kuruluş Görev ve Yetkileri Hakkında Kanun'un 10. maddesi uyarınca bu suçlar dolayısıyla açılan davalara bakma görevi sulh ceza mahkemesine aittir. Ayrıca TCK'nın 66/1-e bendi uyarınca, bu suçun zaman aşımı süresi 8 yıldır.

● Kişisel Verilerin Kaydedilmesi 135. Madde;

(1) Hukuka aykırı olarak kişisel verileri kaydeden kimseye altı aydan üç yıla kadar hapis cezası verilir.

(2) Kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerine; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgileri kişisel veri olarak kaydeden kimse, yukarıdaki fıkra hükmüne göre cezalandırılır. Burada kastedilen "gerçek kişiyle ilgili her türlü bilgi" nin kapsama girdiği verilerdir (Meran 2004).

Kişisel verileri bir hastalık dolayısıyla hekim veya diğer sağlık personeli tarafından gerçek kişilere ilişkin edinilen her türlü bilgi olarak kabul edebiliriz. Hastaya ait olup hekim veya diğer sağlık personelinin hukuka uygun olarak öğrendiği ama hastanın başkaları tarafından duyulmasının istenmeyeceği bilgiler kişisel veri olarak kabul edilir. Kişisel verilere sadece sağlık personeline aktarılan değil, hastanın kimliği ve adresi, kişinin bir hekimi, hastaneyi vs. ziyaret etmesinden kaynaklanan kayıtlar, teşhis, tedavi, hastalığın türü, psikolojik belirtiler, hastanın öyküsü, bedeni eksiklikler ve özellikler, hasta dosyası, röntgen filmleri, muayene sonuçları ile kişisel, ailevi, mesleki, ekonomik duruma ilişkin bütün veriler kişisel veri olarak değerlendirilir (Hakeri 2007).

Maddenin gerekçesinde ise açıkça, hastanelerde hastalara veya sigorta şirketlerinde sigortalılara ilişkin kayıtların bilgisayar ortamına geçirilip muhafaza edildiği ve bu bilgilerin amaçları dışında kullanılmasından veya herhangi bir şekilde üçüncü kişilerin eline geçerek hukuka aykırı olarak yararlanılmasından dolayı hakkında bilgi toplanan kişilerin büyük zararlara uğrayabileceği ve bu bakımdan da kişilerle ilgili bilgilerin hukuka aykırı olarak kayda alınmasının suç olduğu ifade edilmiştir (Meran 2004).

Kişisel verilerin hukuka aykırı olarak kaydedilmesi suçun oluşması için yeterlidir. Dolayısıyla suçun maddi unsuru, hukuka aykırı olarak başkasına ait kişisel verileri kaydetmektir. Hakkında bilgi toplanan kişiler açısından bu fiil, bilgilerin amaçları dışında kullanılması veya herhangi bir şekilde üçüncü şahısların eline geçerek bunlardan hukuka aykırı olarak yararlanılması ve kişinin bu suretle büyük zararlara uğratılması tehlikesini taşımaktadır. Suçun oluşması için kişinin bu nedenle zarara uğramış olması aranmamaktadır. Buna örnek olarak; hastanede hastalara, bankalarda ve kredili alışveriş yapılan mağazalarda müşterilere, sigorta şirketlerinde sigortalılara ilişkin kişisel veriler hukuka aykırı olarak toplanıp bilgisayar ortamlarında veya kâğıt üzerinde veya başka herhangi bir yöntemle kaydedilmişse söz konusu suç oluşmuş olur.

Maddenin 2. fıkrasında tanımlanan suçun maddi unsuru, "kişilerin siyasi, felsefi veya dini görüşlerine, ırki kökenlerinde; hukuka aykırı olarak ahlaki eğilimlerine, cinsel yaşamlarına, sağlık durumlarına veya sendikal bağlantılarına ilişkin bilgilerin kişisel veri olarak kaydedilmesi" olarak tanımlanmıştır.

2. fıkrada sayılan hususların tümü değil bunlardan sadece bir veya birkaçının kişisel veri olarak kaydedilmesi suçun oluşması bakımından yeterlidir. Tanımda, kişisel verilerin bilgisayar ortamında veya kâğıt üzerinde veya başka herhangi bir yöntemle kayda alınması arasında bir ayrım yoktur. Suçun oluşabilmesi için kaydın, hukuka aykırı olarak alınması gerekmektedir yani kişisel verilerin kaydedilmesi için hukuka uygunluk hali mevcut ise suç oluşmayacaktır. Nitekim maddenin gerekçesinde de, çeşitli kamu kurumlarında kanun hükmünün gereği olarak kişisel verilerin kamu hizmetinin neticesi olarak kişilerle ilgili bazı bilgilerin ilgili kanun hükümlerine istinaden kayıt altına alındığı dolayısıyla kişinin rızası ile kendisi

hakkında bilgilerin kayda alınmasının suç oluşturmayacağı vurgulanmış (Parlar ve Hatipoğlu 2008).

Kişisel Verilerin Korunması Hakkında Kanun Tasarısı'nın 6. maddesinde de hukuka uygunluk sebepleri düzenlenmiştir. Buna göre;

(1) Kişisel veriler ancak ilgili kişinin açık rızasıyla işlenebilir.

(2) Kanunlarda öngörülen yükümlülüklerin yerine getirilmesi dışında, ilgili kişinin bir itirazda bulunması halinde veri işlenemez.

(3) Aşağıdaki hallerde de hukuka uygunluk sebeplerinin bulunduğu kabul edilir:

a) Kanunun öngördüğü bir zorunluluk dolayısıyla, kamu yararına veya resmi olarak verilmiş bir görevin yerine getirilmesi amacıyla veri işlenmesi,

b) Kişisel verilerin, ilgili kişinin rızasını açıklayamayacak durumda olması hâlinde kendisinin veya başkasının hayatını veya beden bütünlüğünü korumak amacıyla işlenmesi,

c) Bir sözleşmenin kurulması ve ifasıyla doğrudan doğruya ilgili olması kaydıyla, sözleşmenin taraflarına ait kişisel verilerin işlenmesi,

ç) İlgili kişiler tarafından açıklanmış olması veya açık sicillerde mevcut bilgiler olması sebebiyle herkesçe bilinen kişisel verilerin işlenmesi,

d) Veri kütüğü sahibinin kendi haklı çıkarları için, ilgili kişinin temel hak ve özgürlükleri ile meşru çıkarlarına zarar vermediği sürece, veri işlemesinin zorunlu olması."

Maddede tanımlanan suçların manevi unsuru genel kasttır. Bu suçların taksirle işlenmesi mümkün değildir (Özbek 2008).

2.1.3.7. Verileri Hukuka Aykırı Olarak Verme\Ele Geçirme

Madde 136 - Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.

Bu madde ile hukuka uygun olarak kaydedilmiş olsun veya olmasın, kişisel verileri hukuka aykırı olarak başkalarına vermek, yaymak veya ele geçirmek bağımsız bir suç olarak tespit edilmiştir (Meran 2004).

Bir önceki maddede de izah edildiği gibi kişisel verilerin hukuka aykırı elde edilmesi suçunun yanında bundan farklı olarak kurum ve kuruluşların bilgisayar ortamlarında saklanan kişisel verilerin, bir hastanenin hastalarına, sigorta şirketinin sigortalılarına, bankaların müşterilerine ilişkin kişisel veri kapsamındaki kayıtların hukuka aykırı olarak bir başkasına verilmesi, yayılması veya ele geçirilmesi gibi hallerin de söz konusu maddeye uyan suçu oluşturduğu açıktır. Bu bağlamda örneğin evlilik, birlikte çalışma gibi sebeplerle ortak elektronik posta kullananlar, birliktelik bittikten sonra verileri izinsiz açıklayamazlar (Malkoç 2007; Parlar ve Hatipoğlu 2008).

Halen yasalaşma süreci bitmeyen Kişisel Verilerin Korunması Hakkında Kanun Tasarısının "kişisel verilerin üçüncü kişilere aktarılması" başlıklı 8. maddesinden itibaren, kişisel verilerin kimlere ve nasıl aktarılacağı açıkça düzenlenmiş olup, tasarının kanunlaşması halinde, burada belirtilen usullere aykırı olarak kişisel verilerin başkasına verilmesi, yayılması veya ele geçirilmesi suç kabul edilecektir.

Ayrıca CMK' nın 46/1-b maddesi uyarınca, hekimler, diş hekimleri, eczacılar, ebeler ve bunların yardımcıları ve diğer bütün tıp meslek veya sanatları mensuplarının, bu sıfatları dolayısıyla "hastaları ve bunların yakınları hakkında öğrendikleri bilgiler" dolayısıyla tanıklıktan çekinme hakları vardır (Hakeri 2007).

Tanıklıktan çekinme sayesinde meslek sahibinin mesleğini yürüttüğü esnada öğrendiği sır niteliği taşıyan bilgilerin meslek sahibi tarafından hiçbir kimse ya da kurum önünde açıklanmaması sağlanır. Çünkü yargılamanın açık yapıldığı durumlarda hekimin öğrendiği sırlarla ilgili tanıklık yapması halinde sır sahibine ait gizli bilgiler herkesçe bilinebilecek bir duruma gelmektedir. Bu sebeple, genel olarak hekimlerin tanıklıktan çekinebilecekleri öngörülmektedir (Donay 1978).

CMK madde 46/1-b'ye göre tanıklıktan çekinme yetkisinin temelinde güven ilişkisi bulunmaktadır. Şöyle ki; bu hak sadece güven verdikleri halde hizmet verebilecek meslek mensuplarına tanınmıştır. Orantılık ilkesi gereği maddi gerçeğin

ortaya çıkarılması ile güven ilişkisi karşılaştırıldığında güven ilişkisi ağır bastığından bu meslek mensuplarına tanıklıktan çekinme yetkisi verilmiştir. Ancak, aynı maddenin 2. fıkrasına göre ise avukatlar, stajyerleri veya yardımcılarının sır sahibinin onamı olsa bile tanıklıktan çekinebilecekken, içine sağlık mesleği mensuplarının da dâhil olduğu diğer meslek mensupları sır sahibinin talebi olması halinde tanıklıktan çekinemeyeceklerdir. Bununla beraber Yeni Kanun tasarısında önceki düzenlemeye göre sağlık mesleği mensuplarının tanıklıktan çekinmesi konusunda daha açıklayıcı ve genişletici bir ifade kullanılması hasta hakları açısından daha olumlu bir sonuç meydana getirecektir (Sert 2008).

2.2. Bilgi Sistemleri ve Güvenliği

Bilgi, kavram olarak "informare" kökünden gelmektedir. Latince' de bir şeye biçim vermek anlamındadır (Floridi 2010). Bilginin ortaya çıkış, bir şey ile etkileşim sonucu anlam kazanmasıdır. Gerçekliğin insan aklı ile harmanlanarak bir olgunun elde edilmesi, anlamları simgeleştirerek kolaylık sağlayan kodlardır (Argyris 1993).

2.2.1.2. Bilgi Sistemi

Bilgi sistemi, girdi şeklinde veri kaynaklarını alan ve belirli bir süreçten geçirip bilgi ürünleri çıktı şeklinde veren sistemdir. Bu sistemde veri bilgiye dönüştürülürken, yani; girdi, süreç, çıktı, saklama ve kontrol faaliyetleri yerine getirilirken kaynak olarak insan, donanımı, yazılım, şebeke ve veri kullanır. Bilgi sürecinde kullanılan bütün fiziksel araç ve malzemeler donanım kapsamındadır. Donanım ayrıca bilgisayar, hesap makinesi, verilerin kaydedildiği kağıtlar, manyetik diskler vb. veri ortamlarını da kapsar. Tüm bilgi işlem komutları da yazılımı içermektedir. Yazılım kavramı ile sadece bilgisayar donanımını kontrol eden ve yönlendiren, işletim talimatları kümesinden oluşan programlardan değil, aynı zamanda insanların gereksinimi olan bilgi işleme komutları kümesi denilen yöntemlerden de söz edilmektedir. Yazılım, bilgi üretim sürecinde kullanılacak donanımın kullanma talimatı olarak tanımlanabilir (Kavuncubaşı 2000).

Bilgi sisteminin temel öğesi olmaktan daha fazla anlam taşıyan Veri kavramı, rakam, harf ve diğer özel şekillerden oluşarak sayısal değerler olabileceği gibi cümle ve paragraflardan oluşan metin ve resim de olabilir. Genellikle veri, veri tabanlarında ve bilgi sistemlerinde işlenmiş ve organize edilmiş şekilde bulunur. Bu şekilde

istenildiğinde tüm verilere rahatlıkla ulaşılabilir. Bilgi sistemleri her mevcut olduğu sistemin doğal bir alt sistemidir. Mevcut bulunduğu organizasyonun amaçlarına yardımcı olacak her türlü veriyi toplar, bu verileri işleyip ve anlam kazandırır (süreç) ve yine ürettiği (çıktı) bilgiyi üst sisteme iletir (Kağnıcıoğlu 2005).

İnsan sadece yazılım ve donanımdan meydana gelmiş gibi görülen bilgi sistemlerinin aslında en önemli bileşenidir. Bilgi sistemleri, üç köşesinde üç bileşeni bulunan bir üçgen şeklindedir denebilir. Aslında üçgendeki girdi ve çıktı (donanım), süreç (yazılım) en önem olduğu kabul edilen bileşenlerdir. Bu ikisi normalde bilişime ait kavramlardır dolayısıyla sistem döngüsü bileşeni kullanılmadan sadece geri bildirim ile sonlandırılırsa, bu bilişime ait bir sistem olur. Bunlardan farklı olarak bilgi sistemi ise insan boyutunun sisteme katılması ile farklı boyut kazanır (Wirken 2012). Bu süreçte, toplanan veriler ancak anlamlandırılarak kullanılabilir hale gelir (Mole 2006).

Organizasyonel problem çözme sürecinin bir sonucu olan yeni bilgi sistemleri faaliyet alanı ve amaçları ne olursa olsun fark etmemektedir. Yeni bir bilgi sistemi örgütün karşılaştığı problemlerin türüne göre çözüm üretme amacındadır. Bu problemler ise ya yönetici ve çalışanların, organizasyonun beklenen performansı göstermediğini fark ettiklerinde ya da yeni fırsatların değerlendirilmesi huşunda ortaya çıkar. Sistem geliştirme, organizasyon ile ilgili yenilikler elde edebilmek ya da örgütsel bir sorunu çözmek için, bir çeşit bilgi sistemi kullanılarak çözüm üreten eylemlere denir (Turkish Ministry of Health 2006).

2.2.1.3. Bilgi Sistemlerinin Sınıflandırılması

Bilgi teknolojilerinin gelişimine bağlı olarak ilerleme gösteren işletme bilgi sistemleri; veri işleme, ofis otomasyon, karar destek, yönetim bilgi, üst yönetim bilgi sistemleri olmak üzere 5 ana başlıkta ifade edilebilir (Lucas 1990; Kağnıcıoğlu 2005).

2.2.1.4. Veri İşleme Sistemleri

Verilerin anlamsal boyutta değerlendirilmesini kolaylaştırmak için belli bir süreç içerisinden geçirilerek elde edilen bilgileri sağlayan bir unsurdur. Sistem çalışmaların yanında temel ögeleriyle birlikte koordineli şekilde desteklenmesidir.

Sistemin girdilerini, çıktılarını ve sürecini inceleyen dolayısıyla sistemin en temel ögesi olan insan tarafından gerçekleştirilir (Şahin 2003).

2.2.1.5. Ofis Otomasyon Sistemleri

Çalışanların verimliliğini artırmak amacı ile ofiste tasarlanmış olan elektronik takvim, elektronik posta, kelime işlemci, randevu, program ve planlama sistemi gibi unsurlardan meydana gelen sistemlerdir (Kağnıcıoğlu 2005). Faaliyetlerde etkinlik, verimlilik ve hız sağlayan; organizasyonlarda iletişimin sağlanmasını ve bilginin paylaşılmasını temin eden bir sistemdir. İşletmede elektronik posta, intranet ve video konferans uygulamaları, telefon, faks, ofis otomasyon sistemlerinin birkaç unsurunu oluşturan başlıktır. Bu başlığın diğer bazı unsurları da kelime işlem sistemleri, tablolama ve hesaplama sistemleri, masaüstü yayıncılık ve doküman görüntüleme sistemleridir (Lucas 1990).

2.2.1.6. Karar Destek Sistemleri

Karar destek sistemleri organizasyonun yönetim seviyesine hizmet sunan, yapısal ve yarı yapısal nitelikteki kararların verilmesinde yöneticilere destek veren, ileri düzeyde kolaylıkla tanımlanamayan, çabuk değişen sistemlerdir. Bu sistem hem klinik hem de yönetimsel amaçlı kullanılır. İşletme yöneticilerinin yönetimsel kararlar vermesinde onlara yardımcı olmak için çeşitli model ve araçları, veri tabanı aracılığı ile kullanıma sunar. Yöneticiler bu sistemlerden, karmaşık, stratejik ve nadiren karşılaşılan durumlar için kararların verilmesinde yararlanır (Kağnıcıoğlu 2005; Mumcu 2011).

2.2.1.7. Yönetim Bilgi Sistemleri

Yönetim bilgi sistemleri, eş zamanlı olarak organizasyonun güncel performansı ve eski kayıtlarına ulaşıp, ilgili örnekleri ve raporları yöneticilere sağlayarak, organizasyonun orta düzey yönetimine destek temin eden kısımdır.

Bu sistem özellikle, organizasyonun işlevlerine ait bilgileri planlayıcı, denetleyici ve düzeltici önleyici faaliyetlerde bulunabilmek için geliştirilmiş ve pazarlama, muhasebe, finans ve insan kaynakları çeşitli araçlar aracılığı ile yöneticilere sunan bir sistemdir. Temelde "Yönetim, Bilgi, Sistem" kavramlarından oluşan Yönetim bilgi sistemleri, yönetim ve bilginin birlikte ele alınarak belli bir

sistem içinde bütünleştirilmesi dayanmaktadır. İşletme yönetimi için gerekli olan anlamlı iç ve dış bilgilerin sağlanması ancak bu tarz bir bilgi sistemlerinin geliştirilmesi ve kullanılması ile olabilir (Kağnıcıoğlu 2005).

1960'lardan bu yana kullanılan bu sistem bilgisayar teknolojisinden en fazla yararı hedefler. Kurumun bilgi üretmekle eş zamanlı olarak yönetsel açıdan da dengeli kararlarını desteklemektedir. Ayrıca kuruma bağlı birimlerle birlikte bütünün devamlılığını sağlar (Şahin 2003).

2.2.1.8. Üst Yönetim Bilgi Sistemleri

İşletmenin misyonunu, vizyonunu, değerlerini ve stratejilerini belirleyen kişiler için organizasyonun stratejik düzeyine hizmet sunan bu sistem, genel müdür ve yönetim kurulu üyeleri gibi kişiler için oluşturulmaktadır. Üst yönetim bilgi sistemi iç ve dış çevre koşulları konusunda eksiksiz, doğru ve zamanında bilgilendirme yapmalıdır çünkü o düzeyde yapılacak hatalar işletmenin geleceğini riske sokabilir. Üst yönetim bilgi sistemleri ancak üst düzey yöneticiler tarafından verilebilecek; karmaşık, önceden programlanamayan, nadiren karşılaşılan, stratejik önem taşıyan kararlar için kullanılan bilgi sistemleridir (Lucas 1990).

2.2.2. Bilgi Yönetimi

Verinin bilgiye dönüşümü sağlandıktan sonra, geri bildirimler ile birlikte desteklenen yeni bilgi sürecin sonraki tüm basamaklarında yönetiminde kullanılır. Dolayısıyla bilginin yönetilmesi kavramı ortaya çıkar. Bilgi yönetimi; bilgi tanımlama, yaratma, paylaşma, depolama ve kullanma faaliyetlerini organize eden, organizasyonel hedeflere ulaşmak üzere en doğru kararları verme gibi organizasyonun tüm faaliyetlerinde, bilgiyi gereken zamanda ve gereken yerde kullanıma sunan bir süreç şeklinde tanımlanabilir. Doğru zamanda doğru kararlar verebilmek için, bilginin doğru kişiler ile paylaşılması, organizasyonel hedeflere ulaşmak için bilginin yaratılma, dağıtılma ve kullanım yönetimini kapsayıp, bilginin toplanması, oluşturulması, kullanılması ve paylaşılmasına olanak tanıyan, insanları, süreçleri, faaliyetleri ve teknolojiyi kapsar (Altındiş 2010).

Amaç; uygun iş sürecini geliştirmektir. Böylece bilginin organizasyon içinde hızla dağılması ve paylaşılması sağlanır, verimsizlik ve zaman kaybı önlenir, bilginin yönetilmesini, ayrıca iş birliği koşullarının belirlenmesini, işletme stratejileri ile

ilişkilendirmesini amaçlar. Burada sürekli değişim ve hareket halinde olan bilgilerin temel fonksiyonu, organizasyon hedeflerine ulaşmak üzere etkili bir şekilde hizmete sunulmaktır (Tengilimoğlu 2006).

"Üretken" bilgi, kurum için anlam taşıyan, işletme için yararlı olduğu anlaşılan bilgidir. Üretken bilginin elde edilmesi, paylaşılması, geliştirilmesi ve kullanılması ile ilgili olan bilgi yönetiminin işletme performansını artırmak amacı ile kurum amaçları ve gereksinimleri doğrultusunda ele alınması gerekmektedir. Burada temel hedef, bilgiyi üretken hale getirmektir. Düşünceler, öngörüler, yaşanan deneyimler, uygulama neticeleri ve öğrenilen dersler sonuncunda oluşan bilginin her zaman tamamı değil ama her zaman bir kısmı yararlıdır. Yönetilecek bilgi, yalnızca kurumun faaliyetleri neticesinde değerlendirilebilir. Kurumdaki bilginin üretilmesi sürecinde başlayan bilgi yönetimi, organizasyonlar için en temel unsurdur. Bu süreç bir işletmede hemen hemen bütün çalışanların katıldığı örgütsel bir aktivitedir. Bu nedenle bilgi yönetimi, bilgi paylaşımını, bilgi öğrenmeyi, bilgi teknolojilerini kullanmayı cesaretlendiren kurumsal bir kültüre ihtiyaç duyar. Dolayısıyla, öğrenen organizasyon kavramı ile bilgi yönetimi arasında önemli bir bağlantı vardır (Krogh 2007).

Günümüzde artık bilgi, bir organizasyon için mali kıymetler ne kadar önem taşıyorsa, en az o kadar önem arz eder hale gelmiştir. Bununla beraber küreselleşen dünyada, bilgiler, bilişim sektörünün artan gücüne paralel olarak giderek artan sayıda ve çeşitlilikte tehditlere maruz durumdadırlar. Bilgi güvenliği de işte bu noktada karşımıza çıkmaktadır.

Bilgi yönetiminin temel amaçları; organizasyon içinde yeni bilgi üretimi, örgütsel kararlarda ulaşılabilir bilginin kullanılmasının temini, daha hızlı bir öğrenme ile iyileştirme, doğru bilginin, doğru insanlara, doğru zamanda ulaştırılması, dış kaynaklardaki kıymetli bilginin kuruma kazanımı, bilgiyi dokümanlar, yazılımlar ve veri tabanları yardımıyla ile sunmak, oluşan bilgilerin örgütün birimleri ya da başka örgütlerdeki benzer birimler arasında transferini gerçekleştirme, kurumsal bilgiyi değerlendirilerek entellektüel sermayeye evrimini sağlamak ve ölçülmesini temin etmek olarak sıralanabilir (Zaim 2005).

Bilgi yönetimi bilginin; tanımlanması yaratılması, depolanması, paylaşılması ve kullanımı faaliyetlerinden oluşmaktadır. Bilginin tanımlanmasında;

organizasyonda mevcut kayıtlı veya potansiyel bilgi kaynaklarının belirlenmesi, çalışanların bilgilere erişiminin kolaylaştırılması, iş sürecine dâhil edilmesi sadece işletme içinde temel bilgi ihtiyaçları, yapısı, görsel sunumu ve bilginin nasıl karşılanacağının tanımlanması, bireylerin uzmanlık alanlarının tanımlanması gibi unsurları bulunan hedef bilginin tanımlanması ile mümkün olabilir. Bilginin yaratılması süreci; girişimin ilkelerinin ortaya konulması, araştırmalardan elde edilen çıktılar, belirli faktörler arasındaki yeni ilişkilerin tespit edilmesi veya bir vaka çalışması biçiminde gerçekleşebilir. Yaratma süreci ayrıca bir organizasyonun yeni fikirler ve çözüm yolları geliştirme yeteneği ile bağlantılıdır. Bir konu hakkında bazı sağlık kurumlarındaki tercihler ve uygulama esaslarını esas alan sağlık programları, bir araştırma süreci aracılığı ile belirli sağlık alanlarındaki tecrübeler, bir araştırma bulgusunun sentezi ya da belirli klinik vakalar ile ilgili tecrübelerin toplanması vb. yollarla bilgi yaratılabilir. Bilginin depolanması, bilginin türüne, kullanım amacı ve organizasyonun hedeflerine uygun olarak tasnif edilmesi, çalışanların istenildiği zamanda erişimine olanak verecek şekilde saklanmasıdır. Bu faaliyet ile bilgiye istenildiğinde tekrar ulaşmanın da yolu açılmakla beraber bilginin değerlendirilmesi sürecine de ayrı bir katkı sağlayacağı ortadadır. Bilginin paylaşılması, belirli bir amaç çevresinde bir araya gelen kişilerin oluşturduğu gruba yönelik, onların bilgi kaynaklarını, görüşlerini, tecrübelerini paylaşma ortamı sağlayıp, bu eylemleri sistematik olarak yönetip planlayan bir aktivite olarak tanımlanabilir. Bilginin kullanımı; bilginin oluşturulması, paylaşılması ve depolanması için referans noktasıdır. Her bilgi mutlaka kısa vadede bir sorunun çözümüne ya da karar verme sürecine katkı sağlamayabilir. Ancak uzun sürece yayıldığında elde edilen birikimlerle daha sağlıklı kararlar verilmesine dolaylı olarak etki edebilir. Dolayısıyla bilgi sadece ilişkili olduğu organizasyon içinde anlam ifade eder (Altındiş 2010).

2.2.3. Bilgi Güvenliği

Bilgi güvenliği, ilgili kurumun her türlü bilginin korumasını sağlamasını oluşturmaktadır. Bu bağlamda denetimsiz her türlü girişin kontrolü sağlanmalıdır. Bilgi güvenliğini sağlanması adına sistemin risk analizleri de yapılaması gereken bir durumdur. Bu bağlamda kurum tüm idari ve teknik tedbirleri almakla yükümlüdür. Otomasyon sistemini bu denli önemli hale getiren şey hasta bilgilerinin korunmasını sağlamaktadır. Nitekim bu bilgiler şahsidir ve üçüncü kişilerle paylaşılamaz. Hem

ülkemiz özelinde hem dünya genelinde birçok kurum kendi ürettiği sistemde olsa bilgilerin gizliliğini koruyamamaktadır. Bilgilerin üçüncü şahısların eline geçmesi ise en çok siber saldırılar neticesinde olmaktadır. Siber saldırıların başarıya ulaşmasında birçok neden bulunmaktadır. Bunlar özetlemek gerekirse; bilgi kaynakları depolanırken güvenli olan opsiyonların tercih edilmemesi, hesaplara giren personellerin genellikle zayıf ya da kolaylıkla çözülebilen şifreler kullanmaları, sistemi kullanan çalışanların şifrelerini başkaları ile de paylaşması, işten ayrılan personellerin sistem hesaplarının kapatılmaması ve bu hesaplara istenildiği zaman girilebiliyor olması, siber saldırılarda saldıran kişilerin kimliklerinin tespit edilememesi, kamu kurumlarının sistemlerinde bulunan kişilerin ayrıntılı bilgilerin olması, bazı bilgilerin depolanması yönünden ekstra özen gösterilmemesi, internet için güvenlik duvarlarının yeterli olmaması şeklinde sıralanabilir. Bununla birlikte birçok kurumda bilgiye erişim sağlanırken yetkilendirme konusunda sorunlar yaşandığı görülmektedir. Bu durum erişim sağlayan kişilerin tehditleri fark etmemesine neden olmaktadır. Bilgi güvenliğinin standartların altında kalması da bir diğer sorun olarak öne çıkmaktadır (İleri 2016).

Ayrıca, birçok kurumda özellikle bilgi kaynaklarına erişim ve yetkilendirme konularında büyük bir bilgi eksikliği göze çarpmakta, bilgi kaynaklarına yönelik tehditlerde sorumluların tespitinde yaşanan zorluk ve zafiyetler bilgi kaynaklarının güvenliğinin yeterli ölçüde izlenemediğini ve erişimlerin standartlara uygun şekilde kayıt altına alınamadığını göstermektedir.

Kuruluşun sahip olduğu özel bilgilerini, başkalarının hukuka aykırı şekilde ele geçirmesi ve uygun görülmeyen kullanımdan korumayı amaçlayan programına bilgi koruma programı denir. Rakipler ile rekabet edebilmek, bu rekabette avantajı sağlayabilmek için bilginin korunması belli bir sistem dâhilinde temin edilmelidir.

Bu sebeple kuruluşlar çalışanlarına yönelik iş tanımları, davranış kuralları ve talimatlar gibi uygulamalarla bilgiyi korumak için önlemler almakta, işletme için gizli ve hayati ehemmiyete haiz bilgilere ulaşmayı sınırlayan teknolojiler, yazılım programları ve sistemler kullanmak zorundadırlar.

Organizasyon eğer elde ettiği, kullandığı ya da kullanmaya hazırlandığı bilgiyi muhafaza altında tutamazsa hem rekabet avantajını kaybeder hem de bilgi yönetiminin etkinliği zarar görür. Bilgiyi koruma konusunda başarısız olan

kuruluşlar elde edilen bilgi ile o an için verimli sonuç alsa bile bu bilgi daha sonra başka kuruluşlar tarafından da kullanılacağı için bilginin rekabet avantajı sağlama özelliği kaybolur (Çakar ve Yılmaz 2010). İşte bu noktada TS ISO EN 27001 Bilgi Güvenliği Yönetim Sistemi oluşturmak bilgileri korumanın en önemli yollarından biridir denebilir (Özkan 2010).

Günümüzde artık bilgi, bir organizasyon için mali kıymetler ne kadar önem taşıyorsa, en az o kadar önem arz eder hale gelmiştir. Bununla beraber küreselleşen dünyada, bilgiler, bilişim sektörünün artan gücüne paralel olarak giderek artan sayıda ve çeşitlilikte tehditlere maruz durumdadırlar. Bilgi güvenliği de işte bu noktada karşımıza çıkmaktadır.

