



T.C.

MARMARA ÜNİVERSİTESİ

SAĞLIK BİLİMLERİ ENSTİTÜSÜ

**HASTANE BİLGİ YÖNETİM SİSTEMİNİN
BİLGİ GÜVENLİĞİ AÇISINDAN DEĞERLENDİRİLMESİ**

PINAR KILIÇ AKSU

DOKTORA TEZİ

HASTANE İŞLETMECİLİĞİ ANABİLİM DALI

DANIŞMAN

Prof. Dr. Gonca MUMCU

2014 – İSTANBUL

TEZ ONAYI

Kurum : Marmara Üniversitesi Sağlık Bilimleri Enstitüsü
Programın seviyesi : Doktora
Anabilim Dalı : Hastane İşletmeciliği
Tez Sahibi : Pınar KILIÇ AKSU
Tez Başlığı : Hastane Bilgi Yönetim Sisteminin Bilgi Güvenliği Açısından
Değerlendirilmesi
Sınav Yeri : Marmara Üniversitesi Kartal Yerleşkesi
Sınav Tarihi : 18.06.2014

Tez tarafımızdan okunmuş, kapsam ve kalite yönünden Doktora Tezi olarak kabul edilmiştir.

Danışman (Unvan, Adı, Soyadı)

Prof. Dr. Gonca MUMCU

Kurumu

Marmara Üniversitesi

İmza



Sınav Jüri Üyeleri (Unvan, Adı, Soyadı)

Prof. Dr. Mehveş TARIM

Marmara Üniversitesi

Prof. Dr. Ayşe NUHOĞLU

Bahçeşehir Üniversitesi

Yrd. Doç. Dr. Cem DİKMEN


Bilim Üniversitesi

Yrd. Doç. Dr. Leyla KÖKSAL

Marmara Üniversitesi



Yukarıdaki jüri kararı Enstitü Yönetim Kurulu'nun 09.07.2014 tarih ve 31. sayılı kararı ile onaylanmıştır.


Prof. Dr. Feyza ARICIOĞLU
Sağlık Bilimleri Enstitüsü Müdürü

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

-Bu form bilgisayar ortamında doldurulacaktır.

BEYAN

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



PINAR KILIÇ AKSU

İÇİNDEKİLER	iii
TABLolar LİSTESİ	v
ŞEKİLLER LİSTESİ	viii
KISALTMALAR LİSTESİ	ix
EKLER LİSTESİ	x
ÖZET	11
SUMMARY	12
1. GİRİŞ ve AMAÇ	13
2. GENEL BİLGİLER	16
2.1. Türkiye Sağlıkta Dönüşüm Programı ve E-Sağlık Projesi	16
2.1.1. Ulusal Sağlık Veri Sözlüğü ve Minimum Sağlık Veri Setleri	17
2.1.2. Sağlık Kodlama Referans Sunucusu	18
2.1.3. Aile Hekimliği Bilgi Sistemi ve E-Sağlık	19
2.1.4. Elektronik sağlık kayıt sistemi	20
2.1.5. Tele-tıp ve telekomünikasyon	23
3. BİLGİ SİSTEMLERİ ve BİLGİ GÜVENLİĞİ	26
3.1. Bilgi Sistemleri	26
3.1.1. Bilgi sistemlerinin sınıflandırılması	28
3.2. Bilgi Yönetimi	31
3.2.1. Bilgi yönetimi faaliyetleri	31
3.2.2. Bilgi yönetiminin temel amaçları	33
3.2.3. Bilgi yönetiminin önemi	33
3.3. Bilgi Güvenliği	34
3.3.1. Bilgi güvenliğini etkileyen faktörler	35
3.3.2. Bilgi güvenliği sağlama araçları	40
3.3.3. Bilgi güvenliği standartları	40

4. HASTANE BİLGİ YÖNETİM SİSTEMLERİ ve BİLGİ GÜVENLİĞİ	46
4.1. Hastane Bilgi Yönetim Sistemleri	46
4.1.1. Hastane bilgi yönetim sistemlerinin kullanım alanları	47
4.1.2. Hastane bilgi yönetim sistemlerini oluşturan temel bileşenler	51
4.1.2.1. Yönetimi desteklemeye yönelik sistemler	51
4.1.2.2. Tanı ve tedaviyi desteklemeye yönelik sistemler	56
4.2. Hastane Bilgi Yönetim Sistemlerinde Bilgi Güvenliği	60
5. GEREÇ VE YÖNTEM	69
6. BULGULAR	73
7. TARTIŞMA	97
8. SONUÇ VE ÖNERİLER	112
9. KAYNAKLAR	114
10. EKLER	121
10. ÖZGEÇMİŞ	129

TABLolar LİSTESİ

Tablo 1: Bilgi güvenliği ölçeğine ait maddelerin faktör analizi ile dağılımı	72
Tablo 2: Araştırmaya katılan tıbbi ve idari birim çalışanlarının sosyo-demografik özellikleri	73
Tablo 3: Araştırmaya katılan tıbbi ve idari birim çalışanlarının çalışma durumları ve HBYS kullanımları	74
Tablo 4: Araştırmaya katılan tıbbi ve idari birim çalışanlarının HBYS kullanımı için eğitim alma durumları	75
Tablo 5: Araştırmaya katılan tıbbi ve idari birim çalışanlarının HBYS kullanımları	76
Tablo 6: Araştırmaya katılan tıbbi ve idari birim çalışanlarına göre HBYS kullanımında erişim denetimi	77
Tablo 7: Araştırmaya katılan tıbbi ve idari birim çalışanlarının bilgi güvenliği uygulamaları	78
Tablo 8: Araştırmaya katılan tıbbi ve idari birim çalışanlarının bilgi güvenliği kazalarına bakışı	80
Tablo 9: Araştırmaya katılan tıbbi ve idari birim çalışanlarına göre bilgi güvenliği kazalarının duyurulma ve farkındalık sağlama yöntemleri	80
Tablo 10: Araştırmaya katılan tıbbi ve idari birim çalışanlarına göre güvenlik politikası boyutu	81
Tablo 11: Araştırmaya katılan tıbbi ve idari birim çalışanlarına göre örgütsel güvenlik boyutu	82

Tablo 12: Araştırmaya katılan tıbbi ve idari birim çalışanlarına göre güvenlik uygulamaları boyutu	83
Tablo 13: Araştırmaya katılan tıbbi ve idari birim çalışanlarına göre erişim ve yetkilendirme boyutu	84
Tablo 14: Araştırmaya katılan tıbbi ve idari birim çalışanlarına göre bilgi güvenliğinde hizmet sunumu boyutu	85
Tablo 15: Araştırma grubunda bilgi güvenliği alt boyutlarına ait puan ortalamaları	86
Tablo 16: Araştırma grubunda bilgi güvenliği alt boyut puanları arasındaki ilişkiler	87
Tablo 17: Araştırma grubunda bilgi güvenliği alt boyutları ile yaş arasındaki ilişki	88
Tablo 18: Araştırma grubunda bilgi güvenliği alt boyutları ile çalışma süresi arasındaki ilişki	89
Tablo 19: Araştırma grubunda bilgi güvenliği alt boyutları ile eğitim durumu arasındaki ilişki	90
Tablo 20: Araştırma grubunda bilgi güvenliği alt boyutları ile HBYS eğitimi alma durumu arasındaki ilişki	91
Tablo 21: Tıbbi ve idari birimlerde bilgi güvenliği alt boyutları ile HBYS eğitimi alma arasındaki ilişki	92
Tablo 22: Bilgi güvenliği alt boyutları ile cinsiyet arasındaki ilişki	93

Tablo 23: Bilgi güvenliği alt boyutları ile kurumdaki kadro türleri arasındaki ilişkiler	94
Tablo 24: Bilgi güvenliği alt boyutları ile meslek grupları arasındaki ilişkiler	95
Tablo 25: Bilgi güvenliği alt boyutları ile yönetici ve diğer çalışanlar arasındaki ilişkiler	96

ŞEKİLLER LİSTESİ

Şekil 1: Bilgi sisteminin elemanları	26
Şekil 2: Yönetim bilgi sistemi modeli	30

KISALTMALAR LİSTESİ

AHBS	: Aile Hekimliği Bilgi Sistemi
ESKS	: Elektronik Sağlık Kayıt Sistemi
HBYS	: Hastane Bilgi Yönetim Sistemi
HIPAA	: Health Insurance Portability and Accountability
KBS	: Klinik Bilgi Sistemi
MSVS	: Minimum Sağlık Veri Setleri
PACS	: Picture Archival and Communication System
SKRS	: Sağlık Kodlama Referans Sunucusu
TSBS	: Türkiye Sağlık Bilgi Sistemi
USVS	: Ulusal Sağlık Veri Sözlüğü