Sonuç olarak günümüzde hastanelerde ve diğer kurumlarda bilgilerin saklanması depolanması ve diğer insanlarla paylaşılmaması önemli bir değere sahiptir. Kurumların kullanmış olduğu bilgisayar sistemleri çoğu zaman o sistemi kuranlar tarafından yönetilmektedir. Bu durumda bilgilerin çalınması ya da paylaşılması kolaylaşmaktadır. Bu durumda teknolojik olarak güvenlik duvarlarının oluşturulması gerekmektedir (İleri 2018).

2.2.3.1.Bilgi Güvenliği Yönetimi

Bilgi güvenliği yönetimi, örgütsel veri kaynaklarının kapasitesini kavrayarak, bunlara yönelik tüm denetim dışı müdahaleleri engelleme, bu konuda çeşitli risk analizleri kullanarak veri gizlilik ve bütünlüğünün temini için ihtiyaç olan tüm tedbirleri alma, bütün bunları bilgi güvenliği politikaları kapsamında yönetme işidir.

Herhangi bir örgütün ticari kazanç elde etmek, üretimde bulunmak, rakipleri ile rekabet ve örgütsel devamlılığı temin etmek amacıyla kontrol altında tuttuğu her çeşit kaynak bilgi varlıkları kapsamında değerlendirilebilir (Baykara ve ark. 2013).

Bu alanda karşımıza 4 temel unsur, konu başlığı çıkar. Birincisi, bilgi ile ilgili faaliyetlerin tepeden aşağı temini ve takibidir. İkincisi, sürdürülebilir mahiyette bir bilgi altyapısı oluşturulmasıdır. Üçüncüsü, bilgi sermayesinin örgütlenmesi, yenilenmesi ve dönüştürülmesidir. Dördüncü olarak da bilgilerin kullanımıdır (Özcan ve Barca 2008).

Farklı bir bakış açısıyla değerlendirildiğinde organizasyonlar için bilgi yönetimi; üçayaklı bir tabureye benzetilebilir. Üçayaklı bir taburenin bir ayağı ayrılsa, ayakta durması imkânsız hale gelecektir. Bunlar; insan, süreç ve teknoloji ayaklarıdır. Çünkü bilginin bir bireyden diğer bireye aktarılabilmesi için insana, bilginin kullanımını temin etmek ya da onu ilgili aktivitede kullanabilmek için de süreçlere gereksinim duyulmaktadır. Teknoloji ise bilgiye gerektiğinde tekrar ulaşma, depolama ve sayıca çok insan tarafından kullanılabilmesini düzenlemek için gereklidir (Doğan ve Kılıç 2009).

Bilgi yönetimin başarılı olması için güvenliğin temel amaçları olan bilgiye sürekli erişimin sağlanması, bilginin göndericiden alıcısına kadar gizlilik içerisinde, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlük içerisinde iletilmesi gerekmektedir. Bilgi güvenliği bütünüyle bilginin güvenliğine odaklı ve bunun sürdürebilir hale dönüştürülmesini sağlayan bir sistem ve bir olgudur. Bu yönüyle bilgi yönetimine olumlu fayda sağlamaktadır. Bilgi güvenliği yönetiminin eksikliği bilgi yönetimini olumsuz etkileyecektir.

Farklı bir şekilde izah etmek gerekirse bilgi güvenliği yönetimi; bilgi, kaynak ve ürünlerin, dış tehditlerden uzak olacak şekilde muhafazası ve (ihtiyaca binaen) yer değiştirmesi sırasında kendi içinde bütünlüğünün bozulup bozulmadığı hususunda emin olmak (Canbek ve Sağıroğlu 2006), ilgili ve yetkili şahısların bunlara istenildiği an aksamadan ulaşabilmesini temin (iso27001bilgiguvenligi.com), veri kaynaklarına yönelik risk analiz ve değerlendirmeleri yapmak, güvenlik açıklarına yönelik tedbirler almak (bilgiguvenligi.gov.tr), edinilen tecrübelere göre yaşanan siber saldırı vs. tehditlerin tekrarlanmasını önlemek için (He ve ark. 2014) gibi faaliyetlerin kurumdan sorumlu bilgi güvenliği yöneticisi başkanlığında (Sağsan 2007) belirli bir düzen içinde yönetilmesidir.

Her ne kadar kurumlarda tehditlere yönelik üst düzey teknik önlemler alınmış olsa da, veri kaynaklarına yönelik yaşanan saldırıların üst seviyede zararlar vermesinin önü alınamamakta, bu da sadece teknik tedbirlerin bu hasarları engellemeye yetmediğini göstermektedir. Dolayısıyla bu gerçek bilgi güvenliğinin yönetilmesi sürecinde, teknik tedbirlerin yanında içinde salt insan faktörü de bulunan, daha aritmik ve yenilenebilir özelliklere sahip bir anlayışa ihtiyaç duyulduğunu ispat etmektedir (Cavalli ve ark. 2004; Tekerek 2008).

Örgütsel veri tabanlarını çalışamaz hale getirerek direkt veya endirekt zararlara sebep olmak veri tabanına izinsiz müdahalede bulunup normal faaliyetleri aksatmak, durdurmak hatta tamamen işlevsiz hale getirmek anlamına gelebilecek tüm saldırılar (Canbek ve Sağıroğlu 2006) ve ticari mahiyeti olan gizli bilgilerin ele geçirilmesi (Eminağaoğlu ve Gökşen 2009), ticari ve itibari zararlar (Tekerek 2008), verilen hizmetin akamete uğratılması (Vural ve Sağıroğlu 2007) gibi tehditlere yönelik güvenliği sağlamak adına sorumluların, tüm bilgi güvenliği yönetim tedbirlerini kullanarak, bunları tüm sürece yaymaları zamanla tedbirlerin kurumsallaşmasına vesile olacaktır.

Örgütlerde iş ve işlemlerin sanal platformlarda yapılabilir hale gelmesinden sonra, bu işlemlere erişim ve yönetilme hususunun; aynı işlemin kağıt üzerinden halledilmesine oranla daha basit hale geldiği görülmektedir (NEHTA 2007; Bartlett ve ark. 2008).

Sanal veri taban kullanımıyla beraber artık ilgili herkes ulaşmak istediği veriye eksiksiz, süratli ve kesintisiz ulaşmak istemektedir (Şahin 2008). İşte esas hedefi veri tabanlarında gizlilik, eksiksiz muhafaza ve ilgili (yetkili) kişiye istediği anda istediği bilgiye ulaşım izni verme olan bilgi güvenliği yönetim sistemleri tam bu anda devreye girmektedir (Cavalli ve ark. 2004).

Bilgi güvenliği sürecinin geliştirilmesi için örgütsel ve örgütün ilintili olduğu sektörün genel özellikleri ve ihtiyaçları en güncel şekilde, alandan gelen sağlıklı bilgilerle birlikte ele alınmalıdır. Bunlara örnek vermek gerekirse; sağlık sektörünü ilgilendiren çalışmalar, çalışanlarının yeniliğe açık olup olmadığı (Sultan ve ark. 2014), çalışanlarda kişisel gelişim talebi düzeyi, şüphe ve kişisel inanma durumu (Wakefield ve ark. 2007; Fernando ve Dawson 2009; Holden 2011; Yücel ve ark. 2011), kendini geliştirme zorunluluğunun sebeplerini kavrayabilme (Pagliari 2005), veri tabanlarına erişim ve buna bağlı sistemi kullanım düzeyi (Yip ve ark. 2012) gibi sebeplerle yeni işler hale getirilmeye çalışılan sistemlere yönelik direnç olduğu hususunu (Khalifa 2013) ifade etmektedir.

Buna ilave olarak, sağlık birimindeki işleyişe hakkında yapılan araştırmalar, sağlık kurumlarında çalışanların bu veri tabanlarına ulaşım noktasında çoğu zaman birbirlerine şifrelerini verdiklerini dolayısıyla o işlemi gerçekte kimin yaptığının

tespit edilmesinin imkânsızlaştığı görülmektedir (Timmons 2003; Medlin ve Caizer 2007; Williams 2008; Fernando ve Dawson 2009).

Sonuç olarak kurum yöneticileri bu yukarıdaki izah edilen sorunun çözümü için bilgi güvenliği yönetim sisteminin öneminin personelce tam ve eksiksiz anlaşılması, içselleştirilmesi için çaba sarf etmeli bu sayede güvenlik yönetiminin de kurumsallaşmasını temin etmelidirler.

2.2.3.2.Türkiye'de ve Dünyada Bilgi Güvenliği

Günümüzde artık tamamen önünün alınması mümkün görünmeyen bilişim suçları ve siber müdahaleler hakkında devletler milli veri tabanlarını bilgi güvenliği yönetim sistemlerini tüm kurumları bazında kurarak, gerçek manada uygulanmasını sağlayarak tedbir alabilirler. Maalesef bizim ülkemizde de gerek özel sektör gerekse devlet birimleri bazında üretilen yeni bilgi ve teknolojilere yönelik de siber saldırılar vesilesiyle hırsızlık girişimleri olabilmekte, bilgiler yabancı şahıs veya devletlere geçebilmektedir. Bunun en temel sebebi bilgi güvenliği yönetim eksikliğidir.

Bu eksikliğin de detaylarını izah etmek gerekirse; güvenli erişim metotlarının bilinmesine rağmen kullanılmaması, güçlü parola tercih edilmemesi, parolaların yasak olmasına rağmen diğer kişilere verilmesi, örgütte görev yeri değişikliğine tabi olan veya görevden ayrılan çalışanın ayrılmasına rağmen sonlandırılmayan hesap bilgilerinin diğer personel tarafından kullanılmaya devam edilmesi, bu kuruluşlarca herhangi bir başka sebeple çalışanların ve kurumda bilgileri mevcut olan diğer kişilere ait diğerlerince bilinmemesi gereken bazı özel bilgilerinin de yanlış yer ve zamanda açıklanması gibi sıkıntılar karşımıza çıkmakta denilebilir.

Bu ayrıca örgütlerde veri tabanlarına ulaşım ve bu konuda sorumlulukları belirleme hususlarında büyük yanlışlıklar yapıldığı, bilgi eksikliği bulunduğu, sorumlu kişilerin yukarda ifade edilen dış tehditlerden habersiz olduğu ya da haberi varsa bile uygulamada güvenlik konularına uyup uymadıklarının denetlenmediği, erişim standartlarına uymama durumlarının kayıt altına alınmadığını da ortaya çıkarmaktadır.

Önemi her türlü ortamda vurgulanan bu güvenlik tedbirlerine uymamanın işleyişe verdiği maddi ve zamansal kayıplar, sistem kesintileri, veri kayıpları vb. şekillerde ölçülebilir hale de gelmektedir (PWC 2015).

Yapılan araştırmalarda, bilgi güvenliği yönetim sisteminin sağlıklı şekilde uygulanmasında, bu sistemi uygulamadan sorumlu olan kişilerin %56 oranında sistemin uygulanması adına yapılan faaliyetlerde personelin hali hazırda var olan örgütsel kültürden kaynaklı direnç gösterdiklerinden şikâyetçi oldukları yüzde 18 oranında ise üst yönetimdeki sorumluların konuya destekleri noktasında sıkıntı yaşadıkları anlaşılmaktadır (CE 2008).

Bununla beraber her ne kadar üst yöneticilerin destek konusunda eksikliğinden şikâyet oranı düşük gibi görünse de bilgi güvenliği yönetim kültürünün tam manasıyla yerleşmesi için personelce içselleştirme süreci ve eğitim sürecini kısa vadede oturtmak zor olacağı aşikâr olup kısa vadede üst yöneticilerin süreci hızlandırmaya katkı sağlamaları noktasında bilinçlendirilmeleri daha kolay ulaşılabilir bir hedef olarak belirlenebilir.

Araştırmalar Avrupa ülkeleri arasında bilgi güvenliği yönetim sistemi hususunda ülkemizin durumunu daha net göstermektedir. 2014 yılı rakamlarına göre 51 Avrupa ülkesi arasında en çok sertifikaya sahip ülkeler sıralamasında 11. Sıradadır. Sıralamada yönetim sistemine sahip en çok ülke İngiltere olup ülkemiz bunun çok gerisinde görünmektedir. Ayrıca 2014 itibariyle dünyada en büyük 13. Ekonomiye sahip İspanya ve 18. büyük ekonomik güce sahip Hollanda ülkelerinin sahip olduğu sertifika miktarı, ekonomi büyüklüğü olarak 16. Sırada olan ülkemizden fazla görünmektedir (IMF 2014).

Bu bağlamda bilgi güvenliği yönetim sistemlerini hayata geçiren örgütler siber saldırılara ve istenmeyen veri kayıplarına karşı tedbirli olmaları, her yeniliğe hızlı şekilde entegre olarak değişime açık olmaları, iş süreçleri ile güvenlik politikalarını birbirleriyle uyumlu hale getirebilmeleri noktasında ideal düzeye ulaşabilmeleri için bağımsız kuruluşların sürekli denetimlerine açık olmaları gerekmekte, çıkacak raporlara uygun yeni tedbirler almalılar.

Bilgi güvenliği ülkemizde beklenilen hedeflerin altında kalmıştır. Ülkemizin de bu seviyeler gelmesi öncelikle teknolojik değişimlere ayak uydurmasına bağlıdır. Siber saldırılara karşı hazırlıklı olmalı ve bütün güvenlik sistemlerini yönetimin bir parçası olarak saymalıdırlar. Bu güvenlik süreçleri kurum yönetiminin önemli bir parçası olarak idari mekanizmalara entegre edilmelidir. Bununla birlikte her kurum

kendi sistemini bağımsız denetçilere denetletmelidir. Denetleyici firmalar güvenlik duvarlarını güncelleştirerek önleyici birçok faaliyet geliştirirler (İleri 2018).

2.2.3.3.Kurumsal Bilgi Güvenliği Hafızasının Oluşturulması

Bunun için yapılan çalışmanın esasını "Olay Raporlama Prosedürü" oluşturur. Buna göre kurum veri tabanlarından birinde oluşan bilgi güvenliği hadisesi çözüldükten sonra ulaşılan yeni bilgilerin örgütsel kurumsal bilgi havuzuna aktarımı için, hadiseler ışığında kategorize edilmesidir. Başka deyişle yaşanan olayın türü, hangi veri türlerinin etkilendiği, olayın gerçekleşme sıklığı, sebepleri, zararın ölçülüp ölçülemediği vb. sorulara cevaplar verilerek birimlerden sorumlu kişi tarafından BGYS yöneticisine iletilip sisteme girilmesi aşamaları karşımıza çıkmaktadır. Nihayetinde tüm bu yeni verilerle kurum içi bilgi güvenliği veri havuzu oluşmuş olacaktır.

Yukarda işleyiş prosedürü izah edilen bilgi güvenliği hadisesi ile ilgili edinilen tecrübelerin örgüte üç temel yararı olur. İlki, işleyişte yapılan aynı hata hakkında edinilen bilgiler buradan farklı bir veri tabanına girildiğinde oradaki hata tespit uyarı sistemine etkinlik kazandıracaktır. İkincisi, veri tabanı işleyişi veya bilgi güvenlik yönetiminden sorumlu personelin herhangi bir sebeple kurumdan ayrılmaları sonrası daha sonra gelecekler için bilgi kopukluğu yaşanması engellenmiş olacaktır. Sonuncu olarak da; verilerin kurum içinde tek bir havuzda toplanmış olması hem kurumsal hafızanın oluşmasına katkı sağlamış hem de personelde konu hakkında hassasiyet oluşmasına katkı sağlamış, aynı hatanın tekrar etmesini yüksek oranda engellemiş, sonra oluşabilecek farklı zafiyetlerin önceden öngörülebilmesine büyük oranda katkı sağladığı görülmüştür.

2.2.3.4.Bilgi Güvenliğini Etkileyen Faktörler

Bilginin sahibi, bilgiyi kullanan ve bilgi sistemini yöneten kişiler bilgi güvenliğinin sağlanmasından sorumludur. Buradaki güvenliği tehdit unsuru; sistemin ya da kurumun kısmen ya da tamamen zarar görmesine sebep olabilecek istenmeyen bir olayın arkasındaki belirlenemeyen sebep olarak tanımlanabilir (Öztemiz 2013).

Tehditler kaynak açısından ise insan kaynaklı ve doğa kaynaklı olarak, geliş yönüne göre kurum içi ve kurum dışı olarak sınıflandırılabilirler.

● İnsan faktörü: Kurumların ve örgütlerin tamamında bilgi güvenliğinin sağlanmasında çalışanların rolü yadsınamaz. Bilgi güvenliği noktası çalışanların şifrelerinin zayıf olması ya da şifreleri başkaları ile paylaşması sorun oluşturmaktadır. Bununla birlikte denetleyici olan uzmanlarında yapabileceği hatalar bilgi güvenliği noktasında insan faktörünü ifade etmektedir. Özellikle sağlık kuruluşlarının çalışanların yüzlerce insanın bilgilerini kaydetmesi dikkat edilmesi gerek durumu ortaya koymaktadır. Bu bağlamda sadece memurlar değil doktorların da kendi sistemlerine dikkat etmeleri gerekmektedir. Ayrıca hastane personeli bu gizlilik konusunda bilgilendirilmelidir (İleri 2018).

Tüm örgütlerde çalışanların kurumsal bilgi güvenliği üzerindeki etkisi yadsınamayacak seviyede olmakla birlikte, hizmet odaklı olan, çok farklı disiplinlerden uzmanların beraber iş yaptığı, yoğun bilgi erişimi gerektiren sağlık kurumlarında bilgi güvenliğini sağlamada insan boyutu fazlaca önem kazanmaktadır. Sağlık kurumlarında çalışanların bilgi güvenliği algısı noktasında çalışmalar bulunmakla birlikte, bilgi kaynaklarına erişimde sağlık çalışanlarının şifre güvenliği yönetimleri üzerine literatür de çok kısıtlı sayıda çalışma bulunmaktadır. Bu çalışmanın amacı, bilgi güvenliğinin ve bilgi güvenliğini sağlamada insan faktörünün çok önem kazandığı sağlık kurumlarında, hastane bilgi yönetim sistemlerini kullanan hekimlerin kurumsal bilgi kaynaklarına erişimde şifre yönetimi noktasında alışkanlıklarını belirlemektir.

Bilgi güvenliğini tasarlayan, uygulayan ve yöneten unsur olan insan, bilgi güvenliğinin temel taşını oluşturur. Bununla beraber aynı temel öğe olan insan, kurumsal sistem ve bilgileri yönetirken çeşitli sebeplerle sistemde büyük açıklıklara neden olabilir. Kurulan birçok teknolojik alt yapıda insana ait faaliyetler kontrol edilemez, yönetilemez ve ölçülemez olabilmek, bu durum ise (sistemde açık bulunması yönüyle) süreçlerin sağlıklı işlememesine ve kullanıcılar tarafından yapılan hataların yol açtığı sorunların anlaşılamamasına ya da giderilememesine neden olabilmektedir (Yıldız 2009).

● İç tehditler; organizasyon bünyesinde çalışanların oluşturabileceği bilinçli ya da bilinçsiz tehditlerdir ve bunlar bilgi güvenliği tehditleri arasında önemli bir yer tutmaktadır. Bilinçli tehditler iki kategoride ele alınabilir. İlkinde, organizasyonda yer alan kötü niyetli bir çalışanın kendisine verilen erişim haklarını kötüye

kullanması kastedilir. Veri tabanı yöneticisinin, eriştiği verileri çıkar amacı ile başka bir işletmeye satması da buna örnek verilebilir. İkincisinde ise bir çalışanın başka birine ait erişim bilgilerini elde ederek, normalde erişmesi yasak olan bilgilere erişip, kötü niyetli bir eylemde bulunmasını kapsar. Veri tabanı yöneticisi olmayan ve normalde veri tabanına erişim hakkı bulunmayan birisinin, erişim bilgilerini bir şekilde elde ederek, verilere ulaşması ve onları çıkarı için kullanması ikinciye örnektir (bilgiguvenligi.gov.tr).

Amerika Birleşik Devletleri'nde CSI tarafından yapılan bir araştırmada; bazı finansal şirketlerin, kamu ve eğitim kurumlarının ve sağlık işletmelerinin bilgi teknolojileri ve bilgi güvenliği profesyonellerinin katıldığı ankete göre, 2008 yılı içinde katılımcıların % 44'ü iç suiistimal yaşamışlardır. Bu oran, % 50'lik virüs tehdidinden sonra iç suiistimallerin ikinci büyük tehdit olarak ortaya çıktığını göstermektedir. Bu tür suiistimallerin tespitinin zor olduğu ve çoğunlukla organizasyon dışına bu konu ile ilgili çok fazla bilgi verilmek istenmeyeceği de hesap edilirse, oranın % 44'ten çok daha yüksek olabileceği değerlendirilmektedir. Çalışmada, suiistimal tabiri ile sadece bilinçli oluşan iç tehditler kastedilmektedir (sis.pitt.edu).

Bir başka araştırma şirketi (Price Water House Coopers)'nin, 7000'den fazla güvenlik uzmanı ile yaptığı araştırma sonuçlarına göre, mevcut ve eski çalışanların en büyük tehlikeyi oluşturduğu ifade edilmiştir (Yıldız 2009).

İç tehditlerin önemli bir kısmını çoğunlukla uygulama seviyesinde görülmesinin sebebi şirket çalışanlarını çoğunu bilişim alanında detaylı teknik bilgi sahibi olmayan kişilerin oluşturmasıdır. Söz konusu kişiler, uygulamaların kendilerine tanıdığı yetkiler içinde ya da sosyal mühendislik yöntemleri ile başka kişilerin erişim bilgilerini ele geçirip, uygulamaları suiistimal etmektedirler (bilgiguvenligi.gov.tr). Tehditlerin hedefi; yazılım, donanım, veri, depolama ortamları, bilgi aktarım ortamları, insanlar olabilmektedir.

● Kişisel gizlilik; bir kişinin ya da grup üyelerinin kendilerine ait bilginin kimlere, hangi şartlar altında iletilebileceği konusunun, bizzat o kişilerin/grubun onayı ile gerçekleştirilmesine kişisel gizlilik denir. İki farklı durumda da kişisel gizlilik uygulanmalıdır. İlki; kişisel veriler, kişilere ait bilgi sistemlerinde bulunduğu dönemde, dışarıdan tüm tehditlere karşı korunmasıdır. Burada herhangi bir bilginin

korunması için geçerli olan (erişim denetimi, yetkilendirme, sürekliliğin sağlanması gibi konuları içeren) tedbirlerin aynısı uygulanır. İkincisi ise ihtiyaç halinde kişisel verinin bir başka sistem ile paylaşılmasında uygulanacak (verinin içeriğinin kişi tarafından paylaşılması, onaylanmamış kısmının filtrelenmesi, filtrelenmiş verinin ilgili sisteme güvenli aktarımı ve söz konusu verinin sadece veri sahibi kişiler tarafından onaylanmış organizasyonlar ile paylaşılması gibi) güvenlik tedbirlerini ifade eder (bilgiguvenligi.gov.tr).

2010 yılında Anayasa'nın 20. maddesine eklenen 'Herkes kendisi ile ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisi ile ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızası ile işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir' hükmü uyarınca Türkiye'de kişisel verilerin korunması net şekilde anayasal bir hak olarak düzenlenmiştir (Küzeci 2011).

Bununla beraber ülkemizde sağlık verilerinin gizliliğine ilişkin temel kaynak olan 'Hasta Hakları Yönetmeliği' ne göre hasta hakları, temel insan haklarının sağlık alanına yansıması olup, "Kanunlar ile izin verilen durumlar ve tıbbi zorunluluk halleri dışında, hastanın özel ve aile yaşamının gizliliğine dokunulamaz" şeklinde ifade edilen, kişisel sağlık verilerinin korunması bu kapsam içindedir. Yönetmelikte belirtildiği üzere, hastalar kendi kişisel verilerine erişim hakkına sahiptir, hasta kayıtlarına yalnızca (hastanın izni varsa) tedaviyle ilişkili kişiler bakabilir. Hastaya ilişkin sağlık hizmeti sonucunda edinilen bilgiler yasanın izin verdiği durumlar haricinde kesinlikle açıklanamaz (Küzeci 2010).

Bilgi güvenliği ihlalleri; izinsiz erişim (kopyalama, okuma, dinleme), zarar verme (kaybolma, ulaşılamaz/kullanılamaz duruma getirme), değişiklik yapma (bilgileri/programı değiştirme, veri aktarma), üretim (veri taklidi, ekleme) olarak sayılabilir (Öztemiz 2013).

Güvenlik olayları genel çerçevede 6 başlığa ayrılabilir (Vardal 2009):

- Çalışan sahtekârlığı: Kurum/kuruluştaki görevlilerce sahtekârlığa yönelik aktiviteleri içeren olaylar.

● Taklit: Kişi ya da kurumun kendini gerçekte olmayan bir kişi ya da kurum gibi göstererek gerçekleştirdiği eylemler.

● Kayıp: Bilgilerin muhafaza edildiği fiziksel materyallerin kaybolmasını ya da tahrip edilmesi.

● Sızma/nüfuz etme: Bilgisayar yazılımına/sistemine/ağına sızma olayları.

● Hırsızlık: Bilgilerin muhafaza edildiği fiziksel materyallerin çalınması.

● Yetkisiz açıklama (ifşa): Bilgilerin kanunen yetkisi olmayan ilgisizi kişilere ifşası.

2.2.3.5.Bilgi Güvenliği Sağlama Araçları

Fiziksel güvenlik, fiziksel olarak (güvenli oda/yapı gibi) önlemler alınmasıdır. Tek kullanımlık parola, akıllı kart gibi kullanıcı doğrulama araçları, kullanıcı doğrulaması yöntemleri olarak geçer. Şifreleme, güvensiz ağlar üzerinden geçen veriler için şifreleme yapan donanımların kullanılmasıdır. Yönetsel önlemler, güvenlik politikaları; kurumsal, konuya özel ve sisteme özel güvenlik politikalarının oluşturulması. Standartlar ve prosedürler; konfigürasyon yönetimi, yedekleme ve yedekleme ortamlarını saklama, olay müdahale, iş sürekliliği ve felaket kurtarma prosedürleri olarak karşımıza çıkmaktadır. E- imza, anti-virüs sistemleri, güvenlik duvarları, erişim denetimi bilgi güvenliği temin araçları olarak sayılabilir (Öztemiz 2013).

2.2.3.6.Bilgi Güvenliği Standartları

Organizasyonun genel varlıklarını korumak için tasarlanmış bir genel güvenlik politikasını ifade eden güvenlik süreci için bir işletme; bilgi varlıklarının yeterli şekilde korunmasını güvence altına almak amacıyla, bilgi güvenliğinin yönetilmesinde öncesinde kendi sahip olduğu uygulama ilkelerini benimseyebilir, kontrol araçlarını bir araya getirebilir, güvenlik standartlarından birini tercih edip sertifika temin edebilir ya da karma bir taktik izleyebilir (Upfold 2005).

Bilgi güvenliği konusunun önemli ve sürekli geliştirilmesi gerek bir durum olması standartların üzerine düşünülmesini zorunlu kılmıştır. Bu bağlamda kaynakların doğru yapılandırılması güvenliğinin sağlanmasına dikkat edilmelidir.

Ayrıca yasal düzenlemelerin de yapılandırılması önem kazanmaktadır. Bilgi güvenliğinin sağlanmasında karşılaşılan temel zorluklar ortaya çıkabilmektedir. Bunlardan bahsetmek gerekirse ilk olarak, çok büyük oranda uyumsal çalışma gerektiren bilgi teknolojileri sistemlerinin çok geniş bir alanda kullanılmak istenmesidir. Hızlı ve sürekli değişen teknoloji sebebiyle bilgisayara bağlı teknolojinin sürekli olarak sanal tehditler altında kalmıştır. Bu hızlı ve sürekli değişen teknolojik sistemlerin aynı hız ve süreklilikte sanal saldırılara maruz kalmalarına neden olmuştur. Organizasyonların düşük maliyet ama yüksek verimli sistemlere ihtiyaç duyma oranı yükselirken, bilgi güvenliği amacıyla kullanılan yasal ve düzenleyici zorunlulukların getirdiği yükümlülükler de artmıştır. Son olarak kurumların kaynak, kabiliyet ve uzmanlık açısından bilgi güvenliğini temin etmede yetersizlikleri söylenebilir (bilgiguvenligi.gov.tr).

Bu konudaki zorluklardan kaynaklı olarak, işletmeler, herkesin uzmanlık alanına göre güvenliğin sağlanmasına dair tedbirleri ele alan kuralları ifade eden sınırlı standartların oluşturulması ve uygulanması yoluna gitmişlerdir.

Yürürlükteki standartlar;

- 1996 Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA): Bir takım idari, fiziksel ve teknik önlemleri kapsayan, bireylerin sağlık bilgilerini korumak için, mahremiyete ve güvenliğe uygun olarak geliştirilen standartlardır. Bireylerin sağlık bilgilerini aktarmak için internet ya da elektronik sistemler kullanan hastane, eczane, kaza-sağlık sigortası ve tıbbi hizmet planı veren şirketler, tıbbi cihaz satan ve kiralayan şirketler, bireysel hekim klinikleri vb. işletme ve organizasyonlar, HIPAA standartlarının uygulamak zorundadırlar. İdari önlemler olarak gizliliği olması gereken birimlerin denetlenmesi ve bunlar için gerekli prosedürlerin yazılması için bir yönetici belirlenmesi, korunması gereken sağlık bilgilerine kimlerin ulaşıp ulaşamayacağının tespit edilmesi, çalışanların kategorize edilmesi, farkındalık yaratılması için çalışan eğitimleri ile gerekli bilgilendirmelerin yapılması, organizasyon ile beraber iş yapacak diğer kişi ya da kurumların da bu standartlara uyacağına dair anlaşmaların yapılması, acil durumlarda sağlık bilgisi verilerinin geri çekebilmesi ve veri düzeltme işlemlerinin yapılabilmesi, mahremiyete aykırı durumlarını tespit edebilme ve veri üzerinde zarar tespiti yapabilmeleridir. Fiziksel önlemlerde organizasyonda kullanılan cihazların ağ çalışma gruplarına dahil edilir ya

da çıkarılırken gerekli teknik işlemlerin yapılabilmesi, içinde bu tarz mahrem sağlık bilgileri mevcut olan cihazlara ulaşımın kontrol edilmesi ve takibi, bu cihazlara müdahalenin sadece ilgili kişiler tarafından yapılmasının sağlanmasıdır. Teknik önlemler ise bu tarz mahrem sağlık bilgileri mevcut olan cihazların, siber saldırılara karşı muhafazası, mahrem sağlık bilgilerinin ağ üzerinde dolaşımda bulunması halinde, kriptolama yöntemlerinin kullanılması, gizliliğinden sorumlu olunan sağlık verilerinin değişmeyeceği ya da ilgisiz kişilere iletilmeyeceğine dair her birimin risk analizlerinin ve risk yönetimlerinin belgelendirilerek güvence vermesidir (Guthrie 2003).

- 1999 yılının Finansal Hizmetler Modernizasyonu Yasası (GLBA): Müşterilere ait gizli bilgilerin korunmasını esas alınan bu sistem, daha çok bankalar, güvenlik şirketleri ve sigorta şirketlerinin güvenliği ve müşteri mahremiyeti için geliştirilmiş bir standartlar bütünüdür. Gizlilik ve bilgi güvenliği ile ilgili üç temel prensibi vardır. Mali mahremiyet kuralı, müşteri ile ilgili bilgilerin nerede ve nasıl kullanıldığını, bu bilgilerin nasıl korunduğunu belirten müşteri arşivlerini tutulması, müşteri bilgilerinin korunmaması durumunda müşterinin ne gibi haklarının bulunduğunun belirtilmesi, organizasyonun güvenlik ile ilgili yaptığı politika değişikliklerini müşterinin onayına sunulması gibi müşteri mahremiyetini korumak için alınması gereken tedbirleri ifade eder. İhtiyat kuralı her birim için risk yönetim merkezinin kurulup, bilgiyi korumak adına, program geliştirilmesi, izlenmesi ve test edilmesi, bilginin toplanması, sunulması ve kullanılmasına göre politikaların değiştirilmesidir. Ayrıca müşterilerin gizli bilgilerini korumak için ne gibi önlemler alacağına ve hangi yöntemlerin uygulayacağına dair yazılı planların oluşturulup, en azından bir çalışanın bu iş için görevlendirilmesidir. Veri çalınmasının engellenmesi kuralı yetkili ve görevli kişiler haricinde erişim izni olmadan, diğer müşterilerin bilgilerine ulaşımın engellenmesidir (Hayes 2006).

- Bankacılık Düzenleme ve Denetleme Komitesi (BASEL): Bilişim sistemlerinde riskin tamamen ortadan kaldırılamayacağı ancak bu riskin gerçekleşme olasılığının minimize edilebileceği düşüncesi temel alır. Özetle bankaların sermaye yeterliliklerinin ölçülmesi ve değerlendirilmesine dair düşünülmüş standartlar bütünüdür. Amacı bankaların risk yönetimlerini etkin bir hale dönüştürmek, piyasa disiplinini sağlamak, sermaye yeterliliği ölçümlerinin yeterliliğini artırıp etkili bir bankacılık sistemi oluşturmaktır. Bu sistem bilgi güvenliği sağlanması için dört

maddeye önem atfeder. Erişim kontrolü, bilişim teknolojilerine kimin nasıl erişeceği ilişkin sınırların belirlenmesi, çalışanların kullanıcı hesaplarının oluşturulması, kaynak erişim hakları ve ayrıcalıklı yönetici hesaplarının belirlenmesi, şifre ve kullanıcı hesapları ile ilgili standartların belirlenmesidir. İş sürekliliğinin sağlanması, donanım ya da yazılımsal hatalar, elektrik kesintisi ya da doğal afetler gibi her ölçüde acil durumlar için gerekli risk tedbirlerin öncesinde belirlenmesi, organizasyona ait her türlü bilginin korunarak bunların saklandığı sunucuların önceden farklı yerlerde kopyasının tutulması, bu gibi durumlar için acil risk yönetim masalarının oluşturulup müşteri hizmetlerinin devamlılığının sağlanması, tüm bu süreçte yasal sorumlulukların yerine getirilmesidir. Değişiklik yöntemi, talep edilen ve gerekli bulunan değişikliklerin tanımlanıp olası bir değişikliğin muhtemel etkilerinin belirlenmesi, hangi sistemlerin hangi tarihlerde hangi sıra ile güncelleneceğinin tespit edilip bunlardan sorumlu kişileri tespit edilmesi, olumsuz senaryolar için geri dönüşüm prosedürlerinin detaylıca hazırlanmasıdır. Güvenlik yönteminde ise yetkisiz erişimlerin engellenmesi, bilginin değiştirilmesinin ve bilgiye saldırılmasının engellenmesi, koruma için gereken kontrol ve ölçümlerin tespiti, bu ölçümlerin belgelendirilip kontrollerin uygulanmasıdır (Tarullo 2008).

- Ödeme Kartları Endüstrisi Veri Güvenliği Standartları (PCI DSS): Kredi kartı işlemleri ve ödemeleri sırasında, bilgilerin açığa çıkmaması için güvenliğin sağlanması amacıyla oluşturulmuş kurallardır. Bu kurallardan ilki güvenli bir internet ağının oluşturulması ve bakımı; kart sahibinin bilgilerini korumak için güvenlik duvarının oluşturulması, dış kaynak organizasyonlar tarafından sağlanan güvenlik parametrelerine itibar edilmesidir. Kart sahibi bilgilerinin korunması; kart sahibine ait depolanmış bilgilerin, dış müdahaleye açık ağ üzerinden transferi sağlanırken şifrelenerek korunmuş olmasıdır. Saldırılara karşı yönetim biriminin oluşturulması; dış tehdide açık sistemlerin anti-virüs yazılımlarının güncellenmesi, güvenli sistemlerin ve uygulamaların geliştirilip kullanılmasıdır. Erişim kontrol ölçütlerinin zorlaştırılması; kart sahibinin gizli bilgilerine erişiminin kısıtlanması, bilgisayar erişiminde kullanılmak üzere müşterilere ayrı bir kimlik numarası verilmesi ve kart sahibi bilgilerine fiziksel olarak erişimin engellenmesidir. Düzenli olarak ağın izlenmesi ve test edilmesi, düzenli olarak güvenlik sistemlerinin ve işlemlerinin test edilmesi amacıyla ağ kaynaklarına ve kart sahibi bilgilerine erişimlerin takip edilmesidir. Son olarak bilgi güvenliği politikası geliştirilmesi, Bilgi güvenliğini esas alan politikaların belirlenmesidir (Morse 2008).

2.3. Hastane Bilgi Yönetim Sistemleri

Etkin ve verimli bir sağlık hizmetinin sunumu, takım çalışmasını, etkin bir bilgi paylaşımı ve akışını, karşılıklı işbirliğini zorunlu hale getirmektedir. Diğer taraftan sağlık hizmetlerinin çağdaş gelişmişlik seviyesinde uygun bir biçimde sunulmasını sağlamak maksadıyla standartlaşan süreçlere gereksinim duyulmaktadır. Bu durumu elde etmek amacıyla sağlık hizmeti veren kurumlarda bilgi teknolojileriyle birlikte enformasyon sistemlerinin kullanımı çok ciddi seviyede önem arz etmektedir. Bilgi sistemleri bir kurumda o kurumun etkinlik ve verimlilik seviyesini yükseltmek amacıyla kullanılmaktadır (Hevner ve ark. 2006). Bu sebeple sağlık bilgi sistemlerinin amacı etkin ve yüksek nitelikli hasta bakımı işlemlerine katkı sağlamaktır (Haux 2006).

Hastane Bilgi Yönetim Sistemleri (HBYS) sağlık kurumlarında tıbbi bilgiler ile idari bilgilerin pekiştirilmesi neticesinde oluşturulan ve sağlık hizmetlerinin arzını kolay hale getiren, kullanım kalitesinin artmasını sağlayan, bilgi sistemleri şeklinde tanımlanmaktadır. HBYS, çok yoğun bilgi gereksinimi olan çok işlevli veri sistemleri olarak da kısaca tanımlanabilir. Belirli standartlara sahip ve nitelikli şekilde işletilmesi zaruri olan bir takım süreçleri içerir. Sistemlerin içerdiği süreçler ne kadar kaliteli ve doğru yönetilirse, sistemler de o düzeyde nitelikli ve kullanışlı olmaktadır. HBYS sağlık hizmetleri sunumu sürecinde, eksiklikleri düzelten, doğru neticeler ortaya koyan, sağlık verimliliğini yükselten nitelikli bilgi girişleri ile en iyi sonuçları ortaya koymaya çalışan ve ekonomik açıdan da maliyetleri düşüren yapıları ile vazgeçilmez olan sağlık bilgi sistemi olarak ön plana çıkmaktadır (Köksal ve Esatoğlu 2005).

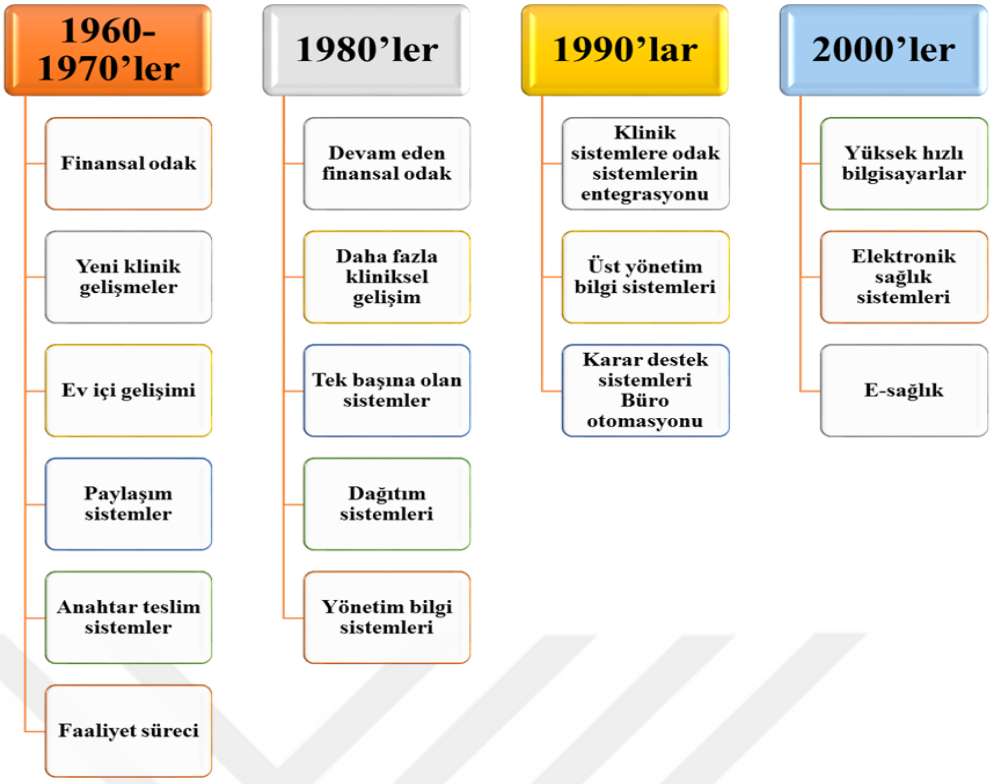
Teknolojik gelişmeler sayesinde hasta ve hastanelere erişim olanağı artmakta, sağlık bilgi sistemlerinden istifade etmek kolay hale gelmekte, etkili ve verimli sağlık hizmetlerinin sunumu sağlanabilmektedir. Teknolojik imkânlar ile İş yükünde azalma sağlanmakta, hem hizmet verenler hem de hizmet alanlar bakımından zaman tasarrufu elde edilmektedir. HBYS insan kaynakları yönetimi, finansman, planlama ve muhasebe işlemleri, stok yönetimi ve ofis otomasyonları vb. yönetsel fonksiyonlar içermektedir. Ayrıca hastalar için sunulan tanı ve tedavi hizmetleri, klinik karar desteği, ilaç ve tıbbi malzeme kontrolü, hemşirelik bakımı, laboratuvar ve radyoloji sistemleri gibi çok farklı fonksiyonları da icra eden karmaşık bir sistemdir. Diğer

taraftan günümüzde yoğun rekabet koşullarında hastaneler ileri tıp teknolojilerinden ve akıllı bina sistemlerinden istifade etmek zorunda kalmaktadır (Akpolat 2013).

2.3.1. Hastane Yönetim Bilgi Sistemlerinin Amacı

Hastane Bilgi Yönetim Sistemi (HBYS) hastanelerde hem kurumlar arası ilişkilerin hem de iş akışının düzenlemesinde etkili olan bir yöntemdir. Bu bilgisayar sistemi bilgisayarın senkronize bir şekilde çalışarak belirli bir program boyunca işlem yapmasını içermektedir. Nitekim birçok HBYS sisteminin kullanımından önce okudum/anladım içerikli geçiş mesajları bulunmaktadır (Uludağ ve İleri 2018).

HYBS'nin esas gayesi bir sağlık kurumlarının yönetiminde gereken bilgilerin tam, doğru ve tam zamanında sağlanmasıdır. Bir hastanenin bilgi gereksinimi, muhtelif alanlarda açığa çıkmaktadır. Bilgi sistemleri stratejik planlama, hizmet geliştirme ve pazarlama alanlarında destek sağlamakta, bu alanlarda görev yapanlara talepler, kullanım oranları ve pazarın özellikleri konularında bilgiler sağlamaktadır. Bu sistemlerde, stratejik planlama ve sürekli kalite geliştirme kapsamında verdikleri destekle hasta memnuniyeti, tıbbi hizmetlerin maliyetleri, etkinlik ve kalite parametrelerinin takibi, tanı ve tedavi planlarının icra edilmesi amacıyla tıbbi veri tabanları işletilmektedir. Bu sistemler verimlilik analizi ve iyileştirme desteğiyle her bir ana maliyet merkezi için belirlenmiş olan performans kriterlerinin kıyaslanmasına olanak tanımaktadır. Diğer taraftan sağlık sektörü çalışanları arasındaki ilişkilerin iyileştirilmesine verdiği destek sayesinde hastaneler ile sağlık hizmetleri çalışanlarının (doktor, laboratuvar, sigorta şirketleri, uzman merkezler vb.) arasında gereken elektronik bağlantıların teşkil edilmesine imkân sağlamaktadır (Austin ve ark. 1995).



Şekil 1: Sağlık Bilgi Sistemlerinin Tarihsel Gelişimi (Austin ve Boxerman 2003).

2.3.2. Hastane Bilgi Yönetim Sistemlerinin Tarihsel Gelişimi

Hastane bilgi sistemleriyle alakalı tarihsel gelişimi ile ilgili olarak yaşanılan tarihsel gelişmeler incelendiğinde 1960'lı yıllardan itibaren kullanımın başladığı görülmektedir. 1959 yılına dek, hastane bilgi sistemleri çoğunlukla manuel olarak mekanik işleme metotları ile icra edilmiştir. 1960 ve 1969 yılları arasında, bilgisayar teknolojisinin gelişimi ile yeni bir dönem başlamıştır. 1970 ve 1979 yılları arasında ise yeni teknolojilerin kullanıldığı sistemlerin gelişimi ile mevcut olan bilgisayar donanımlarıyla ilk çalışmalar yapılmıştır. Daha sonra 1980-1989 yılları arasında kelime işlemcilerin geliştirilmesiyle daha ileri bir düzeye ulaşılmıştır. Bilgi işleme ve kullanma imkânlarının artmasıyla 1990'larda yıllarda hasta bakımı ve stratejik yönetim konuları üzerine yoğun çalışmalar yapılmıştır. Müteakiben 2000'lerde ise yüksek hızlı işlemciler, bilgi ve iletişim teknolojileri sayesinde elektronik sağlık kayıt sistemlerinin geliştirilmesine dönük araştırmalar icra edilmiştir (Austin ve Boxerman 2003). Günümüzde ise, elektronik sağlık kayıt sistemleri ve e-Sağlık uygulamaları sağlık sektörünün başlıca uygulamaları içerisinde yer almaktadır.

2.3.3. Hastane Yönetim Bilgi Sisteminde Olması Gereken Temel Özellikler

Hastane bilgi sistemlerinin geliştirilmesi aşamasında elektronik hasta kayıtlarının tutulması hakkında birçok çalışma ve yayın mevcuttur. İlgili çalışmaların içerisinde en kapsamlı olanlardan biri de IOM (Institute of Medicine) tarafından yapılan çalışmadır. Bu çalışmada çağımızda sağlık sistemlerinin güvenilir, etkin, hasta odaklı, zamanında sonuç getiren ve eşit olması gerektiği vurgulanmıştır. Bu çalışma kapsamında ortaya konan sonuçlara göre, elektronik hasta kayıt sisteminin bütünleşik ve işlevsel olması açısından temel olarak 12 kıstasa sahip olması gerekli olduğu ortaya konmuştur. Buna göre bir sağlık bilgi sistemi (IOM 2001);

- Bir problem listesine sahip olmalı,
- Hastaların sağlık durumu ve fonksiyonel seviyelerinin sistemli bir şekilde ölçümü ve kaydını desteklemeli,
- Tüm tıbbi teşhis ve yorumların klinik gerekçelerinin belgeli hale getirilmesi amacıyla mantıksal bir temele sahip olmalı,
- Hayat boyu sağlık kaydı yapabilmek amacıyla hastaya ait bütün hasta kayıtlarıyla bağlantı kurabilmeli,
- Yetkilendirilmeyen erişimlere karşısında korunmuş olmalı,
- Tüm gerektiği anlarda ulaşılabilir olmalı,
- Bilgilerin kullanıcı gereksinimlerine bağlı olarak düzenlenebileceği ara yüzleri desteklemeli,
- Uzak ve yakın veri tabanları ve sistemler ile bağlantılı olmalı,
- Yapılandırılmış bir veri grubundan doğrudan veri giriş kabiliyetini desteklemeli,
- Karar analiz araçları sağlamalı,
- Doktorlara ve kurumlara bakım maliyetleri ve kalitesinin analiz edilmesi ve yönetilmesi açısından destek sağlamalıdır.

Klinik Modüller	İdari Modüller	Karar Destek Sistemleri
Hasta Kabul Modülü	Vezne Modülü	Karar Destek ve
Poliklinik Modülü	Cihaz Takip Modülü	İstatistik Sistemi
Acil Modülü	Faturalama Modülü	İstatistik Modülü
Laboratuvar Modülü	Tek Düzen Muhasebe	Yönetici Modülü
Doğum ve Ameliyathane	Modülü	İnsan Kaynakları
Modülü	Stok Takip ve	Yönetim Sistemi
Radyoloji Modülü	Demirbaş Modülü	(İKYS)
Servis Modülü	Personel Modülü	Yatırım Takip Sistemi
Hemodiyaliz Modülü	Bordro Modülü	(YTS)
Ağız ve Diş Sağlığı Modülü	Satın alma Modülü	Elektronik Belge
Sağlık Kurulu Modülü	Evrak Modülü	Yönetim Sistemi
Eczane Modülü	Eğitim Modülü	(EBYS)
Nükleer Tıp Modülü	Bilgisayar Yönetim	
Danışma Modülü	Modülü	
Sterilizasyon Modülü	Bilgi İşlem ve Destek	
Kan Merkezi Modülü	Modülü	
Arşiv Modülü	Hizmet Takip Modülü	
	Asistan Modülü	

Şekil 2: Hastane Bilgi Yönetim Sistemleri Modüler Yapısı Örneği (akgunyazilim.com.tr; RMA 2014).

Çağdaş sağlık bilgi sistemlerinde esas olarak iki temel unsurdan bahsedilmektedir: Bunlar elektronik sağlık kayıtları ve bireysel sağlık kayıtlarıdır. Bunlardan ilk olarak elektronik sağlık kayıtlarında, bir sağlık sisteminin gereksinim duyabileceği tüm sağlık verileri bulunmaktadır. Bireysel sağlık kayıtları ise, hastanın gereksinim duyduğu kişisel sağlık kayıtlarını barındırmaktadır. Bu sistemlerle elektronik sağlık kaydı yapılarak, iletişim ve bilgilere erişim kolay hale getirilse de, sağlık sistemi ile hasta arasında yeterince uyum sağlanması gerekmektedir (Tang ve Lansky 2005). Nitelikli bir sağlık hizmetinde, hastalardan verilerin elde edilmesi kadar hastaların bilgilendirilmesi sürecini de göz önünde tutulmalıdır. Hastaların kendi doktorlarına veya diğer sağlık uzmanlarına gerekli bilgileri iletebilme ve doktorlardan bilgi, ikaz ve tavsiye alabilmeli imkânları bulunmalıdır (Tang ve Newcomb 1998).

2.3.4. Hastane Bilgi Yönetim Sistemlerini Oluşturan Temel Bileşenler

HYBS geliştirilmesi esnasında bu sistemi kullanacak paydaşların gereksinimleri esas belirleyiciler olarak ön plana çıkmaktadır. Bu noktada sağlık çalışanlarının, yöneticilerin, tedarikçilerin, karar vericilerin ve hastaların paydaşlar olarak ortaya çıktığı görülmektedir. Bu kapsamda sağlık hizmetlerinin sunumu için kullanılacak bilgi sistemleri aşağıda da gösterildiği gibi genellikle üç sınıfta toplanabilmektedir (Tengilimoğlu ve ark. 2015);

- Klinik Bilgi Sistemleri
- Yönetim ve Finans Bilgi Sistemleri
- Stratejik Karar Destek Sistemleri

Tablo 2'de örnek bir HYBS modüler yapısı gösterilmektedir. Burada paydaşların kademelerine ve gereksinimlerine göre alt modüller ve sistemlerin dizayn edilmiş olduğu görülmektedir.

2.3.4.1. Klinik Bilgi Sistemleri

IOM'nin 1997'de yapmış olduğu tanımda Klinik Bilgi Sistemleri (KBS); "hastalara ait klinik bilgileri toplayan ve kullanılabilir hale getiren bir sistem" şeklinde ifade edilmiştir. Bu tanım kapsamında hasta bakımı ve klinik uygulamaları esas alan bu alanda her çeşit bilginin (resim, görüntü, yazı, ses vb.) toplanarak işlem gördüğü ve depolandığı, ayrıca karar verme aşamasında istifade edilen sistemler Klinik Bilgi Sistemleri şeklinde tarif edilmektedir (Güleş ve Özata 2005).

KBS hasta bakımıyla ile doğrudan ya da dolaylı biçimde ilişkili olan sistemdir. Sistem hasta bakımına destek sağlamak amacıyla düzenlenen bilgilerin oluşturulması, depolanması ve tekrar kullanılabilmesine olanak veren bir sistem şeklinde tanımlanmaktadır (Tengilimoğlu ve ark. 2015).

Diğer bir tanımlamaya göre KBS, teşhis ve tedavi hizmetlerine destek sağlayan ve doktorların daha etkin ve verimli klinik karar almalarına katkı sağlayan verileri oluşturan sistem şeklinde tanımlanmaktadır (Kavuncubaşı ve Yıldırım 2012).

2.3.4.2. Yönetimsel ve Finansal Bilgi Sistemleri

Yönetim Bilgi Sistemleri (YBS), yönetim kademesinde görev yapan yöneticilerin sürekli olarak değişen ortamda muhtelif kararları alabilmeleri amacıyla gerekli olan özel bir bilgi sistemi olarak tanımlanmaktadır. Sağlık kuruluşlarında YBS bölümler bazında fonksiyonları mevcuttur ve her bölümün gereksinimleri dâhilinde işlevlere sahiptir. YBS'nin içerdiği alt sistemler aşağıdaki sıralanabilmektedir (Tengilimoğlu ve ark. 2015);

- Muhasebe ve finansal yönetimi
- Programlama
- Malzeme yönetimi
- Ofis Otomasyonu
- İnsan kaynakları yönetimi (İKY)

YBS, kurumlarda bilgi üretimi ve akışını yöneten bilgisayar tabanlı sistemler olarak kısaca tanımlanabilir. Çoğunlukla yönetsel kontrol amacıyla ve orta düzey yöneticilere veriler sunmak için kullanılmaktadır. YBS, kurumların muhtelif bölümlerinde icra edilen faaliyet işleme sistemine ilişkin bilgileri toplamakta, bu bilgilerden kurum yöneticileri tarafından gereksinim duyulan özetler, tahminler, raporlar, analiz sonuçları vb. düzenlenmiş verileri üretmektedir. Öylelikle sistem, büyük hacimlerdeki veri işlemlerinde ve yapı ile alakalı problemlerin çözümü aşamasında başarılı bir biçimde kullanılabilmektedir. Ancak olağan dışı, özel, karmaşık problemlerin çözümünde ise yeterli düzeyde başarı elde edilememektedir. Kurum çevresi ile alakalı problemlerde YBS'nin yönetim düzeyi kararlara katkı verme imkânı kısıtlı kalabilmektedir. Pek çok sağlık kurumunda YBS'nin yönetim kademesine veri sunmak için muhtelif biçimlerde kurulduğu görülmektedir. Anılan sistemler çoğunlukla hasta ücretleri, ücret bordroları, muhasebe kayıtları geliştirmek amacıyla düzenlenen paket program oldukları görülmektedir. Genel olarak anılan paket programlar donanımlarla beraber tedarik edilmektedir. Ancak kurumlar paket programları satın almaktan ziyade kiralama yoluna da gidebilmektedir. Sonuç olarak YBS, HBYS'lerin bir alt sistemi şeklinde kurulmakta ve alt bir modül olarak kullanılabilmektedir (Çelik ve Tetik 2015).

2.3.4.3. Stratejik Karar Destek Sistemleri

Karar verme sürecini kolay hale getirebilmek, daha etkin ve doğru kararlar almak amacıyla tasarlanan; farklı model ve uygulamaları içeren sistemlere Karar Destek Sistemleri (KDS) adı verilmektedir. Temel olarak kurum bünyesinde alınacak üst kademe kararların doğru, sağlıklı ve gerekçeli şekilde alınmasına olanak tanıyan yazılımlar KDS olarak adlandırılmaktadır (Rajalakshmi ve ark. 2011). KDS, karar vericilere bir analiz sunmakta ve bu analize bağlı olarak bir karar tavsiyesinde bulunmaktadır. KDS'nin tanımlanmasında daha geniş özellikler mevcuttur ve bu özellikler aşağıdaki şekilde sıralanabilir. Buna göre KDS (İstanbul Sağlık Müdürlüğü);

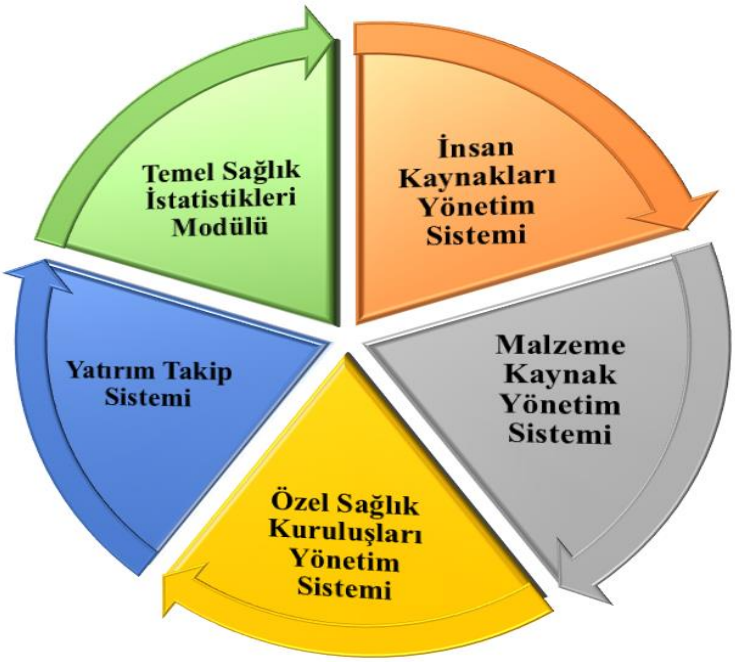
- Sağlık politika yapıcıları, planlayıcıları ve karar vericilerinin kullanımına yönelik analiz, raporlama ve istatistiksel destek sağlayan,

- Farklı kaynaklardan elde edilen bilgileri düzenleyerek, kararın modellemesini yaparak, verilerin analizini yaparak ve değerlendirme sonuçlarını sunarak belirli modellerin kullanımıyla karar verici bireylere tercih esnasında destek sağlayan,

- Kullanıcıların kavrama ve bilme ile alakalı bilişsel becerilerini geliştirerek karar almasına yardımcı olmak amacıyla tasarlanmış olan,

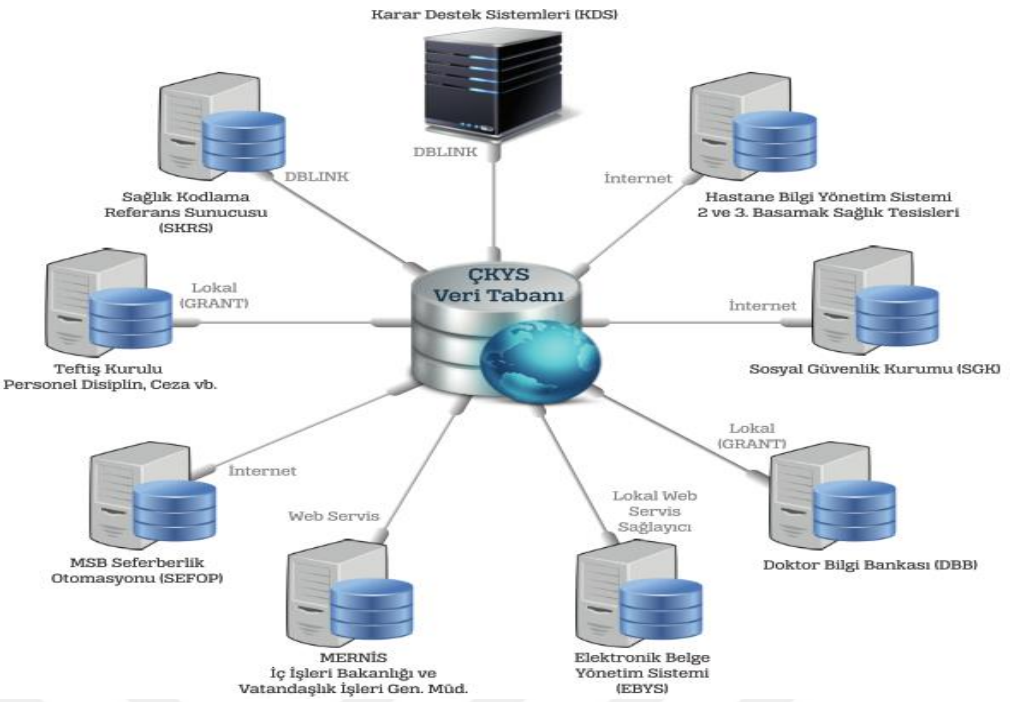
- Yöneticilerin karar verme ve veriler ulaşma, verileri özetleme ve veri analizi faaliyetlerine yardımcı olan bir sistem olarak ön plana çıkmaktadır.

Sağlık Bakanlık sağlık hizmetlerinde stratejik bir kademe olarak, sağlık hizmetleri sunumu kapsamında tek sorumlu ve otorite olması nedeniyle, üniversite hastanelerinden, özel sağlık kurumlarından, koruyucu ve tedavi edici sağlık kurumlarından geniş çapta bilgileri ve verileri toplamaktadır. Bilgiler ve verilerin Karar Destek Sistem (KDS)'lerinde işlenerek, başta sağlık hizmet veren kurumlara ve diğer paydaşlara, müteakiben diğer kullanıcılara yol göstermek maksadıyla veri ambarlarında depolanması, gelecekte meydana gelebilecek muhtemel risklere karşısında tedbirli olma önlemini sağlamış olacaktır.