EKLER LİSTESİ

Ek 1: Etik Kurul onay yazısı	121
Ek 2: Anket formu	122

HASTANE BİLGİ YÖNETİM SİSTEMİNİN BİLGİ GÜVENLİĞİ AÇISINDAN DEĞERLENDİRİLMESİ

Pınar Kılıç Aksu

Danışman: Prof. Dr. Gonca Mumcu

Hastane İşletmeciliği Anabilim Dalı

ÖZET

Bilgi güvenliği sağlık hizmetlerinde kritik bir önem taşımaktadır ve kullanıcılar da bilgi güvenliği sürecinde önemli rollere sahiptirler. Bu araştırmanın amacı, bilgi güvenliği perspektifinden hastane bilgi yönetimi sistemini (HBYS) incelemektir. Bu kesitsel araştırmaya bir hastaneden 424 çalışan katılmıştır. Veriler yüzyüze görüşme yapılarak bilgi güvenliği ölçeğini içeren bir anket formu ile toplanmıştır. Ölçekteki maddeler 5’li Likert skalası (1: kesinlikle katılmıyorum - 5: kesinlikle katılıyorum) ile değerlendirilmiştir. Ayrıca, kurumdaki bilgi güvenliği çalışanlar tarafından 100-mm görsel analog skala (0: çok kötü - 100: çok iyi) ile de değerlendirilmiştir. Faktör analizi sonrasında bilgi güvenliği ile ilişkili beş alt grup tanımlanmıştır. Bilgi güvenliği alt grubu puanlarının, HBYS eğitimi alanlarda almayanlara göre daha yüksek olduğu belirlenmiştir ($p<0.05$). Sağlık hizmeti sunumu alt grubu maddelerine ait puanlar, tıbbi birim çalışanlarında idari birim çalışanlarına göre daha düşüktür ($p<0.05$). Kurumdaki bilgi güvenliği puanının idari birimlerde ($65,01\pm23,52$) tıbbi birimlere ($58,69\pm16,77$) göre daha yüksek olduğu belirlenmiştir ($p=0.004$). Tıbbi ya da idari birim çalışanı olmak ve HBYS eğitimi almak, bilgi güvenliği ile ilişkili önemli faktörlerdir. 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.

Anahtar Sözcükler: Bilgi güvenliği, hastane bilgi yönetim sistemi, çalışanlar.

EVALUATION OF HOSPITAL INFORMATION MANAGEMENT SYSTEM IN THE FRAME OF INFORMATIN SECURITY

Pınar Kılıç Aksu

Supervisor: Prof. Dr. Gonca Mumcu

Department of Hospital Management

SUMMARY

Information security is a critical point in healthcare and users play an active role in the information security process. The aim of this study was to evaluate hospital information management system (HIMS) in the frame of information security. In this cross-sectional study, 424 staffs were included in a hospital. Data were collected by a questionnaire regarding information security scale by face-to-face interviews. Items in the questionnaire was coded by 5-point Likert scale (1: strongly disagree - 5: strongly agree). Moreover, self-reported information security score in the organizaiton was also evaluated by 100-mm visual analogue scale (0: very poor vs 100: very good). After factor analysis, information security related five subgroups were identified. Subgroup scores of information security were higher in staffs educated for HIMS compared to those in others ($p<0.05$). Scores of items in health service delivery subgroup were lower in medical staffs compared to those in administrative staffs ($p<0.05$). Self-reported information security score in HIMS was higher in administrative unit staffs ($65,01\pm23,52$) than that in medical unit staffs ($58,69\pm16,77$) ($p=0.004$). Being administrative or medical staffs and having education for HIMS are crucial factors in information security. Since information security is a critical issue in hospitals for all staffs, especially managers, information security policies are needed to develop and share for all staffs in organizations.

Key Words: Information security, hospital information management system, staffs.

1. GİRİŞ ve AMAÇ

Günümüzde bilgi güvenliği, bilginin elektronik ortamda depolanması ve iletilmesi ile birlikte, hem kişisel hem de kurumsal düzeyde giderek önem kazanan bir konudur. Elektronik uygulamalarda artış, ağ sistemlerinde bilginin paylaşımı, bilgiye birçok noktadan erişimin olması ve bilgi kaybına yönelik tehditlerdeki artışlar, bilgi güvenliğinin öneminin artmasında etkili olan faktörlerdir (17).

Bilgi güvenliği; bilgi bütünlüğünün korunması, bilgiyi kesintiye uğratan, değiştiren ve çalınmasına yol açan süreçlerin önlenmesi olarak tanımlanabilir. Bilgi güvenliği bir işletme içindeki bilginin korunması, işlenmesi ve iletilmesi sürecinin tamamını kapsar (66). Bilgi güvenliği süreci işletmenin genel varlıklarını korumak için tasarlanmış bir güvenlik politikası ile başlar (68). Güvenlik politikaları, işletmelerde kabul edilebilir güvenlik seviyelerinin tanımlanmasına yardımcı olan kurallar kümesidir. Bilgi güvenliği politikaları; her işletme için farklı olup, çalışanların yükümlülükleri, güvenlik kontrol araçlarının kullanımı ve sürecin yönetimine yönelik kurallar ve uygulamalara ilişkin genel beyanları içerir (71).

Bilginin yoğun olarak kullanıldığı işletmelerde, bilgi güvenliğine yönelik teknolojiler aktif şekilde kullanılmaktadır. İşletme yöneticilerinin, kendi iş akışları içinde bulunan bilginin değerini anlamaları ve bilgi güvenliğinin değerlendirilip uygulanmasına yönelik bir bakış açısına sahip olmaları gereklidir (68). Bilgi güvenliği alanında yapılan çok sayıdaki araştırma teknolojinin kullanımına odaklanmaktadır. Bununla birlikte, bilgi güvenliği bileşenlerinin insan, süreç ve teknolojiden oluştuğu da bilinmektedir (25). Bilgi güvenliğinin yönetilmesi sürecinde işletmeler, güvenlik kontrol araçlarını oluşturabilir, uygulama ilkelerini benimseyebilir ve güvenlik standartlarını oluşturabilir (68).

Tüm işletmelerde olduğu gibi sağlık alanında da bilgi güvenliğinin önemi her geçen gün daha da artmaktadır. Ülkemizde sağlık hizmetlerinin sunumunda bilginin elektronik ortama aktarıldığı, kurumlar ve sağlık çalışanları arasında paylaşımının olduğu bir süreç yaşanmaktadır. “Türkiye Sağlıkta Dönüşüm Programı” kapsamında (2003) sağlık hizmetlerinde sekiz ana başlık altında önemli değişimler yaşanmıştır.

Bu başlıklardan biri, bilgiye hızlı ve etkili erişimi sağlayan “Sağlık Bilgi Sistemi”’dir. Elektronik sağlık kayıt sisteminin bir parçası olan Aile Hekimliği Bilgi Sistemi’nin oluşturulması, Tele-Tıp projesinin uygulanması, doktor veri bankasının oluşturulması, klinik uygulamalarda uluslararası hastalık sınıflamasının kullanılması, farklı kurumlar arasında verilerin paylaşım ve entegrasyonunun sağlanması gibi bileşenlerin uyum içinde çalışabilmesi için, bir sağlık bilgi sistemine ihtiyaç duyulmuştur. Bu sistem sağlık çalışanları ve kurumlar arasında veri paylaşımını sağlarken, sağlık politikalarını geliştirenler ve karar vericiler için de analiz, raporlama ve istatistik desteğini de sağlamaktadır (54).

Hastane bilgi yönetimi sistemleri sağlıkta bilgisayar teknolojilerinin kullanımının bir örneğidir. Hastaneler birden fazla fonksiyonun bir arada yürütüldüğü kompleks yapılardır. Hastane bilgi yönetim sisteminin temel işlevleri; eksiksiz tıbbi kaydın tutulması, sağlık çalışanlarının iletişiminin artırılması, laboratuvar ve tıbbi görüntüleme verilerine hızlı erişimin sağlanması (11), finansal kayıtların tutulması, kaynakların uygun şekilde kullanılması, hizmet kalitesinin artırılması, hastane yönetiminin vereceği önemli kararlar için bilgi desteğinin sağlanması, uygun hedef ve stratejilerin belirlenmesinde rol alması olarak sıralanabilir. Bu açıdan hastane bilgi yönetim sistemleri yönetsel, tıbbi ve finansal olarak üç boyutta değerlendirilir (19)(28). Hastane bilgi yönetim sistemi aynı zamanda çalışanların iş süreçlerini de büyük ölçüde değiştiren (30) ve hasta güvenliğini artıran bir özelliğe de sahiptir (58).