Şekil 3: Sağlık Bakanlığı Çekirdek Kaynak Yönetim Sistemi Bileşenleri (istanbulsaglik.gov.tr).

Stratejik Karar Destek Sistemleri örneklerinden biri de T.C. Sağlık Bakanlığı tarafından kullanılmakta olan Çekirdek Kaynak Yönetim Sitemi (ÇKYS)'dir. Bu proje 1 Eylül 1997 tarihinde Dünya Bankası Projesi kapsamında destek sağlanarak geliştirilmiştir. Bu sistem Sağlık Bakanlığı Merkez Teşkilatı (SBMT) ve il sağlık müdürlükleri tarafından istifade edilmekte olan bir sistemdir. ÇKYS ile insan kaynakları yönetimi, malzeme kontrolü, finans kaynakları yönetimi, eczacılık işlemleri yönetimi modern bilgi ve iletişim sistemleri kullanılarak icra edilmektedir. Bu sistem sayesinde yönetim faaliyetleri çok daha etkin ve verimlilik içerisinde kurumsal bir yaklaşımla hayata geçirilebilmektedir. Bu sistemin entegre çalışan 5 ana modülü mevcuttur. Bunlar Şekil 3'te gösterilmektedir.



Şekil 4: Çekirdek Kaynak Yönetim Sistemi İletişim Ağı Mimarisi (RMA 2014).

ÇKYS sisteminin iletişim ağı mimarisi Şekil 4'te gösterilmektedir. Buradaki mimari incelendiğinde yukarıda ifade edilen temel bileşenlerin alt yapısının mevcut olduğu görülmektedir. Ayrıca Milli Savunma Bakanlığı bağlantısı ile seferberlik işlemlerinin koordine edilmesi ve İç İşleri Bakanlığı bağlantısı ile de MERNİS sisteminden vatandaşlık bilgilerinin alınması sağlanmaktadır.

ÇKYS, Sağlık Bakanlığının hem devlet sağlık kurumlarının ve hem de diğer sağlık hizmetleri sunumu yapan diğer kurumların ihtiyaç duyduğu her çeşit verinin muhafaza edildiği ve depolandığı, uygulamaya geçecek bütün hizmetlerin değerlendirildiği veri ambarı modeli olarak görev yapar. Bu model ile Sağlık Bakanlığının pek çok bağlısı birimlerinin, sahadan muhtelif vasıtalarla aldığı verileri bilgi ve iletişim teknolojilerinin getirdiği olanaklarla elektronik ortamda, tek bir yolla yineleme olmadan, doğrudan üretilmiş olduğu noktada, standartlara uygun biçimde toplayarak karar destek sistemi raporları verilmesi hedeflenmiştir (T.C. Sağlık Bakanlığı 2013).

2.3.5. Hastane Bilgi Yönetim Sistemlerinin Kullanım Alanları

Sağlık sektöründe kullanılan bilgi sistemleri ilk başlarda yalnızca doğru faturalama ve irsaliye düzenlenmesi ihtiyacından doğmuş, zamanla gelişerek

hastanelerde yapılan aşağıda sıralanan işlemleri de kapsamıştır. Bu kapsamda HYBS'ler (Rodoplu 2007);

- Hasta kimlik bilgilerinin kayıtları,
- Tetkik kayıtları,
- Muayene bilgileri kaydı,
- Randevu işlemleri,
- Rapor ve reçete düzenleme,
- Laboratuvar sonuçlarının transferi ve sergilenmesi,
- Elektronik hasta kayıtlarının tutulması,
- Stok takibi ve kontrolü,
- Yönetim raporlarının düzenlenmesi,
- Kalite verilerinin analiz edilmesi gibi işlemleri de içeren süreçlere doğru evirilmiştir.

Bundan dolayı HYBS'nin esas fonksiyonu, kullanıldığı kurumun bilgi taleplerine doğru, zamanında ve tam olarak cevap vermektir. Bu minvalde bu sistemlerden, bir hastanenin günlük işlemlerinde (randevu, sevk, hastanın başvuru, kabul, sağlık durumu, laboratuvar, taburcu kayıtları gibi), hastaya yapılan teşhis ve tedaviye ait uygulamalarda (klinik, laboratuvar, radyoloji, ameliyathane, eczane, terapi ve diyet gibi), genel yönetim faaliyetlerinde (sabit tesis, personel, cihaz ve malzeme durumu ve yönetimi vb.) ve mali işlemlerde (müşteri hesapları, muhasebe ve vergilendirme vb.) çok yoğun bir biçimde istifade edilmektedir (Köksal ve Esatoğlu 2005).

2.3.6. Hastane Bilgi Yönetim Sistemlerinde Bilgi Güvenliği

Günümüz ortamında hastaneler, sendikalar, adli tıp kurumları vb. birçok kurum tarafından bireylerin sağlık durumları, cinsel yaşamları, DNA örnekleri veya siyasi görüşleri gibi bilhassa gizliliğini korumasını isteyecekleri bilgiler veri yapıları şeklinde kayıt altına alınmakta ve arşivlenmektedir. Bu verilerin kanunlardan veya bireylerin vermiş olduğu izinlerden kaynaklanmayan bir biçimde hukuka aykırı şekilde bilişim sistemlerine kaydedilmesi ve depolanması TCK'nın 135 maddesi ile suç olarak tanımlanmıştır. Böylece gerek kişiler gerekse de kurumlar açısından,

insanların kişisel bilgilerini sanal ortamlarda veya yazılı ortamlarda kayda alırken veya arşivleme esnasında çok daha özenli davranmak zorunluluğu getirilmiştir (Dülger 2011).

2.3.6.1. HBYS Bilgi Güvenliğinin Hukuki Dayanakları

Ülkemizde bireylerin sağlık bilgilerinin muhafaza edilmesine ve gizliliklerine ait muhtelif düzeylerde kayda değer düzenlemeler yapılmış ve yürürlüğe girmiştir. 3359 sayılı Sağlık Hizmetleri Temel Kanunu'nun 3. Madde f fıkrası "Herkesin sağlık durumunu takip edebilmek için gerekli kayıt ve bildirim sistemi kurulur" hükmünü ortaya koymaktadır. Bu düzenleme ile bilgi sistemleri açısından kayda değer bir yasal dayanak oluşturulmuştur. Bununla beraber doktorların ve diğer sağlık çalışanlarının sorumluluğuna ait hükümler kanunda mevcuttur. Bu konuyla alakalı düzenlemelerin çoğunluğu da ilgili yönetmelikler ve etik kuralların belgelerinde belirtilmiştir (Küzeci 2010).

2.3.6.2. HBYS'de Bilgi Güvenliği Önlemleri

Kişisel verilerin elde edilmesi, kayıt altına alınması, düzenlenmesi, muhafaza edilmesi, üzerinde değişiklik yapılması, birleştirilmesi, okunması, uyarlanması, sorgulanması, kullanılması, erişilebilir duruma getirilmesi, açıklanması, transfer edilerek başka kişilere verilmesi, yayılması veya hazır bulundurulması amacıyla icra edilen işlemlerin yanında verilerin kombinasyonu veya ilişkilendirme işlemlerinin yapılması ve hatta engellenmesi, silinmesi veya imha edilmesi yoluyla yapılan her çeşit işlem veya işlemlerin tamamı kişisel verilerin işlenmesi bağlamında değerlendirilmektedir. Veri işleme, otomatik veya otomatik olmayan işlemlerle icra edilen kişisel veriler ile alakalı olabilecek her çeşit süreci kapsar. Otomatik işleme sürecinden ifade edilen, verilerin bilgisayar ve sunucular vb. otomasyon sistemleri kullanılarak işlenmesidir. Böylece verilerin elde edilmesinden itibaren, işlem yapılan bütün evreleri içeren tüm işlemler koruma ve kayıt altında tutulmaktadır (Dülger 2015).

2.3.6.3. Veri Güvenliği Açısından Tehditler

Sağlık bilgi sistemlerinde veri güvenliği açısından oluşan tehditler sistematik ve organizasyonel olarak iki ana grupta ele alınmaktadır (Rindfleisch 1997).

● Organizasyonel Tehditler**:** Bu tür tehditler, sistem içerisinden ya da dışından hasta bilgilerine uygunsuz ve izinsiz şekilde erişim sağlamaya çalışma kaynaklıdır. Bilgi sistemlerine erişim yetkisi olan dâhili tehdit unsurlarının da yetkilerini kötüye kullanabildikleri görülmektedir. Ayrıca harici tehdit unsurlarının da sistemin açıklarından istifade ederek sisteme yetkisiz biçimde erişim sağlamaya çalıştıkları görülmektedir. Hastaların sağlık bilgilerine karşı yapılan saldırıların çok büyük bir bölümü ekonomik sebeplerle yapılmaktadır. Buna ilişkin bilgiler özel sağlık kurumları, sigorta şirketleri ve muhtelif suç örgütleri bakımından mali anlamda yüksek değere sahip olan veriler olarak öne çıkmaktadır (Rindfleisch 1997).

● Sistematik Tehditler: Sağlık bilgi sistemlerinde gizlilik ve güvenlik ihlallerinin çok büyük bir bölümünün, bilgi sistemine yasal şekilde erişim yetkisi olan bireyler tarafından verilerin sistematik şekilde farklı gayelerle kullanılması sonucu oluştuğu da gözlenmektedir (Etzioni 1999). Örnek olarak sigorta şirketlerinin hasta sağlık bilgilerini hastaların tedavi giderlerini karşılamak amacıyla kullanmasına ilave olarak, bu bilgilerin analizini yaparak insanların sağlık riskleri konusundan hesap yapmak amacıyla da kullanmaları sistematik ihlal olarak görülmektedir. Diğer taraftan işverenlerin, çalışan adaylarını sağlık durumlarına bağlı olarak seçmesinin de sistematik mahremiyet ihlali açısından örnek teşkil ettiği söylenebilir.

2.3.6.4. Bilgi Güvenliği Önlemleri ve Kimlik Doğrulama

Bilgi güvenliğinin sağlanması kapsamında birçok modern yöntemlerden faydalanılmaktadır. Bu kapsamda kimlik doğrulama, sertifikalı erişim sağlama, VPN (Virtual Private Network) kullanma gibi bilgi güvenliğine ilişkin önlemler alınmaktadır (Sağlık Bakanlığı 2005).

Bilgi sistemlerinin iletişim halinde olan alt sistemleri bilgi güvenliği açısından birbirlerini doğrulamaları gerekir. Bundan ötürü kimlik doğrulama metotları güvenliğin sağlanması açısından bir ön şart halini almıştır. Sağlık bilgi sistemlerinin bilgi güvenliğinin sağlanması açısından koşul çok ciddi seviyede öneme sahiptir. Bundan dolayı, tüm sağlık çalışanlarının erişime yetkilendirildikleri hasta verilerine ulaşmadan önce kimlik doğrulama sürecinden geçmeleri gerekmektedir (Sun ve ark. 2010).

Sağlık bilgi sistemlerinde kimlik doğrulama metotları birçok farklı şekilde yapılabilmektedir. Burada kimlik doğrulama metotları yalnız başına kullanılabileceği gibi farklı kimlik doğrulama metotlarıyla beraber de kullanılabilmektedir.

● Parola Kullanımı Yoluyla Kimlik Doğrulama: Sağlık bilgi sistemleri kapsamında en fazla istifade edilen kimlik doğrulama metodu diğer sistemlerde olduğu şekilde, doğrulama için bir kullanıcı numarasıyla beraber parola kullanılmasıdır. Kullanıcı numarası ve parolası özel bir veri tabanı içerisinde kaydedileceği gibi birçok alt sistemlerin ortaklaşa kullanmakta olduğu bir veri tabanında da tutulabilmesi de mümkündür. Kullanıcı numarası veri tabanında şifrelenmeden açık biçimde kaydedilmesine karşın, PIN veya parola veri tabanında şifreli biçimde saklanır. Kullanıcı tarafından numara yazıldıktan sonra numara veri tabanında bulunan numaralarla karşılaştırılır. Girilen numara veri tabanındaki numaralardan biri ile eşleşmesi durumunda girilen parola şifrelenerek veri tabanında var olan şifrelenmiş parolayla karşılaştırılır. Parola da eşleşmesi halinde kimlik doğrulama işlemi yapılmış olur (Wager ve ark. 2009).

Yalnızca kullanıcıların bildiği verileri içeren kimlik doğrulama türü olan parolayla kimlik doğrulama metodu kullanılarak oluşturulan tek aşamalı kimlik doğrulamanın yeterli seviyede güvenlik sağlamadığı söylenebilir. Çok daha güvenilir bir yöntem olan iki aşamalı kimlik doğrulama metotlarının kullanılması daha yararlı ve güvenli olmaktadır. İki aşamalı kimlik doğrulama sistemlerinde, kullanıcı tarafından ezberlenmesi gereken bilgilerin olmadığı ikinci bir aşama mevcuttur. Örnek olarak, iki aşamalı kimlik doğrulama sistemlerinde birinci aşama parolayla kimlik doğrulama metodu, ikinci aşama da biyometrik kimlik doğruma metodu olabilir. Ayrıca ikinci aşama olarak kullanıcılara tek kullanımlık şifrelerin her erişimde gönderilmesi metodu da güvenlik seviyesini artırmaktadır (Chess ve Arkin 2011).

● Biyometrik Kimlik Doğrulama: Kimlik doğrulama yöntemlerinden bir diğeri de kimlik doğrulamada biyometrik bilgilerin kullanılmasıdır. Biyometrik sistemler, parmak izi, insan yüzünün şekli, avuç içi izi, iris ve ses vb. anatomik özellikleri kullanarak kişileri tanımlamakta ve yürüyüş şekli, tavır, hal ve hareketler, ıslak imza gibi davranış şekilleri ile de tanımlama yapabilmektedir. İlgili özellikler, kişiye has olması hasebiyle biyometrik sistemlerin içerisinde kimlik doğrulama

yönteminde istifade edilmektedir. Bu metot, sağlık bilgi sistemlerine erişim sağlamak isteyen kullanıcıların belirlenmesinde çok güvenli bir yöntemdir. Bu yöntem diğer taraftan inkâr edilmesi mümkün olmayan kanıtlar ve kayıtlar sunan bir kimlik doğrulama yöntemi olarak öne çıkmaktadır (Jain 2012).

Bu kimlik doğrulama metodu kimlik doğrulama esnasında harcanan süreyi kısaltması nedeniyle sağlık bilgi sistemleri kapsamında iki fazlı kimlik doğrulama işlemlerinde kullanılmaktadır. Yeni geliştirilmiş olan kimlik doğrulama yöntemleri arasında olan ekran parmak izi metodu iki fazlı kimlik doğrulama sistemleri kapsamında ikinci faz şeklinde kullanılabilmektedir. Metotla ilgili kullanıcılar tarafından sistem içerisinde yapmış oldukları tüm işlem ve hareketleri kayıt altına alarak, meydana getirdiği kayıtlar ile bir veri seti oluşturur. Güvenlik açısından bir önlem olarak, kullanıcılar tarafından açılan oturumlarda ilgili veri setlerinden farklılık arz edecek şekilde sistemde dolanım yapılıyorsa sistem bir hata vererek oturumu sonlandırmaktadır (Patel ve ark. 2013). Böylece veri seti için oluşturulan yapılar dışında veriler üzerinde kurallar dışında işlem yapmanın önüne geçilmiş olur.

- Ağ Güvenliğine İlişkin Yöntemler: Sağlık bilgi güvenliği ağına dışarıdan veya içeriden yetkisiz erişim sağlayarak bilgileri hukuksuz şekilde elde etmeye çalışan tehditlere karşı yapılması gereken bir takım önlemler mevcuttur. Örneğin bilgi sistemlerine dışarıdan yapılan saldırılara karşı güvenlik duvarı ve anti-virüs yazılımların kullanılması çok yaygın bir metottur (Ülgü 2008).

Diğer taraftan kurum içinde ya da kurumla diğer ağlar arasında gerçekleşen veri trafiği şifreli ve kriptolu olarak yapılarak yetkisiz kişilerin erişimi engellenmelidir. İlaveten tüm haberleşmelerde VPN ve Açık Anahtar Alt Yapısı (PKI) teknolojilerini kullanmalıdır (Sağlık Bakanlığı 2005).

2.4. Konu İle İlgili Yapılmış Önceki Çalışmalar

Yazar	Çalışma	Sonuçlar
Eminağaoğlu ve Gökşen (2009)	Bilgi Güvenliği Nedir, Ne Değildir, Türkiye' de Bilgi Güvenliği Sorunları ve Çözüm Önerileri	Araştırma sonucunda bilgi güvenliğinin doğru ve etkin yönetimi için üst yönetimden başlayarak tüm çalışanların bilinçlendirilmesi olarak tespit edilmiştir. Kurumun kendine uygun çözümler üretip bunları uygulaması ve düzenli denetimi bilgi güvenliğini olumlu etkilemektedir. Bilgi güvenliğinin sürdürülebilirliği için belli bir rutine bağlanmasıyla değil sürekli güncel tutularak yenilikleri takip etmesiyle mümkün olduğu sonucuna ulaşılmıştır.
Aksu (2014)	Hastane Bilgi Yönetim Sisteminin Bilgi Güvenliği Açısından Değerlendirilmesi	İstanbul'da seçilen bir özel hastanede yapılan çalışmada bilgi sistemlerinde yapılan bir değişiklik karşısında çalışanların direnç gösterdiği tespit edilmiştir. Çeşitli nedenlerden dolayı sistemdeki uygulamaların yetersiz olduğu düşüncesi bile reddedilmesine yol açacağını ve sistemin başarılı olması çalışanların kabulüne bağlanmıştır. Özellikle tıbbi birimde çalışanlarının bekledikleri gibi olmayan sistem için çaba göstermeyi bir yük olarak görmesi ve bunun sonucu olarak bilgi güvenliğine gereken özeni göstermedikleri tespit edilmiştir.
Dülger (2015)	Sağlık Hukukunda Kişisel Verilerin Korunması ve Hasta Mahremiyeti	Bu çalışmada hastaların sır ve kişisel bilgilerinin sağlık kurumlarınca güvende tutulduklarına inanmadığı ve bunun sağlık hizmeti almakta çekimser davranış gösterilmesi ön görülmüştür. Bu nedenle sadece kişinin mahremiyeti değil yaşam hakkı olarak da önemli olduğu sonucuna ulaşılmıştır. Buna ek olarak, hasta mahremiyeti adına uygulanan prosedürlerin olmasına karşın ihlal edilmesi durumlarıyla sıklıkla karşılaşıldığı tespit edilmiştir.
Erçoban ve ark. (2018)	Devlet Hastanesi Çalışanlarının Bilgisayar Kullanım Becerilerinin Değerlendirilmesi	Hastanede yapılan araştırmada çalışanların bilgisayar eğitimlerinin eksik olmasından kaynaklı donanımsal sorunların ortaya çıktığına ulaşılmıştır. Dijitalleşme sürecinde kullanım becerilerini en çok yaşın etkilediğine ulaşılmıştır.

3. GEREÇ VE YÖNTEM

3.1. Araştırmanın Amacı ve Önemi

Günümüzde HBYS sağlık hizmet sunumunun önemli bir parçası olarak kullanılmaktadır. Gittikçe önemi artan bilgi güvenliği yönetimi ve teknolojik gelişmeleri uyum sağlamak, gerekli tedbirleri alabilmek ve alanındaki her türlü bilgi ve beceriyi doğru aktarabilmek için HBYS, çalışanlar açısından önemli bir yere sahiptir. Çünkü hasta bilgilerinin doğru şekilde sisteme aktarılmasıyla birlikte, iletilmesi ve yetkili kişilerce kullanımının sağlanması kurumun hizmet sunumunda oldukça önemli etkiye sahiptir. Ayrıca sistem çalışanlara, hastaların doğru tedaviye yönlendirmek ve sonrasında başarılı bir tedavi sürecini sağlamak adına kolaylık ve pratiklik sağlama noktasında etkin roller yüklemektedir. Yapılan literatür taramasında Türkiye'de bilgi güvenliği bağlamında sağlık hizmetlerinin değerlendirmesini içeren çalışmalar tespit edilmiştir. Ancak genel olarak HBYS'nin kullanımında bilgi güvenliğinde durum tespitinin değerlendirildiği çok az çalışma ile karşılaşılmıştır. Sağlıkta bilgi güvenliğinin değerlendirilmesi ileride yapılacak uygulamalar ve izlenecek güvenlik politikaları açısından önemli olarak görülmektedir.

Çalışmanın amacı Süleyman Demirel Üniversitesi Araştırma ve Uygulama Hastanesi çalışanlarının, HBYS'yi ve sistemin bilgi güvenliği açısından değerlendirilmesidir. Ayrıca, çalışanların ihtiyaç duyulan talebin karşılanırken HBYS'nin doğru ve etkili kullanımı ile hasta mahremiyetine uygun bilgi güvenliğinin yeterli düzeyde olduğunu görmektir. Bu çalışma sonucunda çalışanların vermiş olduğu cevaplar neticesine göre bilgi güvenliğinde yetersiz kalınması durumunda; HBYS'de iyileştirmeler ve geliştirmeler yapılmasının gerekli olacağı düşünülmektedir. Son olarak, bu alanda yapılacak olan yeni çalışmaları besleyeceği için hem literatür hem de eğitim açısından önemli bir yere sahip olacağı düşünülmektedir.

3.2. Araştırma Evreninin Belirlenmesi ve Örneklemi

Araştırmanın evrenini Isparta merkezinde bulunan Süleyman Demirel Üniversitesi Araştırma ve Uygulama Hastanesi'ndeki HBYS'yi kullanan tıbbi birimde hekim, hemşire, tıbbi sekreter ve idari birimde masa başı personel ile birlikte

toplam 1265 çalışan oluşturmaktadır. Örneklem evren üzerinden basit tesadüfi örnekleme yöntemi ile belirlenmiştir. Ulaşılması gereken en az örneklem sayısı 1265 kişilik evrenden aşağıdaki formül (İslamoğlu 2009) ile hesaplanarak %95 güven düzeyinde 295 olarak bulunmuştur.

$$n = \frac{Z^2PQ}{E^2 + \frac{Z^2PQ}{N}} = \frac{1{,}96^2.0{,}5.0{,}5}{0{,}05^2 + \frac{1{,}96^2.0{,}5.0{,}5}{1265}} = 295$$

Formülde verilen parametrelerin anlamları ise şunlardır:

Z: 1,96 (Standart normal değişken = %95 güven düzeyinde)

N: Evren büyüklüğü

P: Anakütle oranı = (%50) 0,5 sapma payı (Maksimum hata olarak alındı),

Q: 1-P = 0,5

E: Varsayılan hata (%5) = 0,05

3.3. Veri Toplama Yöntemi

Veriler araştırmacı tarafından yüz yüze görüşme yöntemi kullanılarak 12.04.2018-25.07.2018 tarihleri arasında toplanmıştır. Bu çalışmada veri toplama yöntemlerinden anket kullanılmıştır. Örneklemde toplam 352 kişi bulunmaktadır. Anketlerin bir kısmı e-mail üzerinden bir kısmı ise yüz yüze doldurulmuştur. Sorunlu anketler ayıklanarak 317 anket analize tabii tutulmuştur.

3.3.1. Boyutların Psikometrik Özellikleri

Araştırmalar sonucu elde edilen veri setinin normal dağılım sergileyip sergilemediğini yorumlayabilmek için basıklık ve çarpıklık katsayılarının -1 ile +1 arasında bir değer alması gerekmektedir (Morgan ve Leech 2004). Tablo 3.3.1'e bakıldığında bu çalışmanın basıklık ve çarpıklık katsayılarının -1 ile +1 arasında değerlerler aldığı görülmektedir. Bu sebeple veri setinin normal dağılıma uygun olduğu görülmüş ve verilerin analizinde parametrik testler kullanılmıştır.

Bilgi güvenliği alt boyutlarına ait ortalama puanlar incelendiğinde en yüksek ortalamanın hizmet sunumu boyutunda, en düşük ortalamanın ise güvenlik uygulamaları boyutunda olduğu görülmektedir (Tablo 3.3.1).

Tablo 3.3.1. Boyutların Psikometrik Özellikleri

Boyutlar	İfade Sayısı	Max-Min	Cronbach Alfa	Normallik Testi	
				Kurtotis (Basıklık)	**Skewness (Çarpıklık)**
Erişim ve Yetkilendirme	9	1-5	0,88	-0,06	-0,32
Güvenlik Uygulamaları	5	1-5	0,77	0,10	-0,32
Hizmet Sunumu	4	1-5	0,84	-0,17	-0,42
Örgütsel Güvenlik	5	1-5	0,80	0,17	-0,37
Güvenlik Politikaları	4	1-5	0,83	-0,35	-0,14

Tablo 3.3.1'de verilen her bir boyuta ait bilgiler aşağıda verilmiştir:

- **Erişim ve Yetkilendirme Boyutu:** Bu boyut 9 ifadeden oluşmaktadır. Bu boyuttaki ifadeler ile katılımcılardan, HBYS' de kimin hangi yetkilerle sınırlandırıldığı, kullanıcı-yönetici hesaplarının oluşturulması ve standartlarının belirlenmesi, kaynak erişim hakları gibi konularda değerlendirme alınmıştır. Erişim ve Yetkilendirme boyutunun aritmetik ortalaması 3,64 ve standart sapması 0,79 olarak bulunmuştur. Boyutun güvenilirlik derecesi (Cronbach Alpha) ise 0,88 olarak yüksek derecede güvenilir bulunmuştur.
- **Güvenlik Uygulamaları Boyutu:** Bu boyutta 5 ifade yer almaktadır. Bu boyut altında yetkisiz erişimlerin engellenmesi, bilginin aslının korunması ve bunun için gereken denetimin ve ölçümlerin belirlenmesi, denetimlerin belgelendirilerek devamlılığın sağlanmasına dair ifadeler toplanmıştır. Güvenlik Uygulamaları boyutunun aritmetik ortalaması 3,00 ve standart sapması 0,92 olarak bulunmuştur. Boyutun güvenilirlik derecesi (Cronbach Alpha) ise 0,77 olarak güvenilir bulunmuştur.
- **Hizmet Sunumu Boyutu:** Bu boyutta 4 ifade yer almaktadır. Bu boyut altında hastaya ait bilgilerin, çalışanlar tarafından yapılan işlemlerce bakanlığa elektronik ortamda güvenli şekilde aktarımı ve ihtiyaç dahilinde başka yetkililerin erişimine dair ifadeler toplanmıştır. Hizmet Sunumu boyutunun verildiği üzere aritmetik ortalaması 3,65 ve standart sapması 0,95 olarak bulunmuştur. Boyutun

güvenilirlik derecesi (Cronbach Alpha) ise 0,84 olarak yüksek güvenilir bulunmuştur.

- **Örgütsel Güvenlik Boyutu:** Bu boyutta 5 ifade yer almaktadır. Bu boyut altında bilgi güvenliğini temel alarak belirlenen politikalara dair ifadeler toplanmıştır. Örgütsel Güvenlik boyutunun aritmetik ortalaması 3,43 ve standart sapması 0,85 olarak bulunmuştur. Boyutun güvenilirlik derecesi (Cronbach Alpha) ise 0,80 olarak yüksek güvenilir bulunmuştur.
- **Güvenlik Politikaları Boyutu:** Bu boyutta 4 ifade yer almaktadır. Bu boyut altında çalışanların sorumluluklarını, güvenliğin denetim araçlarının kullanımına ve sürecin yönetilmesindeki prensip ve işletime dair ifadeler toplanmıştır. Güvenlik Politikaları boyutunun aritmetik ortalaması 3,24 ve standart sapması 1,00 olarak bulunmuştur. Boyutun güvenilirlik derecesi (Cronbach Alpha) ise 0,83 olarak yüksek güvenilir bulunmuştur.

3.4. Anket Formunun Hazırlanması

Araştırma verilerinin toplanmasında çalışanlarına 55 soruluk anket formu (Ek-A) kullanılmıştır. Araştırmada kullanılan anket; bilgi güvenliği ölçeği ve bilgi güvenliği konusunda yapılan araştırmalardan yola çıkılarak hazırlanan sorulardan oluşmaktadır. Bu yapılandırılmış anket formunda; tıbbi ve idari bölümde çalışanlara ait kişisel özellikler ve bilgi güvenliğine yönelik sorular yer almaktadır.

Araştırmada bilgi güvenliği ölçeği olarak, Upfold ve Sewry (2005) tarafından geliştirilen ve Aksu (2014) tarafından Türkçeye çevrilen sağlık alanı dışında kullanılan bir ölçek ile çalışılmıştır. Ölçeğin puanlama yöntemi orijinal ölçekte olduğu gibi 5'li Likert Skalası (1: Kesinlikle Katılmıyorum, 2:Katılmıyorum, 3:Orta Derecede katılıyorum, 4:Katılıyorum, 5:Kesinlikle Katılıyorum) ile değerlendirilmiştir. Anket formu iki bölümden oluşmaktadır. İlk bölümde yer alan 1-13 numaralı sorular, katılımcının kişisel özelliklerine yöneliktir. İkinci bölümde bulunan 14-55 numaralı sorular ise bilgi güvenliğine yönelik sorulardır. Ölçekte yer alan 4 soru diğer sorular ile uyumlu olması açısından ters puanlanmıştır.

3.5. Analiz ve Yöntem

Araştırmacı tarafından anket formları aracılığıyla elde edilen veriler Statistical Package for the Social Sciences (SPSS 24.0) programı kullanılarak analiz edilmiştir.

Anketten elde edilen veriler aritmetik ortalama, standart sapma, frekans ve yüzde hesaplamaları ile analiz edilmiş ve istatistiksel değerlendirmeler bu puan ortalamaları üzerinden yapılmıştır. Daha sonra veriler normallik testine tabi tutulmuştur. Verilerin normal dağılıma uygun olup olmadığını tespit etmek için her bir boyutun çarpıklık ve basıklık değerleri bulunmuştur (Tablo 3.3.1). Bütün boyutlarda veriler normal dağılım gösterdiği tespit edildikten sonra parametrik testler yapılmıştır. Parametrik testlerden ikili grupların karşılaştırılmasında "t-testi"; üç ve üzeri grupların karşılaştırılmasında "ANOVA" kullanılmıştır. analizi sonucunda gruplar arasında fark bulunduğunda, farkın kaynağını "Tukey Testi" ile tespit edilmiştir.

3.6. Araştırmanın Etik Boyutu

- Araştırmanın yürütülebilmesi için Necmettin Erbakan Üniversitesi Sosyal Beşeri Bilimler Etik Kurulundan 19.02.2018 tarihli 2018/3 sayılı (Bkz. EK-A) kararı ile etik kurul izni alınmıştır.
- Araştırmanın ilgili kurumlarda yürütülebilmesi için Süleyman Demirel Üniversitesi Araştırma ve Uygulama Hastanesi Başhekimliği Kalite Yönetim Biriminden 12.04.2018 tarihli ve E.117493 sayılı izin (Bkz. EK-B) alınmıştır.
- Katılımcılara araştırma ile ilgili açıklama anket formunun ön kısmında belirtilmiştir ve sözel onam alınmıştır.