Sağlık hizmetlerinde bilgisayar teknolojileri kullanılarak hasta verilerinin elektronik olarak kaydedilmesi, paylaşılması ve transferi sağlanır. Sağlık çalışanlarının sistemi kullanmaya yönelik direnci, teknik alt yapıda oluşan problemler ve finansal yetersizlikler, sistemin uygulanmasında karşılaşılan en temel sorunlardır (61). Sağlık Bakanlığı kamu hastanelerinde sağlık bilgi sistemleri için, yazılım ve donanım standartlarını belirlemiştir (44). Kompleks bir yapıya sahip olan hastanelerde bilgisayar teknolojilerinin kullanımı, sağlık hizmetinin kalitesini artırdığı gibi (62), çalışanların işbirliğini de sağlamaktadır (5). Elektronik sağlık kayıtları, hekim orderlarının elektronik ortama girişi, e-reçete, elektronik karar destek sistemleri gibi klinik bilgi teknolojileri, sağlık hizmetlerinin kalitesini

artırmaktadır. Yazılım geliřtiren firmalardan saęlık hizmetlerinin sunumu iin en etkili tasarımı hazırlamaları istenmektedir (12). Bununla birlikte bilgisayar kullanımı becerisi de sistemin bařarısı iin olduka nemlidir (44).

Bu noktada hastane bilgi ynetim sistemlerinin iřlevlerinin yerine getirilmesinde, bilgi gvenlięinin de korunması byk nem tařımaktadır. Gnmzde bilginin, gizlilik, btnlk ve eriřilebilirlik nitelikleri bakımından srekli olarak korunması gerekmektedir. Koruma birtakım fiziksel ve sistemsel nlemlerin yanında, bireylerin bilgi gvenlięine iliřkin tehdit ve risklerden haberdar olması, kurum bilgi ve gvenlik politikalarının alıřanlar tarafından biliniyor olması, olası risklerin mmkn olabilecek en dřk dzeyde nasıl tutulabileceęi konusunda alıřanların bilgilendirilmesi ile mmkn olabilir (27).

Bu arařtırmada, saęlık hizmetlerinin sunumunda yaygın olarak kullanılan hastane bilgi ynetim sisteminde bilgi gvenlięinin alıřanlar tarafından deęerlendirilmesi amalanmıřtır.

2. GENEL BİLGİLER

2.1. Türkiye Sağlıkta Dönüşüm Programı ve E-Sağlık Projesi

E-Sağlık; bilgi ve iletişim teknolojilerinin tüm fonksiyonlarının, hastaların iyileştirilmesi, sağlık hizmetlerine ulaşabilirliğin artırılması ve sağlık sektöründe yer alan tüm paydaşların kaliteli, verimli ve etkili hizmetleri sunması için kullanılmasıdır (<http://www.e-saglik.gov.tr/> , T.C. Sağlık Bakanlığı Sağlıkta E-Dönüşüm, Sağlıkta Dönüşüm Serisi-3, Ankara, 2007).

Ulusal sağlık bilgi sistemi alt yapısını oluşturmak üzere Sağlık Bakanlığı koordinasyonunda kamu kurumları, sivil toplum kuruluşları, üniversiteler ve özel sektörden temsilcilerin katılımı ile Türkiye Sağlık Bilgi Sistemi (TSBS) başlatılmıştır. TSBS çerçevesinde ulusal vizyon belirlenerek çalışma grupları oluşturulmuştur (<http://www.e-saglik.gov.tr/>, T.C. Sağlık Bakanlığı Sağlıkta e-Dönüşüm, Sağlıkta Dönüşüm Serisi-3, Ankara, 2007).

TSBS ile bilgi ve iletişim teknolojilerinin sağlık alanında etkin ve verimli bir şekilde kullanımının sağlanarak, erişim hakları tanımlanmış yetkili kişi ve kuruluşlarca ulaşılabilir, tüm vatandaşları kapsayan, her bireyin sağlık ile ilgili güncel ve doğru bilgiler ile kendi bilgilerine erişebildiği, tüm yaşam süresince oluşan sağlık ile ilgili verilerin bütün ülkeyi kapsayacak sağlık özel ağı üzerinden paylaşılması amaçlanmıştır (16).

E-Sağlık faaliyetleri çerçevesinde; elektronik sağlık hizmetlerinin ön gereksinimleri olan sağlık bilişim standartları belirlenerek uygulamaya geçilmiş, Sağlıkta Dönüşüm Programı çerçevesinde Aile Hekimliği için bilgi sistemi projesi tamamlanmış, sağlık kayıtlarının güvenlik, mahremiyet ve gizliliğini sağlamaya yönelik imza konusunda gerekli ihtiyaçlar belirlenmiştir (<http://www.e-saglik.gov.tr/>, T.C. Sağlık Bakanlığı Sağlıkta E-Dönüşüm, Sağlıkta Dönüşüm Serisi-3, Ankara, 2007). Geliştirilen Aile Hekimliği Bilgi Sistemi (AHBS) ile sağlık ile ilgili veriler birinci basamakta kayıt altına alınarak, TSBS'nin elektronik sağlık kayıtları alt bileşeninde bütünleştirilmesi planlanmıştır. TSBS ile tüm kayıtlar elektronik ortamda

tutulmaya başlanmıştır. Böylece veriye erişim hızlı ve etkin bir şekilde gerçekleştirilmekte, işletme yöneticilerinin yönetim faaliyetlerini daha etkili bir şekilde yürütülebilmeleri sağlanmaktadır (16).

2.1.1. Ulusal Sağlık Veri Sözlüğü ve Minimum Sağlık Veri Setleri

E-Sağlık uygulamalarında ulusal sağlık veri sözlüğü (USVS) ve Minimum Sağlık Veri Setleri (MSVS) önemli bileşenlerdir. USVS, veriyi üreten ve kullanan tarafların, aynı veriden aynı içeriği anlamalarını ve aynı amaçla kullanmalarını amaçlayan, standardizasyonu sağlayan ve gerekli tüm verilerin detaylı şekilde tanımlandığı bir yapıdır. Veri sözlüğünün temel amacı, sağlık alanındaki bütün paydaşların aynı kavramdan aynı içeriği anlamalarını sağlayacak bir terminoloji birliği oluşturmaktır. Veri sözlüğü, sağlık kurumlarından verilerin belirlenmiş standartlara uygun olarak toplanmasını, analizini ve değerlendirilmesini sağlayacaktır. Aynı zamanda, kurumlardan sağlık verisi toplama konusunda verimi artıracak, tekrarlanan ve hatalı verileri azaltacak ve toplanan verinin amacına daha uygun bir şekilde kullanılmasına olanak tanıyacaktır. MSVS, örneğin Çocuk İzlem Veri Seti, Gebe İzlem Veri Seti vb. şeklinde belirli bir hizmetin sunulması anında ortaya çıkan veri setlerini ifade edecek ve kullanılan bilgi sistemi tarafından açık bir teknoloji (XML Web Servisleri vb.) kullanılarak Sağlık Bakanlığı'na iletilecektir. Dolayısı ile şimdiye kadar kağıt ortamda sağlık kurumlarından İl Sağlık Müdürlükleri'ne, oradan da Sağlık Bakanlığı'na iletilen ve analiz edilmesinde ciddi sorunlar yaşanan bu veriler, artık doğrudan üretildikleri yerde kayıt altına alınarak, elektronik ortamda bakanlığa iletilecektir (<http://www.saglik.gov.tr/TR/dosya/1-53240/h/saglik-netentegr>, T.C. Sağlık Bakanlığı Bilgi İşlem Daire Başkanlığı, Sağlık-Net Entegrasyonu İçin Hastane Bilgi Sistemlerinin Temel Gereksinimleri, Ankara, 2007).

Bu kapsamda MSVS, Sağlık Bakanlığı'nın kurumlardan toplayacağı minimum içeriğe sahip veri gruplarını ifade etmektedir. MSVS sağlık konusunda referans bir sözlük niteliği taşımaktadır. USVS içerisinde, farklı seviyelerdeki sağlık hizmetlerinin verildiği kurumlarda kullanılacak veri elemanları tanımlanacağından, ihtiyaç duyulduğunda aynı standartlara uyarak kayıt altına alınan veriler, setler halinde ilgili kurumlardan talep edilebilecektir. Hastane bilgi yönetim sistemleri, veri

setleri içinde yer alan veri elemanlarına göre veri tabanlarını güncelleyecek ve Sağlık Bakanlığı veri tabanı ile haberleşebilecek bir yapıya ulaşılabacaktır. MSVS içerisinde yer alan verilerin tamamı, USVS içerisinde tanımlanmaktadır

(<http://www.saglik.gov.tr/TR/dosya/1-53240/h/saglik-netentegr>, T.C. Sağlık Bakanlığı Bilgi İşlem Daire Başkanlığı, Sağlık-Net Entegrasyonu İçin Hastane Bilgi Sistemlerinin Temel Gereksinimleri, Ankara, 2007).

Sonuç olarak, USVS içerisinde tanımı ve formatı belirlenen veriler, sağlık kurumlarında kullanılmakta olan bilgi sistemleri için referans teşkil etmektedir. Böylece, sağlık kurumlarında farklı uygulamalar kullanılsa bile, üretilen veriler aynı formatta olacaktır. Bu sayede, USVS içerisinde tanımlanan veriler arasından seçilerek oluşturulacak olan MSVS, ilgili kurumlardan talep edildiğinde, her kurumun bu verileri tedarik edebilmesi mümkün olacaktır. USVS ve MSVS'nin kullanılması ile bakanlığın ihtiyaç duyduğu bilgileri standart olarak bir veri havuzunda toplaması mümkün hale gelmekte ve sağlık politikalarının belirlenmesi için teknik yöntemler kullanılabilir (http://www.saglik.gov.tr/TR/dosya/1-53240/h/saglik-netentegr, T.C. Sağlık Bakanlığı Bilgi İşlem Daire Başkanlığı, Sağlık-Net Entegrasyonu İçin Hastane Bilgi Sistemlerinin Temel Gereksinimleri, Ankara, 2007).

2.1.2. Sağlık Kodlama Referans Sunucusu

Sağlık alanında toplanacak verilerden, kodlanması ihtiyaç duyulan veriler, Sağlık Kodlama Referans Sunucusu (SKRS) olarak isimlendirilen bir sistemde bir araya getirilmektedir. Bu sistem ile sağlık sisteminin izlenebilir, ölçülebilir ve daha kolay yönetilebilir bir yapıya kavuşturulması için ihtiyaç duyulan, kodlama ve sınıflama sistemleri bir araya getirilmektedir. SKRS geliştirilecek olan standartları da bünyesine dâhil ederek ve bu standartları ilgili tüm kullanıcıların kolay erişebilmesi için açık teknoloji standartları ile paylaşan bir referans sunucu olacaktır. (http://www.saglik.gov.tr/TR/dosya/1-53240/h/saglik-netentegr, T.C. Sağlık Bakanlığı Bilgi İşlem Daire Başkanlığı, Sağlık-Net Entegrasyonu İçin Hastane Bilgi Sistemlerinin Temel Gereksinimleri, Ankara, 2007).

Sağlık Bakanlığı bünyesinde tutulan kodlama ve sınıflama sistemlerini barındırmayı ve paylaşımına açmayı amaçlayan SKRS; Tanı Sınıflama Sistemi (ICD-10) , İlaç Kodları, İlaç Sınıfları Kodlama Sistemi, Bütçe Uygulama Talimatı Kodları, Klinik Kodları, Branş Kodları, Sağlık Kurumu Kodları, Meslek Grupları Listesi, Bebek İzlem Takvimi, Gebe İzlem Takvimi, Çocuk İzlem Takvimi, Persentil Değerleri Listesi, Aşı Listesi, Aşı Takvimi, Olası Tanı Kriterleri, Enfeksiyon Etkenleri Tanı Kriterleri, Tümör Yerleri, Kesin Tanı Kriterleri, Histoloji Kodları, Adres Kodları, Parametreler sistemlerini kapsamaktadır (<http://www.saglik.gov.tr/TR/dosya/1-53240/h/saglik-netentegr,T.C.Sağlık Bakanlığı Bilgi İşlem Daire Başkanlığı, Sağlık-Net Entegrasyonu İçin Hastane Bilgi Sistemlerinin Temel Gereksinimleri, Ankara, 2007>).

2.1.3. Aile Hekimliği Bilgi Sistemi ve E-Sağlık

Birinci basamak sağlık hizmetlerinin temelini oluşturan AHBS ile aile hekimlerinin yaptıkları işlemlere ait veriler, bakanlığa elektronik ortamda güvenli bir şekilde iletelebilmektedir. Bu sistem ile bireylere ait sağlık verileri MSVS şeklinde bakanlığa gönderilerek, ihtiyaç duyulduğunda hastanın da izni ile başka doktor tarafından da bu verilere erişilmesine olanak tanımaktadır. Böylece AHBS, etkili hizmet sunumuna ve hizmet kalitesine doğrudan katkıda bulunmaktadır. Ayrıca verilerin otomatik olarak gönderilmesi sağlanarak, asli görevi sağlık hizmeti vermek olan sağlık çalışanlarının, rapor ve bilgi formu hazırlama gibi idari işleri hafifletilerek verimlilik artırılmış olacaktır. Aile hekimi ilgilendiği bireylerin bilgilerini AHBS'ne girerek kaydetmektedir. Dolayısı ile bir sonraki görüşmelerinde, kişinin anamnezi ve kendisine hangi tedavilerin uygulandığı tespit edilebilecektir (<http://www.e-saglik.gov.tr/>, T.C. Sağlık Bakanlığı Sağlıkta E-Dönüşüm, Sağlıkta Dönüşüm Serisi-3, Ankara, 2007).

2.1.4. Elektronik sađlık kayıt sistemi

Hastaların tüm yaşamları boyunca sađlık kayıtlarının oluşturulması, geliştirilmesi ve/veya kalitesinin artırılması, sađlık hizmetlerinin iyileştirilmesi çalışmalarına katkıda bulunabilecek temel konulardan biridir. Sađlık hizmeti sunan çalışanların, sađlık bakımı için gereksinim duyacağı verilere daha iyi ve daha hızlı bir şekilde ulaşım (anında ve uzaktan erişim), daha iyi kalitede veriler ve verileri çok yönlü olarak sunma olanakları sağlamaktadır. Elektronik sađlık kayıt sistemi (ESKS), güvenliği sağlanabilen, kolay okunabilir ve gerektiğinde birleştirilebilir ve sađlık bakımının sonuçlarının ölçülebilmesi için gerekli olan klinik verilere elektronik olarak ulaşılmasını sağlamaktadır. Maliyetleri düşürerek ve personelin verimliliğini artırarak sađlık kurumlarının etkililiğini artırmaktadır (63).

Hastalara ait anamnez, fizik muayene sonuçları, konsültasyonlar, orderlar, laboratuvar ve görüntüleme istekleri ile bunların sonuçları, tedavi protokolleri ve ilaç uygulamalarına ait tüm bilgiler, ESKS içinde yer alır. Verinin güvenli ortamda saklanması ve uygun koşullarda veri değişiminin yapılabilmesi de sistemin diğer özelliklerindendir. ESKS'nin temel fonksiyonları; standart kod sistemleri kullanarak hasta verilerinin entegrasyonunun sağlanması, klinik karar destek sistemlerinin hekim order girişinin değişik tıbbi bilgi kaynaklarına ulaşımın sağlanması, sađlık çalışanları arasında iletişimin geliştirilmesi ve uygun bakımı için bilgi kaynaklarına ulaşımın sağlanması olarak tanımlanabilir. Standart dil ve kod sisteminin kullanılması bölgesel ve ulusal düzeyde bilgi bütünlüğünün temelidir. Bu açıdan bireyin yaşam boyu sađlık durumunu yansıtan E-sađlık sistemi, herhangi bir muayenehane ve hastanedeki tıbbi kayıtlardan farklı bir yapıdadır (63).

Elektronik sađlık kaydına gereksinim duyulma nedenleri

- Hizmetin kalitesi ve hasta güvenliği
- Kağıda dayalı formlardaki sorunlar
- Etkinlik ve üretimin geliştirilmesindeki gereksinimler
- Finansal tasarruf
- Teknolojik avantajlar
- Toplumsal beklentiler

- Hükümetin beklentileri
- Yaşlı/ komplike olan hastalar için iyi koordine edilen bakım gereksinimi (44).