3.7. Araştırmanın Sınırlılıkları

Araştırma Isparta'daki Süleyman Demirel Üniversitesi Araştırma ve Uygulama Hastanesi'nde HBYS'yi kullanan çalışanları kapsaması sınırlılık oluşturmaktadır. Bulgular ve sonuçlar, sadece bu kurum için geçerlidir. Araştırmanın Türkiye'de bulunan diğer üniversite hastanelerini genelleyebilmesi için daha geniş kapsamlı örneklem üzerinde çalışılması gerekmektedir.

3.8. Araştırmanın Soruları

Araştırmanın amacına yönelik sorular hazırlanmıştır. Bu sorular şunlardır;

1. HBYS kullanımı sırasında ulaşılabilen bilgi türleri açısından tıbbi ve idari birimler arasında fark var mıdır?
2. HBYS‘ de günlük işleyiş sırasında kullanılan bilgiler açısından tıbbi ve idari birimler arasında fark var mıdır?
3. HBYS’ de koruma altındaki bilgiler açısından tıbbi ve idari birimler arasında fark var mıdır?
4. Tıbbi birim çalışanları ile idari birim çalışanları arasında bilgi güvenliğinin korunması konusunda fark var mıdır?
5. Farklı yaş gruplarındaki HBYS eğitimi olan çalışanlar arasında bilgi güvenliğinin korunması konusunda fark var mıdır?
6. Farklı cinsiyetteki HBYS eğitimi olan çalışanlar arasında bilgi güvenliğinin korunması konusunda fark var mıdır?
7. Farklı eğitim gruplarındaki HBYS eğitimi olan çalışanlar arasında bilgi güvenliğinin korunması konusunda fark var mıdır?
8. Farklı kıdemdeki HBYS eğitimi olan çalışanlar arasında bilgi güvenliğinin korunması konusunda fark var mıdır?

4.BULGULAR

4.1. Katılımcıların Demografik Değişkenlere Göre Dağılımı

Bu bölümde araştırmaya katılan Süleyman Demirel Üniversitesi Araştırma ve Uygulama Hastanesi çalışanlarının tanımlayıcı bulgularına yer verilmektedir.

Tablo 4. 1. Katılımcıların Tanımlayıcı Bulguları

Değişkenler		**Frekans**	**Yüzde (%)**
Pozisyon	Tıbbi	210	66,2
	İdari	107	33,8
Eğitim	Lise	104	32,8
	Yüksekokul	84	26,5
	Lisans	98	30,9
	Y. Lisans ve üzeri	30	9,8
Yaş	20-29	119	37,5
	30-39	135	42,6
	40-59	63	19,9
Cinsiyet	Kadın	191	60,3
	Erkek	126	39,7
Medeni Hal	Evli	203	64.0
	Bekar	114	36.0
Aylık Gelir	1603 TLve altı	48	15,1
	1.604-2.000 TL	131	41,3
	2.001-3.000TL	42	13,2
	3.001 TL ve üzeri	96	30,3
Kurumda Çalışma Süresi	0-1 Yıl	45	14,2
	1-5 Yıl	87	27,4
	5-10 Yıl	74	23,3
	10 Yıl ve üzeri	111	35,0
HBYS Deneyim	0-1 Yıl	66	20,8
	1-5 Yıl	81	25,6
	5-10 Yıl	71	22,4
	10 Yıl ve üzeri	99	31,2
HBYS Eğitim Alınması	Evet	183	57,7
	Hayır	134	42,3
HBYS Eğitim Süresi	0-1 Hafta	174	54,9
	1 Hafta- 1 Ay	60	18,9
	1-3 Ay	33	10,4
	3 Ay ve üzeri	30	9,5
HBYS Eğitim Yeterliliği	Yetersiz	75	23,7
	Kararsız	105	33,1
	Yeterli	117	36,9
Bilgisayar Kullanım Becerisi	Yetersiz	33	10,4
	Kararsız	75	23,7
	Yeterli	209	65,9

Tablo 4.1'e bakıldığında 191 (%60,3) katılımcının kadın, 126 (%39,7) katılımcının ise erkek; bunların 203'ü (%64,0) evliyken, 114'ünün (%36,0) bekar olduğu tespit edilmiştir. 119 (%37,5) katılımcının 20-29, 135 (%42,6) katılımcının ise 30-39, 63 (%19,9) katılımcının 40 ve üzeri yaş aralığında olduğu görülmektedir.

Katılımcıların eğitime göre dağılımında bakılırsa katılımcıların 104'ü (%32,8) lise, 84'ü (%26,5) yüksekokul, 98'i (%30,9) lisans, 30'u (%9,8) yüksek lisans ve üzeri mezundur. Katılımcıların 210'u (%66,2) tıbbi, 107'si (%33,8) idari birimde çalışmaktadır. Çalışanların kurumda çalışma süresine bakıldığında; 45'i (%14,2) 0-1 yıl, 87'si (%27,4) 1-5 yıl, 74'ü (%23,3) 5-10 yıl ve 111'i (%35,0) 10 yıldan fazla süredir kurumda çalışmaktadır. Aylık gelir düzeyi sorusuna; 48'inin (%15,1) 1603 TL ve altı, 131'inin (%41,3) 1.604-2.000 TL arasında, 42'sinin (%13,2) 2.001-3.000TL arasında, 96'sının (%30,3) 3.001 TL ve üzeri kazancının olduğu görülmektedir. Katılımcıların HBYS deneyimleri sorulduğunda, 66'sının (%20,8) 0-1 yıl arasında, 81'inin (%25,6) 1-5 yıl arasında, 71'inin (%22,4) 5-10 yıl arasında, 99'unun (%31,2) ise 10 yıldan fazla kullandığı ortaya çıkmaktadır. 183 (%57,7) katılımcının eğitim alıp, 134 (%42,3) katılımcının eğitim almaması; bunların da 174'ü (%54,9) 0-1 hafta, 60'ı (%18,9) 1 hafta ile 1 ay arası, 33'ünün (%10,4) 1-3 ay arası ve 30'unun (%9,5) 3 aydan fazla süreyle eğitim aldıkları ortaya çıkmıştır. 119 (%37,5) katılımcının 20-29, 135 (%42,6) katılımcının ise 30-39, 63 (%19,9) katılımcının 40 ve üzeri yaş aralığında olduğu görülmektedir. Verilen HBYS eğitiminin değerlendirilmesi istendiğinde katılımcıların; 75'i (%23,7) yetersiz, 105'i (%33,1) kararsız ve 117'si (%36,9) yeterli bulmuştur. Çalışanların kendi bilgisayar becerilerini değerlendirmeleri istendiğinde; 33'ü (%10,4) yetersiz, 75'inin (%23,7) kararsız ve 209'unun (%65,9) yeterli olarak gördüğü tespit edilmiştir.

4.2. Elde Edilen Verilerin Analizi ve Bulguların Değerlendirilmesi

Araştırmaya katılan bireylerin Bilgi Güvenliği Anketinde yer alan ifadelere vermiş oldukları cevapların aritmetik ortalaması ve standart sapması Tablo 4.2'de gösterilmektedir.

Tablo 4.2. Katılımcıların Bilgi Güvenliği Sorularına Verdikleri Cevaplara İlişkin Puanların Dağılımı

No	İfadeler	$\overline{X}$	SS
1	Hastane bilgi güvenliğinin sağlanması için görevler ve sorumluluklar net olarak belirlenmiştir (örneğin; yedeklerin alınmasından, kullanıcıların sisteme kaydedilmesinden sorumlu olan çalışanlar bulunmaktadır).	3,46	1,11
2	Hastanede, bilgi güvenliğine ilişkin yazılı politikalar vardır.	3,51	1,11
3	Çalışanlar bilgi güvenliği politikalardan haberdardır.	3,15	1,16
4	Tüm personele yeterli ve uygun bilgi güvenliği eğitimi verilmektedir.	3,06	1,20

Güvenlik Politikaları		3,24	1,00
5	Çalışanlar bilgi sisteminde izin verilen ve onaylanmayan uygulamalar konusunda yeterince bilgilidir (örneğin; elektronik posta kullanımı ve internete bağlanma).	3,27	1,24
6	Bilgi güvenliğinin sağlanması için çalışanlar gerekli özeni gösterir.	3,57	1,07
7	Hastanedeki yöneticiler bilgi güvenliğine gereken özeni gösterir.	3,64	1,05
8	Yöneticiler bilgi güvenliliğinin uygulaması konusunda sorumluluk sahibidirler.	3,53	1,05
9	Hastane içinde bilgi güvenliği konusunda bir uzman bulunmaktadır.	3,16	1,27
Örgütsel Güvenlik		3,43	0,83
10	Bilgi güvenliği uzmanı bulunmadığında dışarıdan danışmanlık hizmeti alınmaktadır.	2,77	1,25
11	Çalışanlar, güvenlik ihlali olaylarının derhal yönetime bildirilmesi gerektiğinden haberdardır.	3,47	1,15
12	Çalışanlar kendi çalışma alanlarından uzaklaştığında, bilgisayarlarını daima güvenli şekilde bırakmaları konusunda eğitilmiştir (örneğin; bilgisayar başından ayrıldığında bilgisayarların şifrelenmesi ya da oturumun kapatılması).	3,47	1,20
13	Güvenlik politikalarımızı ve süreçlerimizi ihlal eden çalışanlarımıza yönelik disiplin uygulamaları vardır.	3,23	1,08
14	Sistem arızası, çökmesi ya da hırsızlık gibi durumlarda, veri yedeklerimiz işimizde kesintiye yol açmayacak şekilde bilgilerimizi geri kazanmamızı sağlar.	3,62	1,05
Güvenlik Uygulamaları		3,00	0,92
15	Sistemlerimiz herhangi bir sorun oluşması beklenmeden, önceden oluşturulmuş bir plan doğrultusunda güncellenmektedir.	3,45	1,05
16	Bir güvenlik ihlalinin meydana gelmesi durumunda, yapılacaklar ve yardım için kimin aranacağı bilinmektedir.	3,42	1,17
17	Anti-virüs sistemimiz günceldir ve bir virüs saldırısı durumunda, sistemlerimizi mümkün olan en iyi şekilde korumaktadır.	3,33	1,20
18	Halka açık ağlara bağlı olmasına rağmen, sistemlerimiz İnternet Hizmeti Sağlayıcısının güvenliği ve/veya kendi güvenlik sistemlerimiz tarafından yeterince korunmaktadır.	3,52	1,01
19	Kullanıcıların sistemlerimizde oturum açmalarına yetki verecek uygun mekanizmalar bulunmaktadır.	3,62	0,95
20	Çalışanlar, kendi kullanıcı hesaplarıyla yetkilendirilip tanımlamaları yapılmadan, sistemlerimizde oturum açamaz / sistemlerimize erişim sağlayamazlar.	3,90	1,03
21	Şifre değiştirme sıklığını belirleyen ve şifre karmaşıklığını engelleyen bir şifre yönetim sistemi bulunmaktadır (örneğin, şifre iki haftada bir değiştirilmelidir ve en az .... sayısı kadar karakter uzunluğunda olmalıdır).	3,64	1,09
22	Hastanede, kullanıcıların hangi verilere erişebileceğini belirleyen bir yetkilendirme prosedürü vardır.	3,74	1,05
23	Bilgi işlem uygulamaları sadece yetkilendirilmiş iş amaçları doğrultusunda kullanılır.	3,79	1,06
Erişim ve Yetkilendirme		3,64	0,79
24	Hastanedeki iş yükünün fazla olması, bilgi güvenliğine gereken önemin verilmesini engellemez.	3,59	1,22
25	Bilgi güvenliği süreçleri, hizmet kalitesini olumsuz yönde etkilemez.	3,72	1,09
26	Bilgi güvenliği gün içinde yaptığımız işleri düşününce öncelikli bir konudur.	3,64	1,16
27	Bilgisayar kullanımı ile iş akışında olan değişimler bilgi güvenliğine gereken önemi vermeyi engellemez.	3,67	1,14

Hizmet Sunumu	3,65	0,95

Anketlerde 5'li Likert ölçeğine göre yapılandırılmış ifadelere verilen cevapların değerlendirilmesi yapılırken aralıkların eşit olduğu varsayımında bulunulmaktadır. Bu varsayımdan hareketle aritmetik ortalamalar için puan aralığı "0,80" hesaplanmıştır. Anketteki ifadeler yorumlanırken 1.00-1.79 "Hiç Katılmıyorum", 1.80-2.59 "Katılmıyorum", 2.60-3.39 "Orta Derecede Katılıyorum", 3.40-4.19 "Katılıyorum", 4.20-5.00 "Kesinlikle Katılıyorum" şeklindeki kategori kullanılmıştır (Kaplanoğlu 2014).

Tablo 4.2'ye bakıldığında ankette yer alan her bir ifadenin aritmetik ortalamasına ve standart sapma dağılımlarına yer verilmiştir. Katılımcıların hastanedeki yöneticilerin bilgi güvenliğine gereken özeni gösterdiğine (3,64±1,05), istenmeyen durumlarda veri yedekleri işin aksamadan yürütülmesi (3,62±1,05), kullanıcıların sistemde oturum açmalarına yetkilendiren uygun mekanizmalar olması (3,62±0,95), çalışanlara yetki verilmeden önce sistemde oturumu açamaması (3,90±1,03), şifre yönetim sisteminin bulunması (3,64±1,09), hastanede yetkilendirme prosedürünün olması (3,74±1,05), bilgi işlem uygulamaları sadece iş amaçları doğrultusunda kullanılması (3,79±1,06), hizmet kalitesinin olumsuz yönde etkilenmemesi (3,72±1,09), bilgi güvenliğinin öncelikli bir konu olması (3,64±1,16), değişimlere rağmen bilgi güvenliğine gereken önemin verilmesi (3,67±1,14) konularına katılımı fazladır.

Anket ifadelerine katılım düzeylerinden katılımcıların bilgi güvenliği politikalardan haberdar olduğu (3,15±1,16), çalışanlara bilgi güvenliği eğitimin verildiği (3,06±1,20), çalışanların sistemde izin verilen ve verilmeyen uygulamalar konusundaki hakimiyetleri (3,27±1,24), hastane bilgi güvenliği konusunda bir uzmanın olduğu (3,16±1,27), uzman bulunmadığında dışarıdan danışmanlık hizmetinin alındığı (2,77±1,25), güvenliği ihlal eden çalışanlara karşı disiplin uygulamaları olduğu (3,23±1,08), sistemin mümkün olan en iyi şekilde korunduğu (3,33±1,20) ifadelerine katılım değerlendirildiğinde orta derecede memnuniyet duydukları tespit edilmiştir.

Anketin ifadeleri arasında "Çalışanlar, kendi kullanıcı hesaplarıyla yetkilendirilip tanımlamaları yapılmadan, sistemlerimizde oturum açamaz/ sistemlerimize erişim sağlayamazlar" (3,90±1,03) ifadesi katılım düzeyi en yüksek

ifadeyken, “Bilgi güvenliği uzmanı bulunmadığında dışarıdan danışmanlık hizmeti alınmaktadır” (2,77±1,25) ifadesi katılımcılar tarafından katılım düzeyi en düşük olan ifade olarak görülmektedir.

4.3. Boyutların Demografik Değişkenlere Göre Karşılaştırılması

Bilgi güvenliğini ölçen erişim ve yetkilendirme, güvenlik uygulamaları, hizmet sunumu, örgütsel güvenlik ve güvenlik politikaları boyutları pozisyon, eğitim durumu, yaş, cinsiyet, medeni durum, gelir, çalışma durumu, HBYS deneyim ve bilgisayar becerisinden oluşan demografik bilgiler ile karşılaştırılmıştır.

4.3.1. Erişim ve Yetkilendirme Boyutunun Demografik Değişkenlere Göre Karşılaştırması

Erişim ve Yetkilendirme boyutunun aldığı puanların demografik değişkenlere göre dağılımı Tablo 4.3.1’de verilmiştir.

Tablo 4.3.1. Erişim ve Yetkilendirme Boyutunun Demografik Değişkenlere Göre Karşılaştırması

Değişkenler	N	$\overline{X}$	SS	Test Değerleri
Pozisyon				
Tıbbi	210	3,59	0,82	t= -1,59 p= 0,11
İdari	107	3,73	0,71	
Eğitim				
Lise	104	3,75	0,77	F= 3,46 **p= 0,01**
Yükseko0kul	84	3,65	0,77	
Lisans	98	3,63	0,81	
Yüksek Lisans ve Üzeri	30	3,23	0,71	
Yaş				
20-29	119	3,51	0,87	F=2,70 p= 0,06
30-39	135	3,74	0,63	
40-59	63	3,64	0,89	
Cinsiyet				
Kadın	126	3,70	0,75	t=1,19 p=0,23
Erkek	191	3,59	0,80	
Medeni Hal				
Evli	203	3,65	0,77	t=0,52 p=0,59
Evli Değil	114	3,60	0,81	
Aylık Gelir				
1603 TL ve altı	48	3,37	0,80	F=2,85 **p=0,03**
1603-2000 TL	131	3,66	0,75	
2001-3000 TL	42	3,84	0,91	
3001 TL ve Üstü	96	3,64	0,75	

Kurumda Çalışma Süresi				
0-1 yıl	45	3,76	0,69	F= 2,08 p= 0,10
1-5 yıl	87	3,59	0,90	
5-10 yıl	74	3,47	0,78	
10 yıl ve üzeri	111	3,73	0,71	
HBYS Deneyim				
0-1 yıl	66	3,40	0,75	F= 3,76 **p= 0,01**
1-5 yıl	81	3,75	0,91	
5-10 yıl	71	3,55	0,74	
10 yıl ve üzeri	99	3,76	0,69	
HBYS Eğitimi Alınması				
Evet	183	3,69	0,80	t= 1,54 p= 0,12
Hayır	134	3,56	0,76	
HBYS Eğitim Süresi				
0-1 Hafta	174	3,63	0,82	F= 0,37 p= 0,77
1 Hafta- 1 Ay	60	3,64	0,83	
1- 3 Ay	33	3,65	0,64	
3 Ay ve Üzeri	30	3,80	0,80	
HBYS Eğitim Yeterliliği				
Yetersiz	75	3,34	0,93	F= 7,99 **p= 0,00**
Kararsız	105	3,76	0,70	
Yeterli	117	3,75	0,74	
Bilgisayar Kullanım Becerisi				
Yetersiz	33	3,48	1,10	F= 0,77 p= 0,46
Kararsız	75	3,63	0,60	
Yeterli	209	3,66	0,79	

Tablo 4.3.1'de görüldüğü üzere Erişim ve Yetkilendirme boyutunun katılımcıların pozisyonuna (t= -1,59; p=0,11), yaşına (F=2,70; p=0,06), cinsiyetine (t=1,19; p=0,23), medeni haline (t=0,52; p=0,59), kurumda çalışma süresine (F=2,08; p=0,10), HBYS eğitimi alıp almadığına (t=1,54; p=0,12), HBYS eğitim süresine (F=0,37; p=0,77) ve bilgisayar kullanım becerisine (F=0,77; p=0,46) göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark bulunmamıştır (p >0,05).

Erişim ve yetkilendirme boyutunun puanları katılımcıların eğitim durumlarına göre karşılaştırıldığında, bireylerin eğitim seviyesi arttıkça erişime yönelik puanlar da azalış göstermiş ve gruplar arasında istatistiksel olarak anlamlı bir farklılık olduğu tespit edilmiştir (p=0,01; p<0,05). Yapılan Tukey testi sonucunda farkın lise mezunu bireylerin (3,75±0,77) erişim boyutundan aldıkları puanların, yüksek lisans ve üzeri bireylere (3,23±0,71) göre daha yüksek olmasından kaynaklandığı anlaşılmıştır. Lise mezunlarının HBYS' de erişimin yeterli olduğuna dair algısı daha yüksek bulunmuştur.

Bunun yanı sıra erişim ve yetkilendirme boyutu puanlarının katılımcıların aylık gelirine göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu bulunmuştur (p=0,03; p<0,05). Yapılan Tukey testi sonucunda 2000 ile 3000 TL arası geliri olan bireylerin (3,84±0,91) 1603 TL ve altı geliri olan bireylere göre (3,37±0,80) puanlarının yüksek olduğu görülmüştür. Bu nedenle 2000 ile 3000 TL arasında aylık geliri olan bireylerde erişime ilişkin algı düzeylerinin daha yüksek olduğu söylenebilir.

Erişim ve yetkilendirme boyutu puanları katılımcıların HBYS deneyim durumuna göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu ortaya çıkmıştır (p=0,01; p<0,05). Yapılan Tukey testi sonucunda HBYS deneyimi 0-1 yıl arasında olan bireylerin (3,40±0,75), diğer gruplara göre erişime dair algı düzeylerinin daha düşük olmasından kaynaklandığı tespit edilmiştir.

Son olarak erişim ve yetkilendirme boyutunun puanları HBYS eğitiminin yeterliliği durumuna göre karşılaştırıldığında, istatistiksel olarak anlamlı bir fark olduğu tespit edilmiştir (p=0,00; p<0,05). Yapılan Tukey testi sonucunda HBYS eğitimini yetersiz bulan bireylerin (3,34±0,93), diğer gruplara göre algı düzeylerinin daha düşük olmasından kaynaklandığı tespit edilmiştir.

4.3.2. Güvenlik Uygulamaları Boyutunun Demografik Değişkenlere Göre Karşılaştırması

Güvenlik Uygulamaları boyutunun aldığı puanların demografik değişkenlere göre dağılımı Tablo 4.3.2'de verilmiştir.

Tablo 4.3.2. Güvenlik Uygulamaları Boyutunun Demografik Değişkenlere Göre Karşılaştırması

Değişkenler	N	$\overline{X}$	SS	Test Değerleri
Pozisyon				
Tıbbi	210	3,03	0,97	t= 0,79 p= 0,42
İdari	107	2,94	0,81	
Eğitim				
Lise	104	3,17	0,97	F= 2,88 **p= 0,03**
Yüksekokul	84	2,94	0,63	
Lisans	98	3,00	1,06	
Yüksek Lisans ve Üzeri	30	2,65	0,72	
Yaş				
20-29	119	3,10	1,00	F=1,09

30-39	135	2,94	0,73	p= 0,33
40-59	63	2,95	1,10	
Cinsiyet				
Kadın	126	2,78	0,93	t= -3,51
Erkek	191	3,15	0,89	**p= 0,00**
Medeni Hal				
Evli	203	2,94	0,94	t= -1,62
Evli Değil	114	3,11	0,88	p=0,10
Aylık Gelir				
1603 TL ve altı	48	3,03	0,90	F= 0,24
1603-2000 TL	131	3,04	0,91	p= 0,86
2001-3000 TL	42	2,96	1,27	
3001 TL ve Üstü	96	2,95	0,75	
Kurumda Çalışma Süresi				
0-1 yıl	45	3,50	0,58	F= 7,39
1-5 yıl	87	3,01	0,99	**p= 0,00**
5-10 yıl	74	2,70	0,96	
10 yıl ve üzeri	111	3,00	0,87	
HBYS Deneyim				
0-1 yıl	66	2,77	0,86	F= 2,69
1-5 yıl	81	3,20	1,00	**p= 0,04**
5-10 yıl	71	3,00	0,93	
10 yıl ve üzeri	99	3,00	0,84	
HBYS Eğitimi Alınması				
Evet	183	3,09	0,96	t= 2,08
Hayır	134	2,88	0,84	**p= 0,03**
HBYS Eğitim Süresi				
0-1 Hafta	174	2,97	0,96	F= 0,96
1 Hafta- 1 Ay	60	3,10	0,85	p= 0,40
1- 3 Ay	33	3,18	0,69	
3 Ay ve Üzeri	30	2,85	0,99	
HBYS Eğitim Yeterliliği				
Yetersiz	75	2,68	1,03	F= 6,76
Kararsız	105	3,14	0,83	**p= 0,00**
Yeterli	117	3,10	0,86	
Bilgisayar Kullanım Becerisi				
Yetersiz	33	2,50	1,12	F= 7,25
Kararsız	75	3,22	0,90	**p= 0,00**
Yeterli	209	3,00	0,86	

Tablo 4.3.2'de görüldüğü üzere güvenlik uygulamaları boyutunun katılımcıların pozisyonuna (t=0,79; p=0,42), yaşına (F=1,09; p=0,33), medeni haline (t=-1,62; p=0,10), aylık gelirine (F=0,24; p=0,86) ve HBYS eğitim süresine (F=0,96; p=0,40) göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark bulunmamıştır (p >0,05).

Güvenlik uygulamaları boyutunun puanları katılımcıların eğitimine göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu tespit edilmiştir ($p=0,03$; $p<0,05$). Yapılan Tukey testi sonucunda farkın, lise mezunu bireylerin güvenlik uygulamaları boyutundan memnuniyet düzeylerinin yüksek lisans ve üzeri mezun bireylere göre daha yüksek olmasından kaynaklandığı anlaşılmıştır. Eğitim düzeyi lise (3,17±0,97) olan bireylerin, güvenlik uygulamalarından daha memnun olduğu söylenebilir.

Güvenlik uygulamaları boyutunun puanları katılımcıların cinsiyetine göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu bulunmuştur ($p=0,00$; $p<0,05$). Kadın bireylerin, erkek bireylere göre puanlarının yüksek olduğu görülmüştür.

Güvenlik uygulamaları boyutunun puanları katılımcıların kurumda çalışma süresi durumuna göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu ortaya çıkmıştır ($p=0,00$; $p<0,05$). Yapılan Tukey testi sonucunda farkın, 0-1 yıl arasında çalışan bireylerin diğer gruplardaki bireylere göre (3,50±0,58) daha çok memnun olmasından kaynaklandığı tespit edilmiştir. Katılımcıların en az memnuniyet düzeyine sahip grubun kurumda 5-10 yıl arası çalışan bireylerden (2,70±0,96) oluştuğu sonucuna ulaşılmıştır.

Güvenlik uygulamaları boyutunun puanları katılımcıların HBYS deneyim durumuna göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu ortaya çıkmıştır ($p=0,04$; $p<0,05$). Yapılan Tukey testi sonucunda kurumda HBYS deneyimi 5-10 yıl arasında olan (3,00±0,93) ve 10 yıldan fazla bireylerde (3,00±0,84) güvenlik uygulamalarından memnuniyeti yüksek iken 1-5 yıl arasında olan bireylerin (3,20±1,00) daha yüksek düzeyde olduğu görülmektedir.

Güvenlik uygulamaları boyutunun puanları katılımcıların HBYS eğitimi alıp almadığı durumuna göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu ortaya çıkmıştır ($p=0,03$; $p<0,05$). Farkın, HBYS eğitimi almamış bireylerin (2,88±0,84) HBYS eğitimi alan grubundaki bireylere göre (3,09±0,96) daha az memnun olmasından kaynaklandığı tespit edilmiştir.

Güvenlik uygulamaları boyutu puanları katılımcıların HBYS eğitim yeterliliği durumuna göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu ortaya çıkmıştır ($p=0,00$; $p<0,05$). Yapılan Tukey testi sonucunda farklılığın, eğitimi

yetersiz (2,68±1,03) bulan bireylerde, diğer gruplara göre algı düzeylerinin daha düşük olmasından kaynaklandığı tespit edilmiştir.

Son olarak güvenlik uygulamaları boyutunun puanları katılımcıların bilgisayar kullanım becerisine göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu tespit edilmiştir (p=0,00; p<0,05). Yapılan Tukey testi sonucunda farkın bilgisayar kullanım becerisini yetersiz görenlerin (2,50±1,12) memnuniyet düzeyinin düşük olduğu, bunu kendisini yeterli görenlerin takip ettiği (3,00±0,86) ve kararsızların ise (3,22±0,90) memnuniyetlerinin en yüksek grup olduğu anlaşılmıştır.

4.3.3. Hizmet Sunumu Boyutunun Demografik Değişkenlere Göre Karşılaştırması

Hizmet Sunumu Boyutunun aldığı puanların demografik değişkenlere göre dağılımı Tablo 4.3.3'te verilmiştir.

Tablo 4.3.3. Hizmet Sunumu Boyutunun Demografik Değişkenlere Göre Karşılaştırması

Değişkenler	N	$\overline{X}$	SS	Test Değerleri
Pozisyon				
Tıbbi	210	3,67	0,93	t= 0,50 p= 0,61
İdari	107	3,62	0,99	
Eğitim				
Lise	104	3,76	0,88	F=3,25 **p= 0,02**
Yüksekokul	84	3,73	0,94	
Lisans	98	3,63	1,01	
Yüksek Lisans ve Üzeri	30	3,17	0,91	
Yaş				
20-29	119	3,61	0,94	F=0,20 p= 0,81
30-39	135	3,68	0,83	
40-59	63	3,67	1,19	
Cinsiyet				
Kadın	126	3,65	0,95	t= -0,06 p=0,94
Erkek	191	3,66	0,95	
Medeni Hal				
Evli	203	3,68	0,99	t=0,75 p=0,43
Evli Değil	114	3,60	0,88	
Aylık Gelir				
1603 TL ve altı	48	3,37	0,94	F=3,29 **p= 0,02**
1603-2000 TL	131	3,59	0,91	
2001-3000 TL	42	3,67	1,02	
3001 tl ve Üstü	96	3,87	0,95	
Kurumda Çalışma Süresi				

0-1 yıl	45	3,86	0,85	F= 4,35 **p= 0,00**
1-5 yıl	87	3,60	1,00	
5-10 yıl	74	3,36	1,04	
10 yıl ve üzeri	111	3,81	0,84	
HBYS Deneyim				
0-1 yıl	66	3,46	0,87	F= 1,76 p=0,15
1-5 yıl	81	3,62	1,11	
5-10 yıl	71	3,66	0,82	
10 yıl ve üzeri	99	3,81	0,82	
HBYS Eğitimi Alınması				
Evet	183	3,61	0,93	t= -1,06 p= 0,29
Hayır	134	3,72	0,98	
HBYS Eğitim Süresi				
0-1 Hafta	174	3,63	0,95	F= 1,35 p= 0,25
1 Hafta- 1 Ay	60	3,75	0,89	
1- 3 Ay	33	3,40	0,75	
3 Ay ve Üzeri	30	3,82	0,95	
HBYS Eğitim Yeterliliği				
Yetersiz	75	3,29	1,03	F= 10,90 **p= 0,00**
Kararsız	105	3,92	0,70	
Yeterli	117	3,64	0,85	
Bilgisayar Kullanım Becerisi				
Yetersiz	33	3,56	0,98	F= 1,11 p= 0,33
Kararsız	75	3,80	0,81	
Yeterli	209	3,62	0,99	

Tablo 4.3.3'te görüldüğü üzere hizmet sunumu boyutunun katılımcıların pozisyonuna (t=0,50; p=0,61), yaşına (F=0,20; p=0,81), cinsiyetine (t=-0,06; p=0,94), medeni haline (t=0,75; p=0,43), HBYS deneyimine (F=1,76; p=0,15), HBYS eğitimi alıp almadığına (t=-1,06; p=0,29), HBYS eğitim süresine (F=1,35; p=0,25) ve bilgisayar kullanım becerisine (F=1,11; p=0,33) göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark bulunmamıştır (p >0,05).

Katılımcıların hizmet sunumu boyutunun eğitim düzeyi ile karşılaştırmasına bakılmıştır. Yapılan ANOVA testi sonucunda hizmet sunumu boyutu ile eğitim arasında istatiksel olarak anlamlı bir fark olduğu tespit edilmiştir (p=0,02; p<0,05). Yapılan Tukey testi sonucunda bu farkın, yüksek lisans ve üzeri mezun bireylerin (3,17±0,91) hizmet sunumundan aldıkları puanın, diğer gruplara göre daha düşük olmasından kaynaklandığı tespit edilmiştir. Nitelikli çalışanların hizmet sunumunu yetersiz bulduğu çıkarılabilir.

Hizmet sunumu boyutunun puanları katılımcıların aylık gelirlerine göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu ortaya çıkmıştır (p=0,02; p<0,05). Yapılan Tukey testi sonucunda farklılığın 1603 TL ve altı geliri olan bireylerin (3,37±0,94) memnuniyet düzeylerinin, 3001 TL ve üzeri aylık geliri olan bireylerinkinden (3,87±0,95) daha düşük olmasından kaynaklandığı tespit edilmiştir.

Hizmet sunumu boyutunun puanları katılımcıların kurumda çalışma süresine göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu ortaya çıkmıştır (p=0,00; p<0,05). Yapılan Tukey testi sonucunda farkın, 5-10 yıl arasında çalışan bireylerin 1-5 yıl arası (3,60±1,00) ve 10 yıldan fazla çalışan (3,81±0,84) grubundaki bireylere göre daha az memnun olmasından kaynaklandığı tespit edilmiştir. Katılımcıların memnuniyet düzeylerine ilişkin en çok memnun olan grubu 0-1 yıl arasında çalışan bireyler (3,86±0,85) oluştururken en az memnuniyet düzeyine sahip grubun 5-10 yıl arası çalışan bireylerden (3,36±1,04) oluştuğu sonucuna ulaşılmıştır.

Son olarak hizmet sunumu boyutunun puanları katılımcıların HBYS eğitiminin yeterli olmasına göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu tespit edilmiştir (p=0,00; p<0,05). Yapılan Tukey testi sonucunda farkın, HBYS eğitimini yetersiz görenlerin (3,29±1,03) fiziki şartlardan memnuniyetinin en düşük olduğu, diğer grupların ise görece olarak memnuniyetlerinin yüksek olduğu anlaşılmıştır.

4.3.4. Örgütsel Güvenlik Boyutunun Demografik Değişkenlere Göre Karşılaştırması

Örgütsel Güvenlik Boyutunun aldığı puanların demografik değişkenlere göre dağılımı Tablo 4.3.4'te verilmiştir.

Tablo 4.3.4. Örgütsel Güvenlik Boyutunun Demografik Değişkenlere Göre Karşılaştırması

Değişkenler	N	$\overline{X}$	SS	Test Değerleri
Pozisyon				
Tıbbi	210	3,51	0,82	t= 2,26 **p=0,02**
İdari	107	3,28	0,91	
Eğitim				
Lise	104	3,67	0,77	F=12,41 **p= 0,00**
Yüksekokul	84	3,49	0,63	

Lisans	98	3,37	0,96	
Yüksek Lisans ve Üzeri	30	2,66	0,85	
Yaş				
20-29	119	3,37	0,94	F=1,55 p= 0,21
30-39	135	3,53	0,76	
40-59	63	3,35	0,86	
Cinsiyet				
Kadın	126	3,44	0,85	t=0,05 p=0,95
Erkek	191	3,43	0,86	
Medeni Hal				
Evli	203	3,42	0,87	t= -0,52 p= 0,59
Evli Değil	114	3,47	0,82	
Aylık Gelir				
1603 TL ve altı	48	3,42	0,72	F= 3,57 **p= 0,01**
1603-2000 TL	131	3,61	0,84	
2001-3000 TL	42	3,31	1,08	
3001 TL ve Üstü	96	3,26	0,08	
Kurumda Çalışma Süresi				
0-1 yıl	45	3,60	0,77	F= 4,62 **p=0,00**
1-5 yıl	87	3,53	0,98	
5-10 yıl	74	3,12	0,91	
10 yıl ve üzeri	111	3,50	0,69	
HBYS Deneyim				
0-1 yıl	66	3,24	0,76	F= 2,95 **p= 0,03**
1-5 yıl	81	3,64	1,02	
5-10 yıl	71	3,35	0,85	
10 yıl ve üzeri	99	3,46	0,73	
HBYS Eğitimi Alınması				
Evet	183	3,54	0,77	t= 2,47 **p= 0,01**
Hayır	134	3,30	0,94	
HBYS Eğitim Süresi				
0-1 Hafta	174	3,38	0,89	F= 1,50 p= 0,21
1 Hafta- 1 Ay	60	3,42	0,79	
1- 3 Ay	33	3,58	0,71	
3 Ay ve Üzeri	30	3,70	0,75	
HBYS Eğitim Yeterliliği				
Yetersiz	75	2,86	0,89	F= 30,71 **p= 0,00**
Kararsız	105	3,53	0,76	
Yeterli	117	3,74	0,69	
Bilgisayar Kullanım Becerisi				
Yetersiz	33	3,05	0,83	F= 4,61 **p= 0,01**
Kararsız	75	3,59	0,77	
Yeterli	209	3,44	0,87	

Tablo 4.3.4'te görüldüğü üzere örgütsel güvenlik boyutunun katılımcıların yaşına (F=1,55; p=0,21), cinsiyetine (t=0,05; p=0,95), medeni haline (t=-0,52;

p=0,59) ve HBYS eğitim süresine (F=1,50; p=0,21) göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark bulunmamıştır (p >0,05).

Örgütsel güvenlik boyutunun puanları katılımcıların pozisyonuna göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu ortaya çıkmıştır (p=0,02; p<0,05). Tıbbi birimde çalışan bireylerin (3,51±0,82), örgütsel güvenlikteki memnuniyet düzeyi, idari birimde çalışanlardan (3,28±0,91) daha yüksek düzeyde olduğu görülmektedir.

Örgütsel güvenlik boyutunun puanları katılımcıların eğitimine göre karşılaştırıldığında, bireylerin eğitim düzeyleri arttıkça örgütsel güvenlik puanları da azalış eğilimi göstermiş ve gruplar arasında istatistiksel olarak anlamlı bir farklılık olduğu tespit edilmiştir (p=0,00; p<0,05). Yapılan Tukey testi sonucunda farkın lise mezunu bireylerin (3,67±0,77) örgütsel güvenlik boyutundan aldıkları puanların, yüksek lisans ve üzeri mezunu bireylere (2,66±0,85) göre daha yüksek olmasından kaynaklandığı anlaşılmıştır.

Örgütsel güvenlik boyutunun puanları katılımcıların aylık gelirine göre karşılaştırıldığında gruplar arasında istatistiksel olarak anlamlı bir farklılık olduğu tespit edilmiştir (p=0,01; p<0,05). Yapılan Tukey testi sonucunda farkın 1603-2000 TL aylık geliri olan bireylerin (3,61±0,84) örgütsel güvenlik boyutundan aldıkları puanların, 3001 TL ve üzeri aylık geliri olan bireylere (3,26±0,08) göre daha yüksek olmasından kaynaklandığı anlaşılmıştır.

Örgütsel güvenlik boyutunun puanları katılımcıların kurumda çalışma süresine göre karşılaştırıldığında, gruplar arasında istatistiksel olarak anlamlı bir farklılık olduğu tespit edilmiştir (p=0,00; p<0,05). Yapılan Tukey testi sonucunda 5-10 yılları arasında çalışan bireylerin (3,12±0,91) örgütsel güvenlik boyutundan aldıkları puanların, diğer gruplara göre daha düşük olmasından kaynaklandığı anlaşılmıştır.

Örgütsel güvenlik boyutunun puanları katılımcıların HBYS deneyimlerine göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu tespit edilmiştir (p=0,03; p<0,05). Yapılan Tukey testi sonucunda farkın, 1-5 yıl arasında deneyimi olan bireylerin (3,64±1,02) örgütsel güvenlik boyutundan memnuniyet düzeylerinin

0-1 yıl arasında deneyimi olan bireylere göre (3,24±0,76) daha yüksek olmasından kaynaklandığı anlaşılmıştır.

Örgütsel güvenlik boyutunun puanları katılımcıların HBYS eğitimi almasına göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu ortaya çıkmıştır (p=0,01; p<0,05). HBYS eğitimi alan bireylerin (3,54±0,77), örgütsel güvenlikteki memnuniyet düzeyi, HBYS eğitimi almayan bireylerden (3,30±0,94) daha yüksek düzeyde olduğu görülmektedir.

Örgütsel güvenlik boyutunun puanları katılımcıların HBYS eğitiminin yeterliliğine göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu ortaya çıkmıştır (p=0,00; p<0,05). Yapılan Tukey testi sonucunda farkın, HYBS eğitimini yetersiz bulan bireylerin (2,86±0,89) diğer gruplara göre daha az memnun olmasından kaynaklandığı tespit edilmiştir.

Son olarak örgütsel güvenlik boyutunun puanları katılımcıların bilgisayar kullanım becerisine göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu tespit edilmiştir (p=0,01; p<0,05). Yapılan Tukey testi sonucunda farkın, bilgisayar kullanım becerisini yetersiz görenlerin (3,05±0,83) fiziki şartlardan memnuniyetinin en düşük olduğu, bunu kararsız ve yeterli olarak değerlendirenlerin görece olarak memnuniyetlerinin yüksek grup olduğu anlaşılmıştır.

4.3.5. Güvenlik Politikaları Boyutunun Demografik Değişkenlere Göre Karşılaştırması

Güvenlik Politikaları Boyutunun aldığı puanların demografik değişkenlere göre dağılımı Tablo 4.3.5'te verilmiştir.

Tablo 4.3.5. Güvenlik Politikaları Boyutunun Demografik Değişkenlere Göre Karşılaştırması

Değişkenler	N	$\overline{X}$	SS	Test Değerleri
Pozisyon				
Tıbbi	210	3,25	0,98	t= 0,27 p=0,78
İdari	107	3,22	1,03	
Eğitim				
Lise	104	3,49	0,99	F= 8,63 **p= 0,00**
Yüksekokul	84	3,32	0,92	
Lisans	98	3,15	1,01	
Yüksek Lisans ve Üzeri	30	2,50	0,83	

Yaş				
20-29	119	3,10	0,95	F=1,95 p= 0,14
30-39	135	3,35	0,94	
40-59	63	3,26	1,16	
Cinsiyet				
Kadın	126	3,27	0,99	t=0,45 p=0,64
Erkek	191	3,22	1,00	
Medeni Hal				
Evli	203	3,23	1,03	t= -0,34 p=0,73
Evli Değil	114	3,27	0,93	
Aylık Gelir				
1603 TL ve altı	48	2,95	0,85	F= 4,99 **p= 0,00**
1603-2000 TL	131	3,44	0,92	
2001-3000 TL	42	3,42	1,21	
3001 TL ve Üstü	96	3,04	1,00	
Kurumda Çalışma Süresi				
0-1 yıl	45	3,26	1,11	F= 1,03 p= 0,38
1-5 yıl	87	3,17	0,86	
5-10 yıl	74	3,13	1,12	
10 yıl ve üzeri	111	3,36	0,96	
HBYS Deneyim				
0-1 yıl	66	2,96	1,01	F= 2,86 **p= 0,03**
1-5 yıl	81	3,19	0,92	
5-10 yıl	71	3,32	1,12	
10 yıl ve üzeri	99	3,41	0,91	
HBYS Eğitimi Alınması				
Evet	183	3,43	0,97	t= 3,95 **p= 0,00**
Hayır	134	2,99	0,98	
HBYS Eğitim Süresi				
0-1 Hafta	174	3,19	1,06	F= 3,79 **p= 0,01**
1 Hafta- 1 Ay	60	3,11	0,87	
1- 3 Ay	33	3,57	0,52	
3 Ay ve Üzeri	30	3,70	1,04	
HBYS Eğitim Yeterliliği				
Yetersiz	75	2,60	0,99	F= 28,22 **p= 0,00**
Kararsız	105	3,40	0,85	
Yeterli	117	3,58	0,91	
Bilgisayar Kullanım Becerisi				
Yetersiz	33	2,90	1,24	F= 2,28 p= 0,10
Kararsız	75	3,22	0,88	
Yeterli	209	3,30	0,99	

Tablo 4.3.5'te görüldüğü üzere güvenlik politikaları boyutunun katılımcıların pozisyonuna (t=0,27, p=0,78), cinsiyetine (t=0,45, p=0,64), medeni haline (t=-0,34, p=0,73), kurumda çalışma süresine (F=1,03, p=0,38) ve bilgisayar kullanım becerisine (F=2,28, p=0,10) göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark bulunmamıştır (p >0,05).

Güvenlik politikaları boyutunun puanları katılımcıların eğitimine göre karşılaştırıldığında, bireylerin eğitim düzeyleri arttıkça örgütsel güvenlik puanları da azalış eğilimi göstermiş ve gruplar arasında istatistiksel olarak anlamlı bir farklılık olduğu tespit edilmiştir ($p=0,00$; $p<0,05$). Yapılan Tukey testi sonucunda farkın yüksek lisans ve üzeri mezunu bireylerin (2,50±0,83) güvenlik politikaları boyutundan aldıkları puanların, diğer gruplara göre daha düşük olmasından kaynaklandığı anlaşılmıştır.

Bunun yanı sıra güvenlik politikaları boyutu puanlarının katılımcıların aylık gelirine göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu bulunmuştur ($p=0,00$; $p<0,05$). Yapılan Tukey testi sonucunda 1603-2000 TL arası geliri olan bireylerin (3,44±0,92), 1603 TL ve altı geliri olan bireylere göre (2,95±0,85) puanlarının yüksek olduğu görülmüştür. Bu nedenle 1603-2000 TL arasında aylık geliri olan bireylerde güvenlik politikalarına ilişkin algı düzeylerinin daha yüksek olduğu söylenebilir.

Güvenlik politikaları boyutu puanları katılımcıların HBYS deneyim durumuna göre karşılaştırıldığında deneyim süreleri arttıkça katılım puanları da artmış ve istatistiksel olarak anlamlı bir fark olduğu ortaya çıkmıştır ($p=0,03$; $p<0,05$). Yapılan Tukey testi sonucunda HBYS deneyimi 10 yıl ve üzeri olan bireylerin (3,41±0,91), diğer gruplara göre güvenlik politikaları dair algı düzeylerinin en yüksek olmasından kaynaklandığı tespit edilmiştir.

Güvenlik politikaları boyutunun puanları katılımcıların HBYS eğitimi alıp almadığı durumuna göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu ortaya çıkmıştır ($p=0,00$; $p<0,05$). Farkın, HBYS eğitimi almamış bireylerin (2,99±0,98) HBYS eğitimi alan grubundaki bireylere göre (3,43±0,97) daha az memnun olmasından kaynaklandığı tespit edilmiştir.

Güvenlik politikaları boyutu puanları katılımcıların HBYS eğitim süresinin durumuna göre karşılaştırıldığında istatistiksel olarak anlamlı bir fark olduğu ortaya çıkmıştır ($p=0,01$; $p<0,05$). Yapılan Tukey testi sonucunda farklılığın, eğitim süresi 3 ayı geçen bireylerin (3,70±1,04), 3 ayın altında eğitim gören bireylere göre algı düzeylerinin daha yüksek olduğu görülmüştür. HBYS eğitim süresini 3 aydan fazla olan çalışanların, güvenlik politikaları düzeyinden daha memnun olduğu söylenebilir.

Son olarak güvenlik politikaları boyutunun puanları HBYS eğitiminin yeterliliği durumuna göre karşılaştırıldığında, istatistiksel olarak anlamlı bir fark olduğu tespit edilmiştir ($p=0,00$; $p<0,05$). Yapılan Tukey testi sonucunda HBYS eğitimini yetersiz bulan bireylerin (2,60±0,99), diğer gruplara göre algı düzeylerinin daha düşük olmasından kaynaklandığı tespit edilmiştir.

4.4. Ankete Katılan Bireylere Yönelik İfadeler

"HBYS kullanım becerinizi nasıl değerlendirirsiniz?" ve "Hastanedeki bilgi güvenliği için kaç puan verirsiniz?" sorularına verilen cevapları inceleyebilmek amacıyla frekans analizi yapılmıştır. Ankette katılımcılara sorulan çoktan seçmeli soruların cevaplarını değerlendirmek için frekans analiz yapılmış ve elde edilen bulgular Tablo 4.4.1'de sunulmuştur.

Tablo 4.4.1. Araştırmaya Katılan Tıbbi ve İdari Birim Çalışanlarının HBYS Kullanımları ve Hastane Bilgi Güvenliği Değerlendirmesi

	Gruplar	**Tıbbi birimler**		**İdari birimler**	
		n	**%**	**n**	**%**
HBYS Kullanım Becerisi (0-100)	0-20 Puan	3	1,4	3	2,8
	21-40 Puan	15	7,1	9	8,4
	41-60 Puan	39	18,6	18	16,8
	61-80 Puan	66	31,4	44	41,1
	81-100 Puan	87	41,4	33	30,8
Toplam		210	100	107	100
Hastane bilgi güvenliği puanı değerlendirme (0-100 puan)	0-20 Puan	24	11,4	3	2,8
	21-40 Puan	6	2,9	3	2,8
	41-60 Puan	42	20,0	17	15,9
	61-80 Puan	60	28,6	39	36,4
	81-100 Puan	78	37,1	45	42,1
Toplam		210	100	107	100

Tablo 4.4.1'de araştırmaya katılan tıbbi ve idari birim çalışanlarının HBYS kullanımları karşılaştırıldığında, HBYS kullanım becerisi puanı, tıbbi birimlerde idari birimlere göre kendisini yeterli görenlerin sayısının daha yüksek olduğu belirlenmiştir. Hastane bilgi güvenliği puanı değerlendirme puanlarına bakıldığında, her iki grupta da bilgi güvenliğin en yüksek puanla değerlendirilmiştir. İdari birimin, tıbbi birime göre alınan önlemleri daha yeterli gördüğü söylenebilir.

Araştırmaya dahil olan katılımcıların "Hastanedeki hangi tür bilgilere kolaylıkla erişebiliyorsunuz?", "Hastanede günlük çalışma düzeninizde hangi tür

bilgileri kullanıyorsunuz?" ve "Hastanedeki hangi tür bilgiler koruma altındadır?" sorularına vermiş oldukları cevapların analiz verileri Tablo 4.4.2'de gösterilmektedir.

Tablo 4.4.2. Araştırmaya Katılan Tıbbi ve İdari Birim Çalışanlarının HBYS Kullanımları

	Gruplar	**Tıbbi birimler**		**İdari birimler**	
		n	**%**	**n**	**%**
HBYS kullanımı sırasında ulaşılabilen bilgi türleri*	Hastaya Ait Bilgiler	207	49,0	92	31,8
	Çalışanlara Ait Bilgiler	24	5,7	36	12,5
	Hastaneye Ait Mali Bilgiler	6	1,5	3	1,0
	Yönetimsel Raporlar	9	2,1	27	9,3
	Süreçsel Raporlar	39	9,2	30	10,3
	Kurum Prosedürleri	39	9,2	30	10,3
	Sigorta Şirketi Bilgileri	9	2,1	15	5,1
	Sosyal Güvence Bilgileri	81	19,1	42	14,5
	Diğer	9	2,1	15	5,1
Toplam		423	100	290	100
HBYS'nde günlük işleyiş sırasında kullanılan bilgiler*	Hastaya Ait Bilgiler	198	44,0	74	25,6
	Çalışanlara Ait Bilgiler	45	10,0	39	13,5
	Hastaneye Ait Mali Bilgiler	6	1,3	30	10,3
	Yönetimsel Raporlar	12	2,7	27	9,3
	Süreçsel Raporlar	51	11,3	33	11,3
	Kurum Prosedürleri	51	11,3	30	10,3
	Sigorta Şirketi Bilgileri	10	2,2	12	4,1
	Sosyal Güvence Bilgileri	66	14,7	27	9,3
	Diğer	12	2,7	18	6,2
Toplam		451	100	290	100
HBYS'nde koruma altındaki bilgiler*	Hastaya Ait Bilgiler	171	20,0	81	17,7
	Çalışanlara Ait Bilgiler	141	16,6	68	14,9
	Hastaneye Ait Mali Bilgiler	141	16,6	62	13,6
	Yönetimsel Raporlar	126	14,8	62	13,6
	Süreçsel Raporlar	84	9,9	50	11,0
	Kurum Prosedürleri	60	7,0	38	8,2
	Sigorta Şirketi Bilgileri	57	6,7	41	9,0
	Sosyal Güvence Bilgileri	57	6,7	41	9,0
	Diğer	15	1,8	15	3,2
Toplam		852	100	458	100

***** Bu sorularda araştırma grubu tarafından birden fazla seçenek işaretlenmiştir.

Tablo 4.4.2'de araştırmaya katılan tıbbi ve idari birim çalışanlarının HBYS kullanımları incelendiğinde, HBYS kullanımı sırasında ulaşılabilen bilgi türleri açısından; hastaya ait bilgilerin %31,8 oranında ve sosyal güvence bilgilerinin %14,5 oranında idari birimlerce, hastaya ait bilgilerin %49,0 oranında ve sosyal güvence bilgilerinin %19,1 oranında tıbbi birimlerce ulaşılabilir olduğu görülmektedir.

HBYS'nde günlük işleyiş sırasında kullanılan bilgiler açısından; hastaya ait bilgilerin %44,0 oranında ve sosyal güvence bilgileri %14,7 oranında tıbbi birimlerce, hastaya ait bilgilerin %25,6 ve çalışanlara ait bilgilerin %13,5 oranında idari birimlerce ulaşılabilir olduğu görülmektedir. HBYS'nde koruma altında olduğu

düşünülen bilgiler değerlendirildiğinde, hastaya ait bilgilerin, çalışanlara ait bilgilerin, hastaneye ait mali bilgilerin, yönetimsel raporların ve süreçsel raporların her iki grupta da yüksek oranda değerlendirme yapıldığı görülmektedir.

Katılımcıların, "HBYS üzerinden hasta verilerine erişim kimler tarafından denetleniyor?" sorusuna verdikleri cevapları incelenmiş ve elde edilen sonuçlar Tablo 4.4.3'te gösterilmiştir.

Tablo 4.4.3. Araştırmaya Katılan Tıbbi ve İdari Birim Çalışanlarına Göre HBYS Kullanımında Erişim Denetimi

	Gruplar	Tıbbi Birimler		İdari Birimler	
		n	%	n	%
HBYS üzerinden hasta verilerine erişim kimler tarafından denetleniyor	Bilgi İşlem Birimi	69	32,9	51	47,7
	Hastane Müdürleri	30	14,2	-	0
	Hemşirelik Hizmetleri	30	14,2	-	0
	Üst Yönetim	3	1,4	3	2,9
	Merkez Yönetim	6	2,9	-	0
	Cevapsız	72	34,2	53	49,6
Toplam		210	100	107	100

Tablo 4.4.3'te araştırma her iki grup tarafından, HBYS kullanımı sırasında hasta verilerine erişim denetiminin tıbbi birimlerde %32,9 oranında ve idari birimlerde %47,7 oranında bilgi işlem departmanı tarafından denetlendiğinin düşünüldüğü görülürken, bu soruya 317 kişiden %39,4'ünün cevap vermediği görülmektedir.

Araştırmaya dahil olan katılımcıların "Bilgi güvenliğinin sağlanması için sisteme girişte kimlik belirleme yöntemi olarak hangilerini kullanıyorsunuz?", "Şifre yapılarından hangilerini kullanıyorsunuz?", "Hastaya ait olan bilgilerin paylaşımı için hastalardan onay formu alıyor musunuz?", "HBYS sisteminde hastaya ait bilgiler için işlemlerden hangilerini yapabiliyorsunuz?", "Hastaya ait hangi bilgilere erişebiliyorsunuz?" ve "HBYS kullanırken bilgi güvenliğini arttırmak için neler yapılmalıdır?" sorularına vermiş oldukları cevapların analiz verileri Tablo 4.4.4'te gösterilmektedir.

Tablo 4.4.4. Araştırmada Tıbbi ve İdari Birim Çalışanlarının Bilgi Güvenliği Uygulamaları

	Gruplar	Tıbbi birimler		İdari birimler	
		n	%	n	%
Bilgi güvenliğinin sağlanması için kullanılan kimlik belirleme yöntemleri*	Kullanıcı adı	165	44,3	72	42,3
	Şifre	165	44,3	83	48,9
	Akıllı kart	27	7,2	6	3,6
	Parmak izi	6	1,7	6	3,6

	Diğer	9	2,4	3	1,8
Toplam		372	100	170	100
Kullanılan şifre yapıları*	1234….	57	17,4	21	14,3
	8765….	57	17,4	15	10,2
	Kullanıcı adı ve şifrenin aynı olması	15	4,6	-	-
	Şifrede kişisel isim kullanımı	75	23,0	21	14,3
	Şifrede bölüm adı kullanımı	6	1,9	6	3,6
	Şifrede hastane adı kullanımı	12	3,7	-	-
	Sayı ve harfin bir arada kullanımı	63	19,2	51	35,0
	Diğer	42	12,9	32	22,0
Toplam		327	100	146	100
Hastaya ait bilgilerin paylaşımı için onam formu alınması	Onam formu alınıyor	117	55,8	48	44,9
	Onam formu alınmıyor	93	44,2	59	55,1
Toplam		210	100	107	100
HBYS de hasta bilgileri için yapılabilen işlemler*	Okuma	159	24,9	83	23,1
	Yazma	117	18,3	60	16,8
	Silme	75	11,8	42	11,7
	Gönderme	51	8,0	36	10,0
	Değiştirme	66	10,3	39	10,9
	Kopyalama	51	8,0	42	11,7
	Ekleme	108	17,0	36	10,0
	Diğer	12	1,9	21	5,9
Toplam		639	100	359	100
HBYS'de erişilebilen hasta bilgileri*	Kimlik bilgileri	198	18,2	86	17,4
	İletişim bilgileri	171	15,8	57	11,6
	Hastalık bilgileri	171	15,8	63	12,8
	Tıbbi raporlar	144	13,2	69	14,0
	Tetkik sonuçları	177	16,3	75	15,1
	Önceden aldığı tıbbi hizmet bilgileri	57	5,2	54	11,0
	Ödeme bilgileri	72	6,7	36	7,2
	Sigorta bilgileri	87	8,0	42	8,6
	Diğer	6	0,6	12	2,4
Toplam		1083	100	494	100
Bilgi güvenliğini artırmak için alınabilecek önlemler*	Anti-virüs programlarının kullanımı	153	13,6	92	13,7
	Yazılım ve donanımın ihtiyaca göre güncellenmesi	144	12,8	92	13,7
	Şifre kullanımı	156	13,8	89	13,2
	Bilgisayarda kişisel usb kullanımının engellenmesi	99	8,8	60	9,0
	Bilgisayarı çalışanlar dışında kişilerin kullanmaması	129	11,4	83	12,3
	Çalışanın birimden ayrılırken bilgisayarını kapatması	138	12,2	71	10,6
	Şifrenin kesinlikle paylaşılmaması	168	14,9	92	13,7
	Şifrenin uygun kalitede seçiminin sağlanması	132	11,7	77	11,4
	Diğer	12	1,0	17	2,6
Toplam		1131	100	673	100

***** Bu sorularda araştırma grubu tarafından birden fazla seçenek işaretlenmiştir.

Tablo 4.4.4'te araştırmaya katılan tıbbi ve idari birim çalışanlarının bilgi güvenliği uygulamaları incelendiğinde, kimlik belirleme yöntemi olarak kullanıcı adı ve şifre kullanım oranlarının, gruplar arasında benzer olduğu belirlenmiştir.

Kullanılan şifre yapıları açısından; şifrede kişisel isim kullanımının %23,0 oranında ile sayı ve harfin bir arada kullanımı şeklindeki şifrelerin %19,2 oranında tıbbi birimlerce, şifrede sayı ve harfin bir arada kullanımı en yüksek %35,0 oranında idari birimlerce kullanıldığı görülmektedir.

Hastaya ait bilgilerin paylaşımı için onam formu alınması uygulamasında, tıbbi birimdekiler onam formu alındığını %55,8 oranında, idari birimdekiler ise onam formu alınmadığını %55,1 oranında değerlendirmişlerdir.

HBYS'nde hasta bilgileri için yapılabilen işlemler için; okuma %24,9 oranında, yazma %18,3 oranında, silme %11,8 oranında ve ekleme %17,0 oranında tıbbi birimlerce, okuma %23,1 oranında, yazma %16,8, silme %11,7 oranında ve kopyalama %11,7 oranında idari birimlerce olduğu tespit edilmiştir.

HBYS'nde erişilebilen hasta bilgilerinin; parametrelerde her iki grupta da kendi içinde yakın oranda dağılım göstermektedir. Önceden aldığı tıbbi hizmet bilgileri %5,2 oranında ve ödeme bilgilerinin %6,7 oranında tıbbi birimlerce, ödeme bilgilerinin %7,2 oranında ve sigorta bilgilerinin %8,6 oranında idari birimlerce erişimin en az olduğu görülmektedir.

Bilgi güvenliğini artırmak için alınabilecek önlemler konusunda, tüm parametrelerde grupların kendi içlerinde benzer oranda etkili görülürken; bilgisayarda kişisel usb kullanımının engellenmesi tıbbi birimlerce %8,8 oranında, idari birimlerce %9,0 oranında en az etkili olarak değerlendirilmiştir.

Araştırmaya katılan katılımcıların, "Kurumdaki bilgi güvenliği konusunda farkındalığı arttırmak için yapılabilecek uygulamaların öncelik sırası ne olmalı?" ve "Bilgilendirmenin yöntemlerden öncelik sırasına göre hangileri kullanılarak yapılmasını istersiniz?" sorularına vermiş oldukları cevapların frekans analizinden elde edilen veriler Tablo 4.4.5'te gösterilmektedir.