ESKS'nin fonksiyonel yapıları

Bu sistemin kullanımındaki fonksiyonel yapılar aşağıdaki şekilde sınıflandırılabilir:

- Klinik karar destek sistemleri hatırlatma ve klinik uygulamalar için rehberleri içermelidir.
- Hasta ile çalışanlar ve çalışanların kendi arasındaki iletişimde güvenlik mesajı olmalıdır.
- Randevu yazılımı ve hasta portalı birbirleri ile ilişkili olmalıdır.
- Elektronik olarak laboratuvar sonuçları ve görüntüleme sonuçlarına ulaşım yapılabilmelidir.
- Hekim orderlarının bilgisayar ortamına girişi sağlanmalıdır.
- Hastalara ait bilgilerin saklandığı hastaya özel bir hesap olmalı, son tedaviler, uygulanan ilaçlar, yapılan uygulamalar izlenebilir. Bilgiye ulaşma ya da bilgi girişinde bireysel dijital yardımcı (Personal Digital Assistant – PDA) ya da bilgisayar kullanılmalı, kurum içinden ya da evden ulaşım olanağı olmalıdır.
- Elektronik reçeteleme olmalıdır.
- Görüntü arşivleme ve iletişim sistemleri ile (Picture Archival and Communication System - PACS) entegrasyonu sağlanmalıdır.
- Halk sağlığı uygulamalarının raporlanması ve izlemi sağlanmalıdır.
- Kişiyi özel sağlık sorunlarının listesi görülebilmelidir (alerjiler, tanılar, girişimler ve ilaçlar).
- Yazılı metinler taranarak elektronik ortama alınabilmeli, optik okuyucular kullanılabilir.
- Kodlama sistemi uygun şekilde değerlendirilmelidir.
- Laboratuvar sonuçları grafikler halinde görülebilmelidir.
- Tanı konan hastalıkların listesi eklenebilir.
- Klinik uygulama rehberleri ile ilişkili koruyucu ilaç izlemeleri yapılabilir.

- Health Insurance Portability and Accountability (HIPAA) standartları ile uyumlu güvenlik olmalıdır.
- Yedekleme sistemleri olmalıdır.
- Web tabanlı uygulamalar ya da server desteği olmalıdır (44).

ESKS'nin adaptasyonundaki engeller

Hekimin direnci: Yeni teknolojiler ileriye dönük olarak maliyetlerin azalmasını, zamandan tasarrufu ve hizmetin hasta açısından daha iyi olmasını sağlayabilir. Sisteme adaptasyon özellikle hekimler için zor olabilir. Bu neden ile adaptasyon sırasında daha fazla zaman harcanabilir. Bunun yanı sıra sisteme adaptasyonda, hekimlerin uzmanlık alanlarına göre farklılıkların olabileceği de gözlenmiştir (44)(35).

Fiziksel engeller: Sistemin kurulum ve uygulama maliyetleri yüksektir (70).

Verimin azalması: Hekimlerin sistem eğitimi ve adaptasyon sürecinden dolayı, çalışma saatlerindeki verimlilikleri azalabilir (44)(10).

İş akışındaki değişiklikler: Kağıda dayalı eski sistemler ile yapılan karşılaştırmalarda, bilginin akış yollarında değişiklik olduğu görülmektedir. İyi bir planlama ile iş akışının nasıl değişeceği kolaylıkla belirlenebilmektedir. İş akışı ile ilgili olarak bilgisayar terminallerinin yerleşimi de uygun şekilde ayarlanmalıdır. Önemli bir unsur da hasta muayenesi sırasında hekimin, ESKS'ni kullanırken hastası ile de göz kontağını kurabilmesidir (32)(44).

Diğer sistemler ile entegrasyonu: Eski sistemlerin çoğunun birbirleri ile iletişim yoktur. Sistemler farklı firmalar tarafından yazılır ve geliştirilir (44).

Standartların eksikliği: Elektronik sağlık kayıtları sistemlerinin birbirleri ile ilişki kurabilmeleri için 2006 yılında Certification Commission for Healthcare Information Technology sertifikasyon işlemi geliştirilmiştir (44).

Elektronik sağlık kayıt sisteminin kullanılmasında hekimin iş yükü, sistemin uygulamasında önemli faktörlerden biridir. Bu teknolojinin kullanımı için motivasyonu artırmak ve sistemin avantajlarını çok iyi anlamak ve anlatmak gerekir.

Sağlık hizmeti sunumunda farklı tedavi birimleri birlikte çalışmak zorundadırlar. Bu tür uygulamaların başarısında, iletişim anahtar rol oynar ve sistemin gerekli desteği sağlaması etkinliği artırır. Elektronik sağlık kayıt sistemleri; zamana (kronolojik kayıtlar), probleme (klinik durum) ve kaynağa (muayene notları, radyoloji raporlarına, laboratuvar testleri) odaklı olarak hizmet verebilmektedir. ESKS’nde bireysel sağlık kayıtlarının doğru alınması, standartların, kodların uygun şekilde seçimi ve entegrasyonun sağlanması, veri güvenliğinin geliştirilmesi ve bilgi yönetiminin sağlanması önemli noktalardır. İleride genetik bilgi kayıtlarının da bu sistemin bir parçası olup sistemin etkinliğini artıracakı düşünülmektedir (44)(35).

Bilişimde yaşanan gelişmeler birçok sektörü, sunduğu hizmetleri teknolojik gelişmeler ile birleştirmeye yönlendirmiş ve kademeli olarak bütünleştirilen sistemler erişim, kapsam, kalite, hız vb. açılardan geçmişe oranla daha etkili bir duruma gelmiştir. Sağlık sektörü de bilişim alanında gerçekleşen bu yenilikler ve gelişmelerden önemli ölçüde etkilenmiş ve etkilenmeye devam etmektedir (44).

2.1.5. Tele-tıp ve telekomünikasyon

Tele-tıp; uzaklığın problem olduğu durumlarda sağlık hizmetinin sunulabilmesi için, elektronik bilgi ve iletişim teknolojilerinin kullanımı olarak tanımlamaktadır (48).

Amerika Tele-tıp Derneği, teletıp kavramını, “hasta tedavisi, hasta ve sağlık personelinin eğitimi, sağlık hizmetlerinin geliştirilmesi amacı ile iki bölge arasında, elektronik iletişim araçları ile tıbbi bilgi alışverişi” olarak tanımlamaktadır (31).

Tele-tıp sayesinde bilgiye istenildiği anda hemen ulaşmak mümkün olmaktadır. Tele-tıp ile hasta ve hekimler için ulaşım zamanı azalacağı gibi, tıbbi kayıtlarda kağıt kullanımının azalması, iyileşme zamanının kısalması, gereksiz ilaç kullanımının azalması ve hasta ve hastane masraflarının azaltılması yolu ile tasarruf sağlanabilmektedir (34).

Tele-tıp kullanım alanları

Tanı ve tedavi: Bir hastanın tanısının konması sırasında zorlanıldığı durumlarda ya da özel uzmanlık isteyen tetkiklerin değerlendirilmesi için, hasta bilgilerinin uzakta bulunan merkezlere ya da uzmanlara gönderilmesi ile tanı konulabilir ve tedavi düzenlenebilir. Tele-tıp uzman bir kişi ya da merkezin yardımı ile tedavinin düzenlenmesi için hasta ya da sağlık profesyoneline önerilerde bulunulmasında (tele-konsültasyon) kullanılmaktadır (53).

Uzaktan hasta izlemi ve hasta kontrolü: En önemli uygulama alanlarından biri; özellikle, diyabet, astım gibi kronik hastalıklarda hastanın evden izlenmesinde kullanımdır (53).

Araştırma: Veri tabanlarına erişimin kolaylaşması sonucunda birçok veri tabanına ulaşılarak kapsamlı araştırmalar yapılabilmektedir (53).

Eğitim: Teknolojik gelişmeler sayesinde uzak bir mesafede olan sağlık çalışanı, yerinden ayrılmadan eğitim ihtiyacını karşılayabilmektedir. Bu eğitim yalnızca sağlık çalışanlarının kendi içinde değil, aynı zamanda sağlık çalışanı ve hasta arasında da olabilmektedir (53).

Sağlık yönetimi: Tıp ve sağlık ile ilgili veriler merkezi birimlerdeki yöneticilerin ulaşabileceği hale getirilir. Bu bilgilerin değerlendirilmesi kalite kontrol ve karar verme mekanizmaları için destek olacaktır (53).

Halk sağlığı eğitimi: Özellikle internette veri tabanları oluşturularak gerek hekim gerekse toplumun bilgilendirilmesi mümkün olabilmektedir (34). Halk sağlığında verilerin toplanması, değerlendirmesi ve planlamaların hızla yapılabilmesi sırasında ağ temelli teknolojiler kullanılmaktadır (6).

Doğal afet ve büyük kazalarda hastaların değerlendirilmesi: Doğal afetlerin ve büyük kazaların yaşandığı durumlarda, iletişim araçlarının kullanılması ile hastaların değerlendirilmesi ve durumun incelenmesi ile o bölgede yaşayanlar bilgilendirilebilir (31).