Tablo 4.4.5. Araştırmaya Katılan Tıbbi ve İdari Birim Çalışanlarına Göre Bilgi Güvenliği Kazalarının Duyurulma ve Farkındalık Sağlama Yöntemleri

Bilgi güvenliği konusunda farkındalığı artırmak için yapılabilecek uygulamalar	**Gruplar**	**Öncelik sıralaması**							
		1.sıra	**%**	**2.sıra**	**%**	**3.sıra**	**%**	**4.sıra**	**%**
	Eğitici poster hazırlanması	6	5,2	9	9,4	29	20,6	62	85,0
	Sms ile hatırlatıcı mesaj gönderilmesi	12	10,4	58	61,0	36	25,6	-	0
	HBYS üzerinden	20	17,3	2	2,1	74	52,4	10	13,7

	hatırlatıcı e-posta gönderilmesi								
	E-konferans düzenlenmesi	77	70,0	26	27,3	2	1,4	1	1,3
Toplam		115	100	95	100	141	100	73	100
Bilgi güvenliği konusunda yaşanan kazaların duyurulma yöntemlerinin tercihi	Sms ile mesaj gönderilmesi	16	11,6	10	9,4	55	56,1	25	29,8
	E-posta gönderilmesi	12	8,7	62	58,4	29	29,6	3	3,6
	E-konferans ile bildirilmesi	76	55,0	27	25,4	5	5,1	-	0
	Haber verilmemesi	34	24,7	7	6,7	9	9,1	56	66,7
Toplam		138	100	106	100	98	100	84	100

Tablo 4.4.5'te araştırmaya katılan çalışanlarının bilgi güvenliği kazalarının duyurulma ve farkındalığına bakışları açısından değerlendirildiğinde, bilgi güvenliği konusunda farkındalığı artırmak için yapılabilecek uygulamalarda e-konferans ile bildirilmesi (%70) ve sms ile mesaj gönderilmesi (%61) öncelikli yöntemler olarak tercih edilmiştir. Bilgi güvenliği kazalarının duyurulması için, e-konferans ile bildirilmesi (%55) ve e-posta gönderimi (%58,4) yöntemleri görülmektedir.

5. TARTIŞMA VE SONUÇ

Bu bölümde, araştırma kapsamında yapılan analizler sonucunda elde edilen bulgular tartışılmış ve HBYS' de bilgi güvenliği konusu ile ilgili yapılan literatürdeki çalışmaların bulguları ile karşılaştırılmıştır.

Bilgi güvenliğinin değerlendirilmesinde anketin ifadelerine bakılarak; ifadeler arasında en yüksek "Çalışanlar, kendi kullanıcı hesaplarıyla yetkilendirilip tanımlamaları yapılmadan, sistemlerimizde oturum açamaz / sistemlerimize erişim sağlayamazlar" (3,90±1,03), en düşük ise "Bilgi güvenliği uzmanı bulunmadığında dışarıdan danışmanlık hizmeti alınmaktadır" (2,77±1,25) ifadelerinden memnun olduğu tespit edilmiştir. Benzer bir sonuç HBYS'de çalışanlar gerektirdiği kadar yetkilendirildiği takdirde daha pratik olması, çalışanlar tarafından desteklendiğini göstermektedir. Bilgi güvenliği için sorumlu görülen sadece teknik hizmet biriminin olmaması gerektiği, çalışanlarında bilgi güvenliğinde etkin olması gerektiği vurgulanmaktadır (İleri 2016).

Çalışanların sundukları hizmetler arasında hastaya ait bilgilerin, çalışanlar tarafından yapılan işlemlerce bakanlığa elektronik ortamda güvenli şekilde aktarımı ve ihtiyaç dâhilinde başka yetkililerin erişimine bu çalışmada "hizmet sunumu" boyutu olarak adlandırılırken, Ay (2009) tarafından yapılan çalışmada "kaliteyi arttıran unsur" olarak değerlendirilmiştir.

Araştırmada güvenlik uygulamaları boyutunun en düşük ortalama değeri aldığı ortaya çıkmıştır. Benzer şekilde, Adams ve Garber'a (2007) göre güvenlik uygulamalarındaki problemlerin %99'u iyi niyetli çalışanlardan kaynaklandığı ve memnuniyet düzeylerinin düşük olduğu saptanmıştır. Sorunun kaynağı için daha çok eğitimsizlik üzerine durulmuştur. Çalışanlara belli bir yerde değil işlerinin başındayken eğitim verildiği belirtilmiştir. Güvenlik uygulamalarının eğitim konusunda Isparta ilinde de çalışanların iyi niyetli davranışları gözlemlenmiştir.

Çalışmaya katılan bireylerin pozisyon değişkenine göre karşılaştırması yapıldığında örgütsel güvenlik boyutunda anlamlı bir farklılık olduğu tespit edilmiştir. Pozisyon değiştikçe bireylerin kurumun güvenliğine dair algılarının da etkilendiği ve tıbbi birimdeki bireylerin daha memnun oldukları saptanmıştır. Diğer boyutlarda ise pozisyon farklılığı memnuniyeti etkilememektedir. Vural ve

Sağıroğlu'nun (2008) yaptıkları çalışmada ise pozisyona bağlı kalmadan örgütsel güvenlik için belirlenen politikaları kapsayan talimatlar tespit edilmiştir.

Katılımcıların eğitim durumları ile bütün boyutlarının karşılaştırılmasına bakıldığında eğitim düzeyi arttıkça memnuniyet düzeyinde azalış görüldüğü tespit edilmiştir. Yüksek lisans ve üzeri mezun bireylerin; erişim ve yetkilendirmeyi orantılı bulmamaktadırlar. Güvenlik uygulamalarının ve hizmette sunumun yetersiz gördükleri ve kurumsal güvenliğin gerçek anlamda sağlanamadığı için de benimsenen güvenlik politikalarının çıkabilecek sorunları karşılamayacağını düşündükleri saptanmıştır. Az derece de bile okuma yazma bilmek algı düzeyini etkileyebilmektedir ve okuryazarlık düzeyinin azı çoğu olmadığı belirtilmiştir (Sanders 1994). Farklı eğitim düzeylerine sahip çalışanlarda yüksek lisans ve üzeri mezunlarının algı düzeylerinin diğerlerinden farklılaştığı tespit edilmiştir.

Katılımcıların demografik değişkenlerden yaş ve medeni durumun tüm boyutlarda anlamlı bir farklılık bulunmamakla birlikte, bilgi güvenliğinin değerlendirilmesi üzerinde bir etkiye sahip olmadığı saptanmıştır. Bunun sebebi olarak bilgi güvenliğinin daha çok eğitimle ilişkili olduğu düşünülmektedir.

Çalışmaya katılan bireylerin aylık gelir değişkenine göre karşılaştırması yapıldığında erişim ve yetkilendirme boyutunda anlamlı bir farklılık olduğu tespit edilmiştir. Gelir düzeyi 2000-3000 TL olan çalışanların geliri daha düşük olanlara göre yüksek mevkide oldukları ve yetkileri kapsamında erişimde sıkıntı yaşamadıkları saptanmıştır. Güvenlik uygulamaları boyutunda gelir düzeyi memnuniyeti etkilememektedir. Hizmet sunumu boyutuna bakıldığında en az gelire sahip çalışanların memnuniyet düzeylerinin düşük olduğu ve kendilerini hasta yerine koyduklarında daha fazla imkândan yararlanamadıklarını düşündükleri görülmüştür. Gelir düzeyi en fazla olan çalışanların yüksek kademelerde olduğu ve örgütsel güvenlik boyutundaki memnuniyet düzeyleri düşük çıkmıştır. Güvenlik politikaları boyutunda algı düzeyinin fazla olduğu grup 1603-2000 TL geliri olan çalışanların olduğu ve çoğunluğunu orta düzey amirlerden oluştuğu tespit edilmiştir.

Çalışmaya katılan bireylerin kurumda çalışma süresi değişkenine göre karşılaştırması yapıldığında güvenlik uygulamaları, hizmet sunumu ve örgütsel güvenlik boyutlarında anlamlı bir farklılık olduğu tespit edilmiştir. Yeni başlayan çalışanların kurumun bilgi güvenliğine ve hizmete dair memnuniyetleri yüksekken,

bu 5-10 yıldır çalışan tecrübeli kişilerde memnuniyet düzeyi tam tersidir. Bu durumda yaşça büyük bireylerde memnuniyetin daha düşük olmasıyla birlikte bugünün şartlarına göre uyum sağlamakta zorlandıkları düşünülmektedir. Tecrübeli çalışanlarda üstlenilen görevlere kıyasla kişilerin beklentileri oluşmakta ve bu beklentilerin üst kademelerce karşılanması gerektiği söylenebilir (Şahinaslan ve ark. 2009).

Katılımcıların HBYS deneyim değişkenine göre karşılaştırması yapıldığında erişim ve yetkilendirme, güvenlik uygulamaları, örgütsel güvenlik ve güvenlik politikaları boyutlarında anlamlı bir farklılık olduğu görülmüştür. Deneyimi farklı olan çalışanlarda boyutlara göre memnuniyet düzeyi değişirken, 0-1 yıl arasında deneyime sahip çalışanlarda her zaman en düşük memnuniyet düzeyi saptanmıştır. Benzer bir çalışmada kurumdaki deneyimin anlamlı bir farklılık göstermediği ancak kurumdaki güvenliği sağlamak adına çalışanların deneyimine bakılmadan risk ve hataların en aza indirgenmesi için bilgi verilmesi gerektiği söylemiştir (Tüzüner ve Özaslan 2011).

Dülger'in (2009) yaptığı bir çalışmada çalışanların bilgi güvenliğine dair eğitim almaları, farkındalığı ve bilinçlendirmeyi artırmakta önemli görmüştür. Yönetimsel düzenlemelerinde bu konuda desteklenerek kuruma göre eğitimin uygun verilmesi ve denetimle durum tespiti sonucunda önlemleri alınması, gereken gelişim ve değişimin önünü açacağı söylenebilir. Bu çalışmada da katılımcıların bilgi güvenliği algısını ölçmek için HBYS eğitimleri sorulmuştur. Katılımcıların %57,8'i (184 kişi) "HBYS eğitimi aldım" olarak işaretlerken, %42,2'i (134 kişi) "HBYS eğitimi almadım" olarak belirtmiştir. Bu eğitimlerin ise güvenliği için yapılan uygulamalarda, kurumun güvenliğini sağlamak adına ve benimsenen güvenlik politikalarında anlamlı bir fark oluşturduğu tespit edilmiştir. HBYS eğitim süresinde ise üç aydan fazla süren çalışanların algı düzeyi, diğer çalışanlara göre güvenlik politikaları boyutunda anlamlı bir şekilde artış gözlemlenmiştir. Bu eğitimlerin yeterliliği değerlendirildiğinde tüm boyutlarda yetersiz bulanların algı düzeyleri en düşük olarak saptanmıştır. Buna dayanarak eğitimleri yetersiz bulanların, bilgi güvenliğinin sağlanmasında kendilerini sorumlu görmedikleri düşünülmektedir.

Erçoban ve ark.'na (2018) göre çalışanların bilgisayar kullanım becerileri, dijitalleşen her geçen gün için önemi artmaktadır. Araştırmaları sonucunda

çalışanların bilgisayar kullanma becerilerinin geliştirilmesi için eğitim verilmesi, oluşabilecek teknik aksaklıkların önüne geçtiği saptanmıştır. Özellikle ileri yaştaki çalışanların için döneme uyum sağlamaları üzerinde durulmuştur. Bu çalışmada ise bilgisayar kullanım becerilerini yetersiz gören çalışanların güvenlik uygulamaları ve örgütsel güvenlik boyutlarında olduğu tespit edilmiştir. Gruplar arasındaki farka bakıldığında ise tıbbi birimlerce yeterlilik düzeyi %41,4 oranında 81-100 puan arasındayken, idari birimlerde %41,1 oranında 61-80 puanları arasındadır. Buna dayanarak tıbbi birim çalışanlarının, idari birimlere göre bilgisayar kullanım becerilerini daha yeterli gördüğü söylenebilir.

Bu çalışmada bireylerden, HBYS'nin nasıl algılandıkları ve beklentilerinin karşılanıp karşılanmadığını bilgi güvenliği bağlamında değerlendirmeleri istenmiştir. Çalışma kapsamında Isparta il merkezindeki Süleyman Demirel Araştırma ve Uygulama Hastanesi'nde çalışan toplam 317 kişiye ulaşılmıştır. Araştırmacı tarafından oluşturulan anketin ifadeleri 5 boyutta toplanmıştır. İlk faktör olan erişim ve yetkilendirme boyutunda çalışanlara, HBYS' de kimin hangi yetkilerle sınırlandırıldığı, kullanıcı-yönetici hesaplarının oluşturulması ve standartlarının belirlenmesi, kaynak erişim hakları gibi konuları içeren 9 ifade yer almıştır. İkinci faktör olan güvenlik uygulamaları boyutunda yetisiz erişimlerin engellenmesi, bilginin aslının korunması ve bunun için gereken denetimin ve ölçümlerin belirlenmesi, denetimlerin belgelendirilerek devamlılığın sağlanmasına dair 5 ifade ile değerlendirilmiştir. Üçüncü faktör olan hizmet sunumu boyutunda hastaya ait bilgilerin, çalışanlar tarafından yapılan işlemlerce bakanlığa elektronik ortamda güvenli şekilde aktarımı ve ihtiyaç dahilinde başka yetkililerin erişimine dair 4 ifade ile değerlendirilmiştir. Dördüncü faktör olan örgütsel güvenlik boyutunda çalışanlara, bilgi güvenliğini temel alarak belirlenen politikalara dair 5 ifade yer almıştır. Son faktör olan güvenlik politikaları boyutunda çalışanların sorumluluklarını, güvenliğin denetim araçlarının kullanımına ve sürecin yönetilmesindeki prensip ve işletime dair ifadeleri ölçen 4 ifade yer almıştır.

21. yüzyıldan itibaren bilgi çağının başlamasıyla kurum ve kuruluşlar ayak uydurmaya çalışmışlardır. Rekabette en önemli unsur haline gelen bilgi, tüm süreçleri etkilemeyi başarmıştır. Her türlü işlemlerin daha nitelikli hale gelmesiyle bilgi, önemini daha da arttıracağı söylenebilir. Kavram olarak bakıldığında değerli bulunan bilgi, hem güvenlik hem de güvenilirlik açısından birlikte

değerlendirilmelidir. Bilginin güvenli bir şekilde yönetilmesi, işin kapsamı ne olursa olsun isteğe bağlılıktan çok bir gereksinim haline gelmiştir. İlgili kurumun bilgi güvenliğini yönetebilmesi halinde, iş süreçlerinin ve ulaşılan çıktıların sorunsuz olmasını sağlayacaktır. Bunlara ayak uyduramayan kurum ve kuruluşlarda, sıkıntıların artıp çözüme ulaştıramamanın ve maddi manevi sorunların etkileri artması söz konusudur. Bu yüzden sağlık sektörüne çalışan üst düzey yöneticilerin süreçlerin işleyişini ve takibini gereken şekilde yapılabilmesi için destek olmalıdırlar. Uygulamaların hastanede kademe gözetmeksizin her birimde uygulanması önem taşımaktadır. Bilgi güvenliği için geliştirilen standartlardan da yararlanılması sağlıklı olacaktır. Uygulamaların belirlenmesi kadar sürekliliği de sağlanmalıdır. Bilgi güvenliği denilince akla bilgisayar ve yazılımsal önlem gelse de sadece bunlardan ibaret değildir. Bu önlemlerin gereksiz görülüp ihmal edilmesi kurumda itibarı zedeleyebilir (ITGI 2007; Tipton ve Krause 2007). Bu açıdan araştırmanın sonuçlarının değerli olduğu düşünülmektedir.

Ayrıca HBYS ile sağlık hizmeti sunumunda büyük gelişmelerin yaşandığı ve sağlık hizmetlerinden memnuniyet düzeyinin yükseldiği bilinmektedir. Ancak HBYS sonrası bilgi yönetimi açısından çalışanların bakış açısıyla hastane bazlı durumun ne olduğunu ortaya koyan güncel bir çalışma ile literatürde karşılaşılmamıştır. Bu sebeple araştırma, hastane çalışanlarının HBYS'ye duydukları güven açısından da önem taşımaktadır.

Araştırmada bilgi güvenliği yönetimi, öncelikle erişim ve yetkilendirme boyutunda ele alınmıştır. Ayrıca bilginin korunması için gereken güvenlik uygulamaları, güvenli bilgi kullanımının sağlanmasında hizmet sunumu, belirlenen politikalar doğrultusunda örgütsel güvenlik ve güvenliğin denetim organları olarak güvenlik politikaları boyutları hastane çalışanları tarafından değerlendirilmiştir. Çalışanların en çok memnun kaldıkları konunun çalışanlara yetki verilmeden önce sistemde oturum açamaması olduğu tespit edilmiştir. Çalışanların erişim ve yetkilendirme, örgütsel güvenlik ve güvenlik politikaları iyi düzeydeyken; benimsenen güvenlik uygulamaları boyutunda algıları orta düzeyde olduğu bulunmuştur.

Çalışanların erişim ve yetkilendirme ile hizmet sunumu boyutundan memnuniyetlerinin iyi düzeydeyken; benimsenen bilgi güvenliği yönetimi

değerlendirilmesinin alındığı güvenlik uygulamaları, örgütsel güvenlik ve güvenlik politikaları boyutunda çalışanların algılarının orta düzeyde olduğu bulunmuştur.

Demografik değişkenlerden eğitim grubuna bakıldığında nitelik arttıkça, çalışanların sisteme ilişkin erişim ve yetkilendirme algılarının da yükselme eğiliminde olduğu sonucuna varılmıştır. Ancak çalışanların niteliği arttıkça güvenlik uygulamalarından memnuniyet düzeylerinin azaldığı ve uygulamaların yüksek lisans ve üzeri mezun çalışanları daha az tatmin edici olduğu sonucu elde edilmiştir. Lise mezunu çalışanların bilgi güvenliği yönetiminden genel olarak daha memnun oldukları sonucuna ulaşılmıştır. Bir diğer sonuç olarak da HBYS deneyim süresi 0-1 arasında olan bireylerin erişim durumlarına, güvenlikle ilgili uygulamalara, hizmet sunumuna, örgütün güvenliğine ve güvenlik için uygulanan politikalara dair algılarıyla birlikte diğer gruplara göre daha düşük olduğu sonucuna varılmıştır.

Araştırmada ortaya çıkan hizmet sunumu boyutunda demografik değişkenlere göre genel olarak memnuniyet düzeyinin yüksek olduğu görülmüştür. Çalışanların hastaya ait bilgileri nasıl kullanılacağına dair elektronik ortamda güvenli şekilde aktarımı ve ihtiyaç dahilinde başka yetkililerin erişiminde genel olarak yaptıkları ve bireylerin bu durumdan memnun oldukları sonucuna varılmıştır.

Araştırma sonucunda bilgi güvenliğinin değişen roller bağlamında benimsenen güvenlik uygulamalarında yetersiz olduğu, çalışanların bilgi güvenliği yönetiminden orta derecede memnun oldukları sonucuna varılmıştır. Ancak çalışanlar örgütün güvenliğinin sağlandığı ve güvenlikteki politikalardan iyi derecede; erişimdeki yetkilendirmelerin orantılılığında ve hizmet sunumunda yüksek derecede memnun oldukları bulunmuştur.

Çalışmada tıbbı ve idari birimlerin ortak olarak hasta ve sosyal güvence bilgilerine ulaşabildikleri tespit edilmiştir. Ayrıca grupların, bilgi işlem yetkilendirmelerinden benzer olduğu sonucuna ulaşılmıştır. Bu yüzden ilgili olmayan bilgilere erişim ve işlem yetkileri bilgi güvenliği açısından risk oluşturabilir. Bilgi güvenliğini arttırma için alınması gereken önlemler ve bilgi güvenliğinde yaşanılan aksaklıkların duyurulması konularında cevaplayanların yarısından fazlasının fikir beyan etmediği anlaşılmıştır. Buna bağlı olarak ilgili konularda gereken hassasiyetin yeterli olmadığı tespit edilmiştir.

Sonuçlar değerlendirildiğinde bilgi güvenliğine yönelik aşağıdaki önerilerin önemsenmesi buna yönelik tedbirlerin alınmasının faydalı olacağı değerlendirilmiştir:

- Sağlık birimi çalışanlarının şifre yapılarında kişisel isim, 1234 ve 8765 gibi sayıları çokça kullanmaları bilgi güvenliği açısından zafiyet teşkil etmektedir. Şifrelerde bu tür yapıların kullanılmaması gerektiğinin anlatılması;

- Bilgi güvenliği sorunlarının nedenlerinin en çok denetimsizlik, ceza olmaması, bilgisayarların ortak kullanılması ve bilgi yetersizliğinden kaynaklandığı ifade edilmektedir. Çalışanların bu görüşü dikkate alınarak daha sıkı denetim yapılmasının, bilgi güvenliği konusuna yeterince özen göstermeyen personele cezai yaptırım uygulanmasının, bilgisayarların mümkün mertebe ortak kullanıma kapatılmasının;

- Bilgi güvenliğinin daha da artırılması için anti-virüs programları kullanılmasının, şifrelerin kesinlikle kullanıcının kendisi dışında biriyle paylaşılmamasının ve yazılım/donanım güncellemeleri yapılmasının;

- Yöneticilerin olduğu kadar diğer çalışanların da bilgi güvenliği konusunda bilinçlendirilmesinin;

- HBYS eğitimleri görmüş personelin sayısının artırılması, daha çok personelin bu eğitimi almalarının sağlanmasının faydalı olacağı değerlendirilmektedir.

Bundan sonraki dönemde aynı konuda yapılacak çalışmalarda anketlerin devlet hastanesi, aile tıp merkezleri vb. farklı türdeki sağlık kuruluşlarında uygulanarak çıkan sonuçların bu araştırma sonuçlarıyla karşılaştırılmasının sağlık birimlerindeki bilgi güvenliğine yönelik tutumların daha iyi anlaşılmasını sağlayacağı değerlendirilmektedir.

KAYNAKLAR

Adams JL, Garber S. Reducing medical malpractice by targeting physicians making medical malpractice payments. J Empirical Legal Stud 2007; 4:185-222. http://dx.doi.org/10.1111/j.1740-1461.2007.00087.x (10.07.2018).

Akartepe A. Tedavi sözleşmesinin hukuki niteliği, Erzincan Sağlık Hukuku Sempozyumu, Yetkin Yayınları, Ankara, 2007.

Akpolat M. Hastane bilgi sistemleri kurulum süreci. Sağlık kurumlarında bilgi sistemleri (Ed. A. Yılmaz), Eskişehir, 2013; s:109.

Akyıldız S. Hekimin cezai sorumluluğu bakımından uygulamada sorunlar, V. Türk Alman Tıp Hukuku Sempozyumu, Tıp Hukukunun Güncel Sorunları, Türkiye Barolar Birliği Yayınları, Ankara 2008;142.

Alpar R. Uygulamalı istatistik ve gerçeklik- güvenirlik. Detay Yayıncılık, 4. Baskı, Ankara, 2016; ss:413-431.

Altındiş S, Kurt M. Bilgi yönetim uygulamalarının hasta güvenliğine etkisine ilişkin bir araştırma: Afyonkarahisar ilinde bir uygulama. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 2010; 24: 45-61.

Argyris C. Knowledge for action: a guide to overcoming barriers to organizational change. Jossey-Bass, San Francisco, 1993.

Arslan Ç, Azizağaoğlu B. Yeni türk ceza kanunu şerhi, Asil Yayıncılık, Ankara, 2004.

Austın C. J, Boxerman, S. B. Information systems for health care management, Health Administration Press. Institute of Medicine, Crossingthe Quality Chasm: A New Health System for the Twenty-first Century. National Academies Press, Washington, 2003.

Austın C. J, Trimm J. M, Sobczak P. M. Information systems and strategic management. Health Care Management Review, 1995; 20(3): 26-33.

Ayan M, Tıbbi müdahalelerden doğan hukuki sorumluluk, Ankara,1991.

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

Bartlett C, Boehncke K, Haikerwal M. E-health: enablerfor australia's health reform, 2008. www.health.gov.au/nhhrc/publishing,(18.02.2015).

Başalp N. Kişisel verilerin korunması ve saklanması, Yetkin Yayınları, Ankara, 2004.

Baykara M, Daş R, Karadoğan İ. Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi. 1st International Symposium on Digital Forensicsand Security (ISDFS'13) Proceedings, http://isdfsweb.firat.edu.tr/Upload/ISDFS2013_Proceeding_Book.pdf – 2013 (10.07.2018).

Bayraktar K. Hekimin tedavi nedeniyle cezai sorumluluğu. İstanbul Üniversitesi Hukuk Fakültesi Yayınları, 1972.

Canberk G, Sarıoğlu Ş. Bilgi güvenliği ve süreçleri üzerine bir inceleme. Politeknik Dergisi, 2006; 3: 165-174.

Cavallı E, Mattasoglio A, Pinciroli F, vd. Information security conceptsand practices: the case of a provincial multi-specialty hospital. International Journal of Medical Informatics, 2004; 73(3): 297-303.

CE (Certification Europe). ISO 27001 global survey: the factsand the figures underlying the growth of ISO 27001 world-wide, 2008. http://www.d10736251.blacknight.com/format/ISO27001 GlobalSurvey.pdf (08.02.2015).

Chess B, Arkin B. The case for mobile two-factor authentication. IEEE Security & Privacy, 2011: 81-85.

Çelik L, Tetik M. Afyonkarahisar ağız ve diş sağlığı merkezi personelinin bilişim teknolojileri kullanım becerilerinin incelenmesi. Journal of Strategic Research in Social Science, 2015; 1(1): 37-52.

Çokluk Ö, Şekercioğlu G, Büyüköztürk Ş. Sosyal bilimler için çok değişkenli istatistik SPSS ve Lisrel Uygulamaları. Pegem Akademi, 4. Baskı, Ankara, 2016.

Donay S. Meslek sırrının açıklanması suçu. İstanbul,1978.

Dural M. Türk medeni hukukunda gerçek kişiler. Filiz Kitabevi, İstanbul, 1995.

Durmuş B, Yurtkoru E. S, Çinko M. Sosyal bilimlerde SPSS'le veri analizi. Beta Basım Yayım, 4.Baskı, İstanbul, 2011.

Dülger V. Bilişim suçları ve internet iletişim hukuku. Seçkin Yayıncılık, 3.Baskı, Ankara, 2013.

Dülger V. Sağlık hukukunda kişisel verilerin korunması ve hasta mahremiyeti. Hukuk Günlüğü, 2015.http://www.hukukgunlugu.org/saglik-hukukunda-kisisel-verilerin-korunmasi-ve-hasta-mahremiyeti/ (03.02. 2018).

Eminağaoğlu M, Gökşen Y. Bilgi güvenliği nedir, ne değildir, Türkiye' de bilgi güvenliği sorunları ve çözüm önerileri. Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 2009; 11(4): 1-15.

Erçoban N, Sökel S, Özcan H, Akıner F. Devlet hastanesi çalışanlarının bilgisayar kullanım becerilerinin değerlendirilmesi.2018, sy:6.

Er Ü. Sağlık hukuku, Savaş Yayınevi, Ankara, 2008.

Erdem M, Sancaklı O, Tezcan D. Avrupa insan hakları sözleşmesi ve uygulaması. T.C. Adalet Bakanlığı Eğitim Dairesi Başkanlığı, Ankara, 2004.

Erdem M, Ruhan V. Tıp hukukunun güncel sorunları. Türk Alman Tıp Hukuku Sempozyumu, Türkiye Barolar Birliği Yayınları, Ankara, 2008; 142.

Erman B. Ceza hukukunda tıbbi müdahalelerin hukuka uygunluğu. Seçkin Yayıncılık, Ankara, 2003.

Etzıonı A. The limits of privac basic books. New York, 1999.

Fernando J. I, Dawson, L. L. The health ınformation system security threat lifecycle: an ınformatics theory. International Journal of Medical Informatics, 2009; 78(12): 815–826.

Floridi, L. Information: a very short ıntroduction. Oxford University Press, New York, 2010.

Guthrie J. Time is running out-the burdens and challenges of HIPAA compliance: a look at preemption analysis, the minimum necessary standard and the notice of privacy practices. Annals Health L., 2003; 12,143.

Güleş H. K, Özata M. Sağlık bilişim sistemleri. Nobel Yayın Dağıtım, Ankara, 2005.

Hakeri H. Tıp hukuku. Seçkin Yayıncılık, Ankara, 2007.

Hancı H. Malpraktis tıbbi girişimler nedeniyle hekimin ceza ve tazminat sorumluluğu. Seçkin Yayıncılık, Ankara, 2006.

Hatırnaz E. G. Özel hastanelerin hukuki sorumluluğu ve hasta hakları. Seçkin Yayıncılık, Ankara, 2009.

Hatun Ş. Hasta hakları. İletişim Yayıncılık, İstanbul, 1999.

Haux R. Healthin formation systems; past present future. International Journal of Medical Informatics, 2006; 75: 268–281.

Hayes M. S. The ımpact of privacy on ıntellectual property in canada1. Intellectual Property Journal, 2006;20(1), 67.

Hevner A. R, Salvatore T. M, Jinsoo P, Sudha R. Design science in information systems research. John Leslie King And Kalle Lyytinen (Eds.). In, Information Systems The State of the Field. West Sussex: John Wiley & Sons Ltd, 2006: 191-232.

Holden R. J. What stands in the way of technology- mediated patient safety ımprovements? a study of facilitatorsand barriersto physicians' use of electronic health records. Journal of Patient Safety, 2011; 7(4): 193-203.

IMF (International Monetary Fund). International financial statistics (IFS), 2014. http://www.imf.org (24 Mayıs 2015).

ITGI Inst. Cobit 4.1; framework, control objectives, management guidelines and maturity models. USA: ITGI Publishing, 2007.

İleri Y.Y. Örgütlerde bilgi güvenliği yönetimi, kurumsal entegrasyon süreci ve örnek bir uygulama. Anadolu Üniversitesi Sosyal Bilimler Dergisi, 2016. http://sbd.dergi.anadolu.edu.tr/yonetim/icerik/makaleler/1376-published.pdf (01.10.2018).

İleri Y. Y. Kurumsal bilgi kaynaklarına erişimde güvenlik: hekimlerin şifre yönetimine yönelik bir araştırma. Usaysad Dergi, 2018; 4(1): 15-25. http://dergipark.gov.tr/download/article-file/471485 (01.10.2018).

İpekyüz F. Y. Türk hukukunda hekimlik sözleşmesi. Vedat Kitapçılık, İstanbul, 2006.

İslamoğlu AH. Sosyal Bilimlerde Araştırma Yöntemleri. Beta Basım. 2009. İzmit.

İstanbul Sağlık Müdürlüğü. Kurumsal uygulamalar. http://ihs.istanbulsaglik.gov.tr/kurumsal-uygulamalar/48 (03.05.2018).

Jaın A. K. Biometric authentication: system security and user privac. IEEE Computer Society. 2012; 87–92.

Kağnıcıoğlu H, Sevim A. Yönetim bilgi sistemi. Anadolu Üniversitesi Yayınları, 2005.

Kalaycı Ş. SPSS uygulamalı çok değişkenli istatistik teknikleri. Asil Yayınları, Ankara, 2010.