Tutuklulara hizmet sunma: Cezaevlerinde bulunan tutuklu ve hükümlülerin, hastalanmaları durumunda bir sağlık kurumuna ulaştırılmaları ve gözetim altında tutulmaları oldukça maliyetlidir. Tutuklu ve hükümlülerin cezaevlerinde sağlık hizmetlerinden yararlanması için, tele-tıp kullanılmaktadır (31).

Tele-tıp çeşitleri

Tele-tıp kullanıldığı alana göre isim almaktadır. Yaygın olarak kullanılmakta olan tele-tıp çeşitlerinden bazıları şunlardır:

Tele-radyoloji: Hastalara ait radyoloji görüntülerinin başka bir kuruma gönderilerek karşı taraftan görüş alınması şeklinde uygulanır (34).

Tele-kardiyoloji: EKG sinyalleri ya da kalp atış sesleri, kalp pillerinin izlenmesi, gibi konularda yaygın olarak kullanılmaktadır (67).

Tele-psikiyatri: Uzmanlar arasında video konferans ve hasta hekim arasında görüntü ve ses aktarımı şeklinde uzun yıllardır kullanılmaktadır (34).

Tele-cerrahi: Fiziksel olarak hastanın yanında olmadan uzak yerlerden ameliyat yapabilme olanağı sağlar. Bu çalışmanın olabilmesi için cerrahi cihaz robotları yüksek hızlı, güvenilir iletişim ağlarına entegre edilmiş olmalıdır. Cerrah uzaktan kontrol ettiği bir robot yolu ile hastaya temas etmeden ameliyat gerçekleştirebilmektedir (48).

Tele-izlem: Veri depolama sistemleri sayesinde, video görüntülerinin ve hasta ile ilgili formların, elektronik posta kullanılarak internet aracılığı ile aktarımını içerir. Tele-izlem çalışmaları eş zamanlı yapabildiği gibi, farklı zamanlarda da yapabilmektedir (67).

Tele-patoloji: Patoloji uzmanları, uzak bir merkezdeki mikroskobu kontrol edebilirler ya da çeşitli patoloji materyallerinin görüntüleri, başka bir merkeze gönderilip görüş alınması sağlanabilir (34).

3. BİLGİ SİSTEMLERİ VE BİLGİ GÜVENLİĞİ

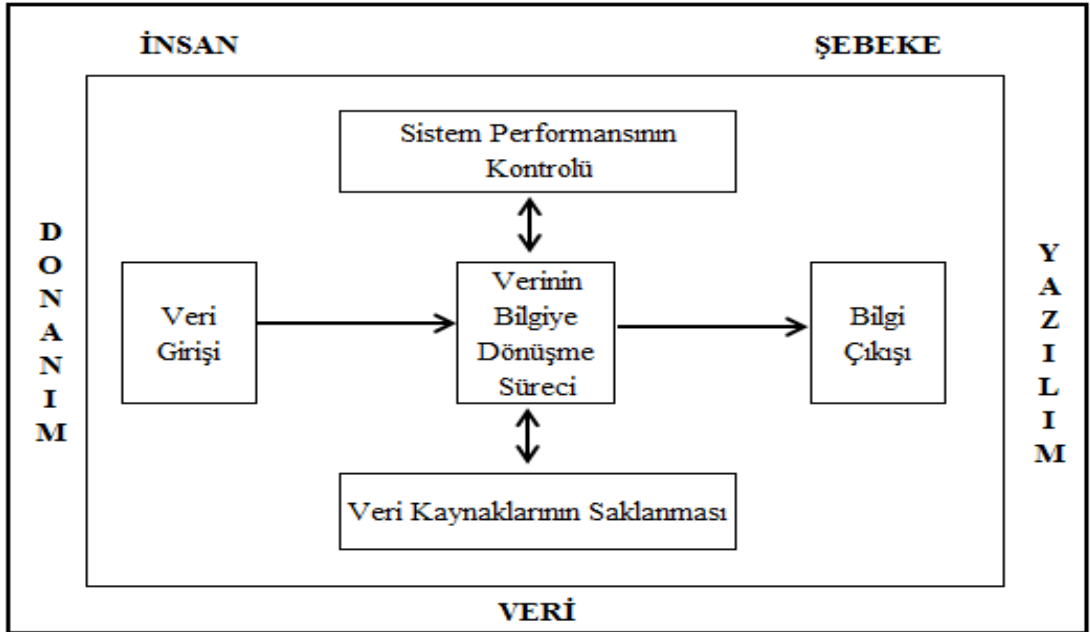
3.1. Bilgi Sistemleri

Bilgi

Bilgi, organizasyonların oluşumu için gereken teşebbüs, sermaye, toprak ve işgücüne ek olarak beşinci temel öğedir. Günümüzün değişen koşulları içinde, varlığını, önceden belirlediği amaçlar doğrultusunda sürdürmek isteyen her işletme için, içeriden ve dışarıdan gelen çeşitli bilgiler, temel yönetim fonksiyonlarının (planlama, örgütleme, yöneltme, koordinasyon, denetleme) başarı ile yerine getirilmesinde en önemli kaynaktır (31).

Bilgi sistemi

Bilgi sistemi, veri kaynaklarını girdi olarak alıp belirli bir süreçten geçiren ve çıktı olarak bilgi ürünlerini ortaya çıkaran bir sistemdir. Bilgi sistemi veriyi bilgiye dönüştürmek için girdi, süreç, çıktı, saklama ve kontrol faaliyetlerini yerine getirirken kaynak olarak insanı, donanımı, yazılımı, şebekeyi ve veriyi kullanır (31).



Şekil 3.1. Bilgi sisteminin elemanları

Kaynak: Kavuncubaşı Ş. Hastane ve Sağlık Kurumları Yönetimi, Siyasal Kitabevi, 2000.

Donanım, bilgi sürecinde kullanılan tüm fiziksel araç ve malzemeleri kapsamaktadır. Yalnızca bilgisayar, hesap makinesi gibi makineleri değil, verilerin kaydedildiği kağıtlardan manyetik disklerle kadar olan veri ortamlarını kapsar. Yazılım, bütün bilgi işleme komutları kümesini 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 (31).

Veri kavramı, bilgi sistemlerinin ham maddesi olmaktan daha fazla bir anlam taşımaktadır. Veri, rakam, harf ve diğer özel şekillerden oluşarak alfa-sayısal olabileceği gibi cümle ve paragraflardan oluşan metin ve resim de olabilir. Bilgi sistemlerinde genellikle veri, işlenmiş ve organize edilmiş şekilde veri tabanlarında bulunmaktadır. Bu sayede istenildiği zaman tüm bilgilere rahatlıkla ulaşmak mümkündür (29).

Bilgi sistemleri kurulduğu sistemin doğal bir alt sistemidir. İçinde bulunduğu organizasyonun amaçlarına ulaşmasına yardımcı olacak her türlü veriyi (girdi) toplar, bu verileri işleyip ve anlam kazandırır (süreç) ve yine ürettiği bilgiyi (çıkıtı) üst sisteme sunar (29).

Bilgi sistemleri ilk bakışta sadece yazılım ve donanımdan meydana gelmiş gibi düşünülse de çok önemli bir bileşeni insan tarafıdır. Bilgi sistemleri, bu üç bileşenin üç köşesini oluşturduğu bir üçgen üzerinde kurulmuştur denilebilir. Bu üçgendeki donanım (girdi ve çıkıtı) ve yazılım (süreç) en önem verilen bileşenlerdir. Bu iki bileşen tek başına bilişime ait kavramlardır ve sistem döngüsü çalışan bileşeni kullanılmadan geri bildirim ile sonlandırılırsa, bu bilişime ait bir sistem olur. Bilgi sistemi ise insan boyutunun da sisteme entegre edilmesi ile anlam kazanır (70). Bilgi sistemini oluşturan süreçte, toplanan veriler anlamlandırılarak kullanılabilir bilgi haline getirilir (44).

Faaliyet alanı ve amaçları ne olursa olsun yeni bilgi sistemleri, organizasyonel problem çözme sürecinin bir sonucudur. Yeni bir bilgi sistemi örgütün karşılaştığı problemlerin türüne çözüm olarak geliştirilir. Problem, yönetici

ve çalışanların, organizasyonun beklenen performansı göstermediğini fark ettiklerinde ortaya çıkabilir ya da yeni fırsatları elde etmesi gerektiğini düşündükleri zaman oluşabilir. Sistem geliştirme, örgütsel bir problemi çözmek ya da organizasyon ile ilgili fırsat elde edebilmek için, bir bilgi sistemi ile çözüm üreten faaliyetlerdir (60).