Kaplanoğlu, E. Mesleki stresin temel nedenleri ve muhtemel sonuçları: Manisa ilindeki SMMM'ler üzerine bir araştırma. Muhasebe ve Finansman Dergisi, 2014; (10), 131–150.

Karasu S. Hekimin sır saklama yükümlülüğü. Vedat Kitapçılık, İstanbul, 2009.

Kayış A. Güvenirlik analizi (Reliability analysis. SPSS uygulamalı çok değişkenli istatistik teknikleri. İçinde: Kalaycı Ş. (ed) , Asil yayın dağıtım, Ankara, 2006; ss: 403-419.

Kavuncubaşı Ş. Yıldırım S. Hastane ve sağlık kurumları yönetimi. Siyasal Kitabevi, Ankara, 2012.

Khalıfa M. Barriersto health ınformation systemsand electronic medical records ımplementation. Procedia Computer Science, 2013; 21: 35–342.

Köksal A, Esatoğlu A. E. Ankara ilindeki üniversite ve özel hastanelerde kullanılan elektronik hastane bilgi sisteminin analizi. Ankara Üniversitesi Dikimevi Sağlık Hizmetleri Meslek Yüksekokulu Dergisi, 2005; 7(1): 53-65.

Krogh VG, Ichıjo K. Bilginin üretimi. Dışbank Yayınları, 2007.

Küzeci E. Kişisel Verilerin Korunması, Elektronik Dergi, 2011 http://www.bilisimdergisi.org/s128 (03.05.2018).

Küzeci E. Kişisel Verilerin Korunması. Turhan Kitabevi, Ankara, 2010.

Lucas HC. Information Systems Conceptsfor Management. New York Mc Graw Hill Book Company, 1990: 442.

Malkoç İ. Açıklamalı İçtihatlı 5237 Sayılı Yeni Türk Ceza Kanunu, Malkoç Kitabevi, Ankara, 2007.

Medlin D. B. & Cazier, J. A. An Empirical Investigation: Healthcare Employee Passwords And Their Crack Times In Relationship To HIPAA Security Standards. International Journal of Health Care Informatics, 2007; 2(3): 39-48.

Meran Necati, Gerekçeli-Karşılaştırmalı 5237 Sayılı Türk Ceza Kanunu, Seçkin Yayınevi, Ankara, 2004.

Mole DJ, Fox C, Napolitano G. Electronic patient data confidentiality practice samongsurgicaltrainees: questionnairestudy. Annals of the Royal Collage of Surgeons of England, 2006; 88(6): 550-553.

Morgan G. A., et al. SPSS for introductory statistics: Use and interpretation. Psychology Press, 2004.

Morse E. A., Raval, V. PCI DSS: Payment card industry data security standards in context. Computer Law & Security Review, 2008; 24(6), 540-554.

Mumcu G. Elektronik sağlık sayıt sistemi: sağlık hizmetlerinde bilişim teknolojisinin uygulama alanları. Bedray Yayıncılık, Ankara, 2011.

Nehta (National E-Health Transition Authority). Privacy blueprint on unique healthcare ıdentifiers. www.nehta.gov.au 2007 (08.05.2015).

Özbek V. Ö. Yeni türk ceza kanununun anlamı, C. 2, Seçkin Yayıncılık, Ankara, 2008.

Özkan H., Akyıldız S. Açıklamalı içtihatlı hasta hekim hakları ve davaları. Seçkin Yayıncılık, Ankara, 2008.

Öztemiz S. Yılmaz B. Bilgi merkezlerinde bilgi güvenliği farkındalığı. Bilgi Dünyası, 2013; 14(1), [Elektronik Dergi], http://www.bd.org.tr/index.php/bd/article/view/105 (08.05.2015).

Öztürkler C. Hukuk uygulamasında tıbbi sorumluluk, teşhis, tedavi ve tıbbi müdahaleden doğan tazminat davaları. Seçkin Yayıncılık, Ankara, 2003.

Pagliari C. Donnan P. Morrison J. vd. Adoption And Perception Of Electronic Clinical Communications InScotland. Informatics in Primary Care, 2005; 13(2): 97-104.

Parlar A., Hatipoğlu M. Türk ceza kanunu yorumu, Seçkin Yayıncılık, Ankara, 2008.

Patel V. M., Yeh T., Fathy M. E., Zhang Y., Chen Y., Chellappa B. R., Davis L. Screen fingerprints: a novel modalityfor active authentication, IT Pro, 2013; 38-42.

Pwc, Managing cyber risksın an ınterconnected world: keyfindings from the global state of ınformation security survey. http://www.pwc. com/gx/en/consulting-services/information-security-survey (07.04.2015).

Rajalakshmi K., Mohan S. C., Babu S. D. Decision support system in health carein dustry. International Journal of Computer Applications, 2011; 26(9): 42-44.

Rindfleisch T.C. Privacy, İnformationte Chnology and Health Care Communi cations of the ACM, 1997; 40: 93-100.

Rodoplu D. Bilgi teknolojileri uygulamalarına karşı çalışan direnci; hastane bilgi sistemi üzerinde bir uygulama. Review of Social, Economic & Business Studies, 2007; 9(10): 409-438.

Sağsan M. Uygulamadan disipline bilgi yönetimi ve bir alan çalışması. Amme İdaresi Dergisi, 2007; 40(4): 103-131.

Sanders B. A is for Ox: Violence, Electronic Media, and the Silencing of the Written Word 1994; 23.

Sarıtaş H. Hasta hakları açısından hekimin sorumluluğu. Bilge Yayınevi, Ankara, 2005.

Savaş H. Sağlık çalışanlarının ve sağlık kurumlarının tıbbi müdahaleden doğan sorumlulukları ceza – hukuk. Seçkin Yayıncılık, Ankara, 2007.

Sert G. Hasta hakları. Babil Yayınları, İstanbul, 2004.

Sert G. Tıp etiği ve mahremiyet hakkı. Babil Yayınları, İstanbul, 2008.

Sultan F., Aziz M. T., Khokhar I. vd. Development of an ın-house hospital ınformation system ın a hospital ın pakistan. International Journal of Medical Informatics, 2014; 83(3): 180-188.

Sun J., Fang, Y., Zhu X. Privacy and emergency responseın e-health care leveraging wireless body sensor networks. IEEE Wireless Communications, 2010; 66-73.

Sütlaş M. Hasta ve hasta yakını hakları, İstanbul, 2000.

Şahin A. Kamu kurumlarında bilgi teknolojilerinin kullanımında yaşanan sorunlar: Konya kaymakamlıkları örneği. Amme İdaresi Dergisi, 2008; 41(1): 149-171.

Şahin, M. Yönetim bilgi sistemi. Anadolu Universitesi, 2003; 784.

Şahinaslan E., Kandemir R., Şahinaslan Ö. Bilgi güvenliği farkındalık eğitim örneği, akademik bilişim'09 - XI. Akademik Bilişim Konferansı Bildirileri Şubat, Harran Üniversitesi, Şanlıurfa, 2009; 194: 11-13.

Şen E. Yeni türk ceza kanunu yorumu. Cilt: I, Vedat Kitapçılık, İstanbul, 2006.

T.C. Resmi Gazete, 15 Mayıs 1987, Sayı: 19461.

T.C. Sağlık Bakanlığı, Kurumumuzda karar destek sistemi, 2013. http://www.e-saglik.gov.tr/belge/1-37906/kurumumuzda-karar-desteksistemi.html (09.01.2018).

T.C. Sağlık Bakanlığı, Veri güvenliği konulu genelgesi, Genelge 2005; 153.

Tandoğan H. Borçlar hukuku özel borç ilişkileri. C.II, Ankara, 1985.

Tang P.C, Lansky D. From the field: the missing link: bridging the patient provider health ınformation gap. Health Aff, 2005; 24(5): 1290-1295.

Tang P.C, Newcomb C. Informing patients: a guide for providing patient health ınformation,. Journal of the American Medical Informatics Association, 1998; 5(6): 563-570.

Tarullo D. K. Banking on basel: the future of international financial regulation. Peterson Institute, 2008.

Tekerek M. Bilgi güvenliği yönetimi. KSÜ Fen ve Mühendislik Dergisi, 2008;11(1): 132-137.

Tengilimoğlu D, Çelik Y, Ulgu M. Comparison of computing capability and information system a bilities of state hospital sowned by ministry of laborand social security and ministry of health. J Med Syst, 2006; 30(4): 269-275.

Tengilimoğlu D, Akbolat M, Işık O. Sağlık işletmeleri yönetimi, Nobel Yayıncılık, Ankara, 2015.

Timmons S. Nurses resisting ınformation technology. Nursing Inquiry, 2003; 10(4): 257-269.

Tipton H. F, Krause M. Information security management handbook. Auerbach Publicaions, 2007.

T.M.H. Turkish ministry of health. Statistical Year Book of Health Care İnstitutions, 2006.

Tüzüner V. L, Özaslan B Ö. Hastanelerde iş sağlığı ve güvenliği uygulamalarının değerlendirilmesine yönelik bir araştırma, İstanbul Üniversitesi İşletme Fakültesi Dergisi, 2011; 40 (2): 138-154.

Uludağ A, İleri Y. Y. Kurum içi halkla ilişkiler bağlamında hastanelerde otomasyon sistemlerin değerlendirilmesi bir tıp fakültesi, 2018; 11(1): 167-178.

Upfold CT, Sewry DA. An investigation of Information Security in Small and Medium Enterprises (SMEs) in the Eastern Cape, In: Venter HS, Elof JHP, Labuschagne L, Eloff MM.(Eds.) Proceedings of the ISSA 2005 new knowledge today conference, South Africa, 2005;b082: 1-17. URL:http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/082 Article.pdf

Ülgü M. Hastane Bilgi Sistemleri Alımı Çerçeve İlkeleri, T.C Sağlık Bakanlığı Bilgi İşlem Daire Başkanlığı, Ankara, 2008; 5.

Vardal N. Yükseköğretimde bilgi güvenliği: bilgi güvenlik yönetim sistemi için bir model önerisi ve uygulaması. G.Ü. Eğitim Bilimleri Enstitüsü, Doktora Tezi, Ankara, 2009 (Danışman: Prof. Dr. Halil İbrahim Yalın).

Vural Y, Sağıroğlu, Ş. Kurumsal bilgi güvenliği: güncel gelişmeler. ISO Turkey, Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı, Ankara, 2007.

Vural, Y, Sağıroğlu Ş. Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 2008; 23(2).

Wager K. S, Lee F. W, Glaser, J. P. Health care ınformation systems, second edition jossey bass, 2009.

Williams P. When trust defies commons, 2008.

Wirken G. Information security in dutch hospitals. Master Thesis Content and Knowledge Engineering Faculity of Science, 2012: 41-53.

Yıldırım T. Hasta hakları, sağlık hukuku ve yeni türk ceza kanunundaki düzenlemeler. Marmara Üniversitesi Hukuk Fakültesi Sempozyumu, İstanbul, 2007;1.

Yıldız Ç. Telekomünikasyon sektöründe firma içindeki bilgi güvenliğini etkileyen faktörler ve bu faktörlerin çalışanlar üzerine etkileri. Gebze Yüksek Teknoloji Enstitüsü Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Gebze, 2009 (Danışman: Doç. Dr. Salih Zeki İmamoğlu)

Yip, W. C. M, Hsiao, W. C, Chen, W, Hu, S, Ma, J, Maynard, A. Early appraisal of China's huge and complex health-care reforms. The Lancet, 2012; 379(9818), 833-842.

Yokuş S. H. Tıp ceza hukukunda kişisel verilerin açıklanması. V. Türk Alman Tıp Hukuku Sempozyumu, Tıp Hukukunun Güncel Sorunları, Türkiye Barolar Birliği Yayınları, Ankara, 2008; 142.

Zaim H. Bilginin artan önemi ve bilgi yönetimi. İşaret Yayınları, 2005; 122-134.

http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm (15 Mart 2018).

http://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/bilisim-sistemleri-guvenligi-arastirmalarinin-yonu.html, Kara M, Bahşi H. Bilgi Sistemleri Güvenliği Araştırmalarının Yönü (15 Mart 2018).

http://www.sis.pitt.edu/jjoshi/courses/IS2150/Fall11/CSIsurvey2008.pdf (19 Mart 2018).

http://bilgiguvenligi.gov.tr/bt-guv.-standartlari/bilgi-guvenligi-standartlari.html, Poşul A. Bilgi Güvenliği Standartları (19 Mart 2018).

EKLER

Ek- A Etik Kurul Onay Yazısı

T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ REKTÖRLÜĞÜ
Bilimsel Araştırma ve Yayın Etiği Kurulu Başkanlığı

KONYA

SOSYAL VE BEŞERİ BİLİMLER ETİK KURULU KARARI

Toplantı Sayısı : 33	**Toplantı Tarihi:** 19/02/2018
Karar Sayısı : 2018/3	

Yrd. Doç. Dr. Yusuf Yalçın İLERİ'nin danışmanlığını yürüttüğü yüksek lisans öğrencisi Hacer Özge KURT'un "Kurumlarda Bilgi Güvenliği Yönetimi; Hastane Bilgi Sistemleri Üzeri Bir Araştırma" isimli araştırma projesi ile ilgili 30/01/2018 tarih ve 4797 sayılı dilekçesi ve ekleri görüşüldü. Başvuru dosyası ve ilgili belgeler araştırmanın gerekçe, amaç, yaklaşım ve yöntemleri dikkate alınarak incelenmiş olup, araştırmanın gerçekleştirmesinde etik sakınca bulunmadığına oybirliği ile karar verilmiştir.

Prof. Dr. Raif PARLAKKAYA

Sosyal ve Beşeri Bilimler Etik Kurulu Başkanı

Nişantaşı Mah.Dr.H.Baybal Cad.No:12 Bera İş Merkezi Selçuklu -KONYA/ TÜRKİYE
Telefon: (0 332) 221 06 88 Faks: (0 332) 236 21 40
e-posta: rektorluk@konya.edu.tr Elektronik Ağ: www.konya.edu.tr
Bilgi: Ayşe CAN

T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ REKTÖRLÜĞÜ
Bilimsel Araştırma ve Yayın Etiği Kurulu Başkanlığı

KONYA

DEĞERLENDİRME FORMU

BAŞVURU BİLGİLERİ

ARAŞTIRMANIN AÇIK ADI	Kurumlarda Bilgi Güvenliği Yönetimi; Hastane Bilgi Sistemleri Üzeri Bir Araştırma	
SORUMLU ARAŞTIRMACI	Hacer Özge KURT	**UZM. ALANI:** Sağlık Bilimleri
ARAŞ. MERKEZİ VE ADRESİ	Necmettin Erbakan Üniversitesi	
ARAŞTIRMANIN AMACI	TEZ AMAÇLI ■ AKADEMİK AMAÇLI □	
ARAŞTIRMANIN TÜRÜ	Araştırma Projesi	
ARAŞ. KATILAN MERKEZLER	TEK MERKEZ ■ ÇOK MERKEZLİ □ ULUSAL ■ ULUSLARARASI □	
ARAŞTIRMA EKİBİ	Yrd. Doç. Dr. Yusuf Yalçın İLERİ (Danışman) Hacer Özge KURT (Yüksek Lisans Öğrencisi)	

KARAR:	**Karar No:** 2018/3	**Tarih: 19**/02/2018
	Yrd. Doç. Dr. Yusuf Yalçın İLERİ'nin danışmanlığını yürüttüğü yüksek lisans öğrencisi Hacer Özge KURT'un "Kurumlarda Bilgi Güvenliği Yönetimi; Hastane Bilgi Sistemleri Üzeri Bir Araştırma" adlı projesi değerlendirilmiştir. Araştırmanın gerekçe, amaç, yaklaşım ve yöntemleri dikkate alınarak incelenmiş, gerçekleştirilmesinde etik sakınca bulunmadığına oy birliği ile karar verilmiştir.	
	Etik bulunmama gerekçesi:	
	Karşı oy açıklaması:	

Yenişehir Mah.Dr.H.Baybal Cad.No:12 Bera İş Merkezi Selçuklu -KONYA/ TÜRKİYE
Telefon: (0 332) 221 06 88 Faks: (0 332) 236 21 40
e-posta: rektorluk@konya.edu.tr Elektronik Ağ: www.konya.edu.tr

T.C.
NECMETTİN ERBAKAN ÜNİVERSİTESİ REKTÖRLÜĞÜ
Bilimsel Araştırma ve Yayın Etiği Kurulu Başkanlığı

KONYA

ETİK KURUL BAŞKAN VE ÜYELERİ

Unvanı/Adı/Soyadı	Kurumu	Arş. İle İlişki	İmza
Prof. Dr. Raif PARLAKKAYA (Başkan)	N.E.Ü. Sosyal ve Beşeri Bilimler Fakültesi	YOK	
Prof. Dr. Bilal KUŞPINAR (Üye)	N.E.Ü. Sosyal ve Beşeri Bilimler Fakültesi	YOK	KATILMADI
Prof. Dr. Ahmet ERGÜLEN (Üye)	N.E.Ü. Sosyal ve Beşeri Bilimler Fakültesi	YOK	KATILMADI
Prof. Dr. Mehmet AKGÜL (Üye)	N.E.Ü. Ahmet Keleşoğlu İlahiyat Fakültesi	YOK	
Prof. Dr. Ahmet Turan YÜKSEL (Üye)	N.E.Ü. Ahmet Keleşoğlu İlahiyat Fakültesi	YOK	
Prof. Dr. Ahmet ÖNKAL (Üye)	N.E.Ü. Ahmet Keleşoğlu İlahiyat Fakültesi	YOK	KATILMADI
Prof. Dr. Nuri KÖSTÜKLÜ (Üye)	N.E.Ü. Ahmet Keleşoğlu Eğitim Fakültesi	YOK	
Prof. Dr. Fatih TEPEBAŞILI (Üye)	N.E.Ü. Ahmet Keleşoğlu Eğitim Fakültesi	YOK	
Prof. Dr. Ahmet SABAN (Üye)	N.E.Ü. Ahmet Keleşoğlu Eğitim Fakültesi	YOK	

Yenişehir Mah.Dr.H.Baybal Cad.No:12 Bera İş Merkezi Selçuklu -KONYA/ TÜRKİYE
Telefon: (0 332) 221 06 88 Faks: (0 332) 236 21 40
e-posta: rektorluk@konya.edu.tr Elektronik Ağ: www.konya.edu.tr

Ek- B Araştırma İzni

Tarih: 12.04.2018
Sayı : E.117493

T.C.
SÜLEYMAN DEMİREL ÜNİVERSİTESİ
Araştırma Ve Uygulama Hastanesi Başhekimliği
Kalite Yönetim Birimi

Sayı :87883530-060.99-E.
Konu :Araştırma İzni (Hacer Özge KURT)

NECMETTİN ERBAKAN ÜNİVERSİTESİ REKTÖRLÜĞÜNE
(Öğrenci İşleri Daire Başkanlığı)

İlgi :26.03.2018 tarihli ve 99132376-48178250-300-E.4275 sayılı yazı

Üniversiteniz Sağlık Bilimleri Enstitüsü Sağlık Yönetimi Tezli Yüksek Lisans Programı öğrencisi Hacer Özge KURT'un Doktor Öğretim Üyesi Yusuf Yalçın İLERİ danışmanlığında " Kurumlarda Bilgi Güvenliği Yönetimi:Hastane Bilgi Sistemleri Üzerinde Bir Araştırma"adlı tez çalışması kapsamında yapılacak anket çalışması uygun bulunmuş olup,bahsi geçen bu araştırmanın verilerinin hastane yönetimi ile paylaşılması gerektiğini bildirir,gereğini bilgilerinize rica ederim.

Prof. Dr. Mehmet YILDIRIM
Başhekim

Doğrulama Linki :https://ebys.sdu.edu.tr/EvrakDogrula.html?2574A9A9
SDÜ Arş.Uyg. Hast. Çünür Doğu Kampüsü ISPARTA
Tel No:(246) 211-9171 Faks No:(246) 211-2830
E-Posta:hastanekaliteyonetim@sdu.edu.tr İnternet Adresi:hastane.sdu.edu.tr
Bilgi İçin:Didem EKER
Hizmet Alımı
Tel No:2119171

Ek- C Anket Formu

Bu anket çalışması "Kurumlarda Bilgi Güvenliği Yönetimi: Hastane Bilgi Sistemleri Üzerinde Bir Araştırma" başlıklı yüksek lisans tez çalışmasına veri desteği sağlamak amacıyla hazırlanmıştır. Anketlerden elde edilecek bilgiler gizli tutulacaktır. Çalışma Doç. Dr. Yusuf Yalçın İLERİ'nin danışmanlığında yüksek lisans öğrencisi Hacer Özge KURT tarafından yürütülmektedir. (İletişim: hozgekurt@gmail.com)

I-Kişisel Bilgiler

1.Çalışmakta olduğunuz pozisyon:……...

2.En son mezun olduğunuz okul:
( )Lise ( )Yüksekokul ( )Lisans ( )Yüksek Lisans ve üzeri

3.Yaşınız:…….

4.Cinsiyetiniz: ( )Erkek ( )Kadın

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

6.Aylık geliriniz:
( )1603 TL ve altı ( )1604-2000 TL ( )2001-3000 TL ( )3001 TL ve üstü

7.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

8.Hastane bilgi yönetimi sistemi kullanımı deneyim süreniz:

( ) 0-1 yıl arası ( ) 1-5 yıl arası ( ) 5-10 yıl arası ( ) 10 yıl ve üzeri

9.Hastane bilgi yönetimi sistemini kullanmak için eğitim aldınız mı?
( )Evet ( )Hayır

10.Hastane bilgi yönetimi sistemini kullanmak için aldığınız eğitim ne kadar sürdü?
( ) 0-1 Hafta ( ) 1 Haftadan fazla, 1 aydan az

( ) 1 aydan fazla, 3 aydan az ( ) 3 aydan fazla

11.Aldığınız eğitimi nasıl değerlendirirsiniz?

( )Yetersiz ( )Kararsızım ( )Yeterli

12.Genel olarak bilgisayar kullanım becerinizi nasıl değerlendirirsiniz?

( )Yetersiz ( )Kararsızım ( )Yeterli

13.Genel olarak hastane bilgi yönetimi sistemi kullanım becerinizi nasıl değerlendirirsiniz?
( )0-20 puan ( )21-40 puan ( )41-60 puan ( )61-80 puan ( )81-100 puan

II-Bilgi Güvenliği İle İlgili Genel Sorular

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

( )Hastaya ait bilgiler ( )Çalışanlara ait bilgiler ( )Hastaneye ait mali bilgi

( )Yönetimsel raporlar ( )Süreçsel raporlar ( )Kurum Prosedürleri

( )Sigorta şirketi bilgileri ( )Sosyal güvence bilgiler ( )Diğer……..

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

( )Hastaya ait bilgiler ( ) Çalışanlara ait bilgiler ( ) Hastaneye ait mali bilgi

( )Yönetimsel raporlar ( ) Süreçsel raporlar ( ) Kurum prosedürleri

( )Sigorta şirketi bilgileri ( )Sosyal güvence bilgileri ( ) Diğer……..

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

( )Hastaya ait bilgiler ( ) Çalışanlara ait bilgiler ( ) Hastaneye ait mali bilgi

( )Yönetimsel raporlar ( ) Süreçsel raporlar ( ) Kurum prosedürleri

( ) Sigorta şirketi bilgileri ( )Sosyal güvence bilgileri ( ) Diğer…….

17. Hastane bilgi yönetimi sistemi üzerinden hasta verilerine erişiminiz kim/kimler tarafındandenetleniyor?.....

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

( )Kullanıcı adı ( )Şifre ( )Akıllı kart ( )Parmak izi ( )Diğer

19.Aşağıdaki şifre yapılarından herhangi birini kullanıyor musunuz?
(Birden fazla seçenek işaretleyebilirsiniz)

( ) 1234….. ( ) Şifrede bölüm adı kullanımı

( ) 8765….. ( ) Şifrede kişisel isim kullanımı

( ) Sayı ve harfin bir arada kullanımı ( ) Şifrede hastane adı kullanımı

( ) Kullanıcı adı ve şifrenin aynı olması ( ) Diğer

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

( )Evet ( )Hayır

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

( )Okuma ( )Yazma ( ) Silme ( ) Gönderme

( ) Değiştirme ( ) Kopyalama ( ) Ekleme ( ) Diğer…….

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

( ) Kimlik bilgileri ( ) İletişim bilgileri ( ) Hastalık bilgileri

( )Tıbbi raporlar ( )Tetkik sonuçları ( )Önceden aldığı tıbbi hiz. ait bilgiler

( )Ödeme bilgileri ( ) Sigorta bilgileri ( ) Diğer…….

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

( ) Anti-virüs programlarının kullanımı

( ) Yazılım ve donanımın ihtiyaca göre güncellenmesi

( ) Şifre kullanımı

( ) Bilgisayarda kişisel USB kullanımının engellenmesi

( ) Bilgisayarı çalışanlar dışında kimsenin kullanmasına izin verilmemesi

( ) Çalışanın birimden ayrılırken mutlaka bilgisayarını kapatması

( ) Şifrenin kesinlikle paylaşılmaması

( ) Şifrenin uygun kalitede seçiminin sağlanması

( ) Diğer…….

24. Sizce bilgi güvenliği ile ilgili sorunların nedeni nedir?.....

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

(….) Eğitici posterlerin hazırlanması

(….) SMS ile hatırlatıcı mesaj gönderilmesi

(….) Hastane bilgi yönetim sistemi üzerinden hatırlatıcı e-posta gönderilmesi

(….) E-konferans düzenlenmesi

(….) Diğer……..

26. Bilgi güvenliği ile ilgili yaşanan kazaların ve nedenlerinin sistem kullanıcılarına duyurulmasını ister misiniz?
( )Evet ( )Hayır

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

(….)SMS ile gönderilmesini isterim (….)E-posta ile gönderilmesini isterim

(….)E-konferans ile bildirilmesini isterim (….)Haber verilmesini istemem

28. Hastanedeki bilgi güvenliği için kaç puan verirsiniz?

(Çok kötü)0……..…100 (Çok iyi)

Aşağıdaki ifadelere ne derece katıldığınızı belirtiniz.

Hiç Katılmıyorum 	 1 2 3 4 5	 Tamamen Katılıyorum

29. Hastane bilgi güvenliğinin sağlanması için görevler ve sorumluluklar net olarak belirlenmiştir (örneğin; yedeklerin alınmasından, kullanıcıların sisteme kaydedilmesinden sorumlu olan çalışanlar bulunmaktadır).	1	2	3	4	5
30. Hastanede, bilgi güvenliğine ilişkin yazılı politikalar vardır.	1	2	3	4	5
31.Çalışanlar bilgi güvenliği politikalardan haberdardır.	1	2	3	4	5
32.Tüm personele yeterli ve uygun bilgi güvenliği eğitimi verilmektedir**.**	1	2	3	4	5
33. Çalışanlar bilgi sisteminde izin verilen ve onaylanmayan uygulamalar konusunda yeterince bilgilidir (örneğin; elektronik posta kullanımı ve internete bağlanma).	1	2	3	4	5
34. Bilgi güvenliğinin sağlanması için çalışanlar gerekli özeni gösterir.	1	2	3	4	5
35. Hastanedeki yöneticiler bilgi güvenliğine gereken özeni gösterir.	1	2	3	4	5
36.Yöneticiler bilgi güvenliliğinin uygulaması konusunda sorumluluk sahibidirler**.**	1	2	3	4	5
37.Hastane içinde bilgi güvenliği konusunda bir uzman bulunmaktadır.	1	2	3	4	5
38.Bilgi güvenliği uzmanı bulunmadığında dışarıdan danışmanlık hizmeti alınmaktadır.	1	2	3	4	5
39.Çalışanlar, güvenlik ihlali olaylarının derhal yönetime bildirilmesi gerektiğinden haberdardır.	1	2	3	4	5
40.Çalışanlar kendi çalışma alanlarından uzaklaştığında, bilgisayarlarını daima güvenli şekilde bırakmaları konusunda eğitilmiştir (örneğin; bilgisayar başından ayrıldığında bilgisayarların şifrelenmesi ya da oturumun kapatılması).	1	2	3	4	5
41.Güvenlik politikalarımızı ve süreçlerimizi ihlal eden çalışanlarımıza yönelik disiplin uygulamaları vardır.	1	2	3	4	5

42.Sistem arızası, çökmesi ya da hırsızlık gibi durumlarda, veri yedeklerimiz işimizde kesintiye yol açmayacak şekilde bilgilerimizi geri kazanmamızı sağlar.	1	2	3	4	5
43.Sistemlerimiz herhangi bir sorun oluşması beklenmeden, önceden oluşturulmuş bir plan doğrultusunda güncellenmektedir.	1	2	3	4	5
44.Bir güvenlik ihlalinin meydana gelmesi durumunda, yapılacaklar ve yardım için kimin aranacağı bilinmektedir.	1	2	3	4	5
45. Anti-virüs sistemimiz günceldir ve bir virüs saldırısı durumunda, sistemlerimizi mümkün olan en iyi şekilde korumaktadır.	1	2	3	4	5
46.Halka açık ağlara bağlı olmasına rağmen, sistemlerimiz İnternet Hizmeti Sağlayıcısının güvenliği ve/veya kendi güvenlik sistemlerimiz tarafından yeterince korunmaktadır.	1	2	3	4	5
47.Kullanıcıların sistemlerimizde oturum açmalarına yetki verecek uygun mekanizmalar bulunmaktadır.	1	2	3	4	5
48.Çalışanlar, kendi kullanıcı hesaplarıyla yetkilendirilip tanımlamaları yapılmadan, sistemlerimizde oturum açamaz / sistemlerimize erişim sağlayamazlar.	1	2	3	4	5
49.Şifre değiştirme sıklığını belirleyen ve şifre karmaşıklığını engelleyen bir şifre yönetim sistemi bulunmaktadır (örneğin, şifre iki haftada bir değiştirilmelidir ve en az ……. sayısı kadar karakter uzunluğunda olmalıdır).	1	2	3	4	5
50.Hastanede, kullanıcıların hangi verilere erişebileceğini belirleyen bir yetkilendirme prosedürü vardır.	1	2	3	4	5
51.Bilgi işlem uygulamaları sadece yetkilendirilmiş iş amaçları doğrultusunda kullanılır.	1	2	3	4	5
52.Hastanedeki iş yükünün fazla olması, bilgi güvenliğine gereken önemin verilmesini engellemez.	1	2	3	4	5
53.Bilgi güvenliği süreçleri, hizmet kalitesini olumsuz yönde etkilemez.	1	2	3	4	5
54.Bilgi güvenliği gün içinde yaptığımız işleri düşününce öncelikli bir konudur.	1	2	3	4	5
55.Bilgisayar kullanımı ile iş akışında olan değişimler bilgi güvenliğine gereken önemi vermeyi engellemez.	1	2	3	4	5