3.1.1. Bilgi sistemlerinin sınıflandırılması

Bilgi teknolojilerinin gelişimine bağlı olarak gelişme gösteren işletme bilgi sistemlerini 5 grupta toplamak mümkündür (29)(41):

- Veri işleme sistemleri
- Ofis otomasyon sistemleri
- Karar destek sistemleri
- Yönetim bilgi sistemleri
- Üst yönetim bilgi sistemleridir.

Veri işleme sistemleri

Organizasyonların temel sistemlerinden biri olan veri işleme sistemleri, işletmenin yürütmesi gereken günlük ve rutin işlemleri kaydeden, işleyen, güncelleştiren bilgisayarlı sistemlerdir. Genellikle çalışanlar tarafından verilerin girilmesi ve güncellenmesi için kullanılan sistemdir (29).

Ofis otomasyon sistemleri

Bir ofiste çalışanların verinin verimliliğini artırmak amacı ile tasarlanmış olan kelime işlemci, elektronik posta, elektronik takvim, randevu, program ve planlama sistemi gibi unsurlardan oluşan sistemlerdir (29).

Organizasyonlarda iletişimin sağlanmasını ve bilginin paylaşılmasını sağlayarak faaliyetlere etkinlik, verimlilik ve hız sağlayan bir sistemdir. İşletmede telefon, faks, elektronik posta, intranet uygulamaları ve video konferans uygulamaları, ofis otomasyon sisteminin birkaç unsurunu oluşturmaktadır. Kelime işlem sistemleri, tablolar ve hesaplama sistemleri, masaüstü yayıncılık ve doküman görüntüleme sistemleri de ofis otomasyon sisteminin diğer unsurlarıdır (41).

Karar destek sistemleri

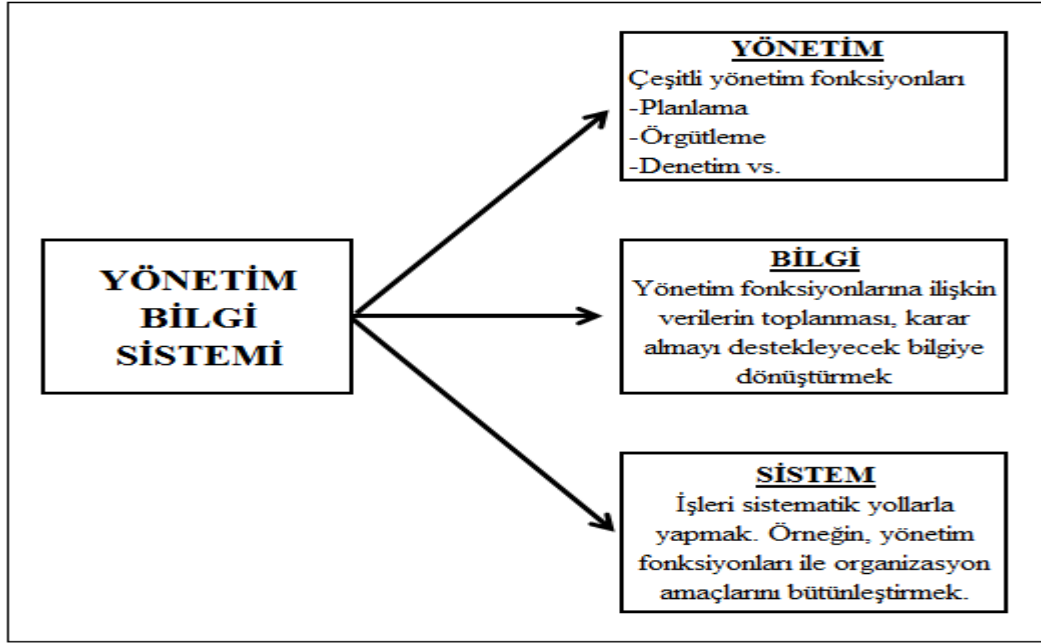
Karar destek sistemleri, hem klinik uygulamalar hem de ynetimsel amalı olarak kullanılmaktadır. Organizasyonun ynetim dzeyine hizmet sunan, ileri dzeyde kolaylıkla tanımlanamayan, abuk deęiřen, yapısal ve yarı yapısal nitelikteki kararların verilmesinde yneticilere destek veren sistemlerdir. İřletme yneticilerinin bu kararları vermesinde, onlara yardımcı olmak iin eřitli model ve araları, veri tabanı aracılığı ile kullanıma sunar. Yneticiler bu sistemlerden, karmařık, stratejik ve nadiren karřılařılan durumlar iin kararların verilmesinde yararlanır (44)(29).

Ynetim bilgi sistemleri

Ynetim bilgi sistemleri, organizasyonun gncel performansı ve eski kayıtlarına eř zamanlı ulařarak, bazı rnekleri ve raporları yneticilere saęlayarak, organizasyonun orta dzey ynetimine destek saęlar.

Ynetim bilgi sistemi; zellikle, planlama, denetleme ve dzeltici nleyici faaliyetlerde bulunabilmek iin geliřtirilmiř ve pazarlama, muhasebe, finans ve insan kaynakları gibi organizasyonun iřlevlerine ait bilgileri eřitli aralar aracılığı ile yneticilere sunan bir sistemdir (29).

Ynetim bilgi sistemleri, “Ynetim, Bilgi, Sistem” kavramlarından oluřmakta olup, ynetim ve bilginin birlikte irdelenerek bir sistem iinde btnleřtirilmesi dřncesine dayanmaktadır. İřletme ynetimi iin gerekli olan anlamlı i ve dıř bilgilerin saęlanması, byle bir dřnceden kaynaklanan bilgi sistemlerinin geliřtirilmesi ve kullanılması ile olabilir (29).



Şekil 3.2. Yönetim bilgi sistemi modeli

Kaynak: Kavuncubaşı Ş. Hastane ve Sağlık Kurumları Yönetimi, Siyasal Kitabevi, 2000.

Yönetim bilgi sistemi, organizasyonun faaliyetlerini daha etkin ve yeterli bir biçimde planlamak, yürütmek ve denetlemek için yöneticiye gerekli tüm bilgiyi zamanında, doğru ve eksiksiz olarak sağlayan ve insan, kaynaklar, bilgisayar donanımı ve yazılımından oluşan sistemdir. Sistemin temel amacı, organizasyon içinden ve organizasyon çevresinden elde edilen bilgiyi toplamak, depolamak ve yaymaktır (29).

Üst yönetim bilgi sistemleri

Üst düzey (tepe) yöneticilerin karar vermek amacı ile kullandıkları bilgi sistemidir. Organizasyonun stratejik düzeyine hizmet sunan bu sistem, başta genel müdür ve yönetim kurulu üyeleri olmak üzere, işletmenin misyonunu, vizyonunu, değerlerini ve stratejilerini belirleyen kişiler için oluşturulmaktadır. Yapılacak hataların işletmenin geleceğini riske sokabileceği düşünülürse, üst yönetim bilgi sistemi iç ve dış çevre koşulları konusunda eksiksiz, doğru ve zamanında bilgilendirme yapmalıdır. Üst yönetim bilgi sistemleri, karmaşık, önceden programlanamayan, nadiren karşılaşılan ve üst düzey yöneticiler tarafından verilen stratejik kararlar için kullanılan bilgi sistemleridir (41).

3.2. Bilgi Yönetimi

Bilgi sistemini oluşturan süreçte verinin bilgiye dönüşümü sağlandıktan sonra, geri bildirimler ile birlikte oluşan bilgi, tüm süreçlerin yönetiminde kullanılır. Bu durumda da bilginin yönetilmesi kavramı ortaya çıkar (4).

Bilgi yönetimi; organizasyonel hedeflere ulaşmak üzere, en iyi uygulamaları gerçekleştirme, en doğru kararları verme gibi organizasyonun tüm faaliyetlerinde, bilgiyi gereken zamanda ve gereken yerde kullanıma sunan, bilgi tanımlama, yaratma, paylaşma, depolama ve kullanma faaliyetlerini organize eden bir süreç şeklinde tanımlanabilir (4).

Bilgi yönetimi, doğru kararlar verebilmek için doğru zamanda, doğru kişiler ile paylaşılan bilginin sağlanmasına yardım eder. Bilgi yönetimi, bilginin toplanması, oluşturulması, kullanılması ve paylaşılmasına olanak tanıyan, insanları, süreçleri, faaliyetleri ve teknolojiyi kapsayan ve organizasyonel hedeflere ulaşmak için bilginin yaratılma, dağıtılma ve kullanım yönetimini kapsayan süreç ile ilgilidir (4).

Daha kısa bir tanımla bilgi yönetimi; bilgiyi yaratmak, elde tutmak, paylaşmak ve uygun iş sürecini geliştirmek olarak tanımlanır. Bilginin organizasyon içinde hızla dağılmasını ve paylaşılmasını sağlar, verimsizliği ve zaman kaybını önler, bilginin işletme stratejileri ile ilişkilendirmesini, yönetilmesini, iş birliği koşullarının belirlenmesini amaçlar. Organizasyon hedeflerine ulaşmak üzere sürekli değişim ve hareket halinde olan, bilinçli ya da bilinçsiz olarak oluşan bilgiler, temel bilgi yönetim faaliyetleri aracılığı ile etkin bir şekilde kullanıma sokulmaktadır (62).

3.2.1. Bilgi yönetimi faaliyetleri

Bilginin tanımlanması: İşletme içinde temel bilgi ihtiyaçları, bilginin yapısı, bilginin görsel sunumu ve bilginin nasıl karşılanacağını tanımlanmasının yanı sıra, bireylerin uzmanlık alanlarının da tanımlanması, bilgi tanımlama sürecidir. Organizasyonda mevcut olan, kayıtlı ya da potansiyel bilgi kaynaklarının ortaya çıkarılarak, çalışanların bilgilere erişiminin kolaylaştırılması ve iş süreçlerine dahil edilmesi, bilginin tanımlanması ile mümkün olabilir. Mevcut bilginin tanımlanması, karar vermeyi desteklemek için zorunludur (4).

Bilginin yaratılması: Bilgi yaratma faaliyeti, bir organizasyonun yeni fikirler yaratıp, çözüm yolları geliştirme yeteneği ile ilgilidir. Bilginin yaratılması, araştırmalardan elde edilen çıktılar, belirli faktörler arasındaki yeni ilişkilerin tespit edilmesi, bir vaka çalışması ya da girişimin ilkelerinin ortaya konulması şeklinde gerçekleşebilir. Ayrıca önemli bir araştırma süreci aracılığı ile belirli sağlık alanlarındaki tecrübeler, araştırma bulgularının sentezi ile ya da bazı sağlık kurumlarındaki tercihler, organizasyonel biçimler ve uygulama normlarını yansıtan sağlık programları ya da hizmetlerinin, belirli klinik vakalar ile ilgili tecrübelerin toplanması yolu ile de bilgi yaratılabilir (4).

Bilginin depolanması: Bilginin depolanması, bilginin türüne, kullanım amacına ve organizasyonun hedeflerine uygun olarak ayrılması ve çalışanların şimdi ve gelecekte erişimine fırsat verecek biçimde saklanmasıdır. Bu faaliyet bilginin değerlendirilmesi açısından önemli olduğu kadar, tekrar kullanılabilmesi açısından da gereklidir (4).

Bilginin paylaşılması: Bilgi yönetiminde bilgi paylaşımı, belirlenmiş bir amaca ulaşmak için hemfikir bireylerin oluşturduğu bir grubu kapsayan, onların bilgi kaynaklarını, görüşlerini ve tecrübelerini paylaşma faaliyetinde bulunan, sistematik olarak planlanıp, yönetilen bir aktivite olarak tanımlanabilir (4).

Bilginin kullanımı: Bilgi ancak organizasyon içinde kullanıldığında değer yaratabilir. Bilginin kullanım aşaması, bilginin oluşturulması, paylaşılması ve depolanması için referans noktası olarak hizmet eder. Bilginin bazı kullanımları, belirli bir sorunun çözümüne ya da karar verme sürecine doğrudan bir katkı sağlamayabilir. Ancak elde edilen birikimler sonucu uzun vadede daha sağlıklı kararlar verilmesine ya da problemlerin daha doğru biçimde çözülmesine dolaylı olarak etki edebilir (4).

3.2.2. Bilgi yönetiminin temel amaçları

- Organizasyon içinde yeni bilgi üretmek,
- Örgütsel kararlarda ulaşılabilir bilginin kullanılmasını sağlamak,
- Daha hızlı bir öğrenme ile iyileştirme sağlamak,
- Doğru bilginin, doğru insanlara, doğru zamanda ulaşmasını sağlamak,
- Dış kaynaklardaki değerli bilgiyi kuruma kazandırmak,
- Bilgiyi dokümanlar, veri tabanları ve yazılımlar aracılığı ile sunmak,
- Oluşan bilgilerin örgütün birimleri arasında ya da başka örgütlerdeki benzer birimler arasında transferini gerçekleştirmek,
- Organizasyonel bilgiyi değerlendirilerek entellektüel sermayeye dönüştürmek ve ölçülmesini sağlamak (73).

3.2.3. Bilgi yönetiminin önemi

Kurum içinde yaşanan deneyimler, uygulamalar, düşünceler, öngörüler ve öğrenilen dersler sonucunda oluşan bilginin yalnızca bir kısmı yararlıdır. İşletme için yararlı olduğu anlaşılan bilgi “üretken” bilgidir ve kurum için anlam taşır. Bu nedenle, kurum amaçları ve gereksinimleri doğrultusunda ele alınması gereken bilgi yönetimi, işletme performansını artırmak amacı ile üretken bilginin elde edilmesi, paylaşılması, geliştirilmesi ve kullanılması ile ilgilenir. Bilgi yönetiminin temel çabası, bilgiyi üretken kılmaktır. Yönetilecek bilgi, sadece kurumun faaliyetlerinin sonuçları ışığında tanımlanabilir ve değerlendirilebilir (36).

Bilgi yönetiminin organizasyonlar için önemi, kurumdaki bilginin üretilmesi sürecinde başlar. Bilgi yönetimi, bir işletmede neredeyse tüm çalışanların katıldığı örgütsel bir aktivitedir. Bu nedenle bilgi yönetimi, öğrenmeyi, bilgi paylaşımını ve bilgi teknolojilerini kullanmayı cesaretlendiren, kurumsal bir kültüre gereksinim duyar. Bu anlamda, öğrenen organizasyon kavramı ile bilgi yönetimi arasında önemli bir bağlantı olduğu söylenebilir (36).

3.3. Bilgi Güvenliđi

Bilgi güvenliđi denildiđinde akla ilk gelen kendimize ait olan bilginin başkasının eline geçmemesidir. Aslında güvenlik sadece bilginin başkasının eline geçmemesi anlamına gelmez. Bilgi güvenliđinin sözlük anlamı; bilgilerin izinsiz erişimlerden, kullanımdan, ifşa edilmesinden, yok edilmesinden, deđiştirilmesinden ya da hasar verilmesinden koruma işlemidir

(http://tr.wikipedia.org/wiki/Bilgi_guvenligi).

Bilgi güvenliđi; verilerin ya da bilgilerin, saklanması ve taşınması sırasında, bütünlüğünün bozulmadan, izinsiz erişimlerden korunması için gösterilen çabaların tümü ya da bilginin bir varlık olarak hasarlardan korunması, dođru teknolojinin, dođru amaç ile ve dođru şekilde kullanılarak, her türlü ortamda istenmeyen kişiler tarafından elde edilmesinin önlemesi olarak da tanımlanabilir (13).

Bir başka tanım ile bilgi güvenliđi; bilginin, hizmetin sürekliliđini sađlamak, maddi kayıpları en aza indirmek, üzere tehlike ve tehdit alanlarından korunmasıdır (49).

Bilgi güvenliđinin temel amacı;

- Veri bütünlüğünün korunması,
- Yetkisiz erişimin engellenmesi,
- Mahremiyet ve gizliliđin korunması,
- Sistemin devamlılıđının sađlanmasıdır.

Bilgi güvenliđi gizlilik, bütünlük ve erişilebilirlik olarak isimlendirilen üç temel unsurdan oluşur ve bu üç temel unsurdan herhangi biri zarar görürse, güvenlik zafiyeti meydana gelir (<http://gul6.bim.gantep.edu.tr>, Bilgi Güvenliđi Nedir ve Nasıl Sınıflandırılır? erişim tarihi 15 Mart 2013).

Gizlilik: Bilginin yetkisiz kişilerin eline geçmemesi için korunmasıdır. Bilginin depolanması, işlenmesi, iletilmesi ya da herhangi bir süreci sırasında, sahibi tarafından yetkilendirilmemiş kurum ya da kişiler tarafından ulaşılmasının engellenmesi anlamına gelir.

Bütünlük: Bilginin yetkisiz kişiler tarafından değiştirilememesidir. Bilginin depolandığı yerde ve aktarılırken doğru ve tam olduğunun yani doğru şekilde işlendiğinin ve yetkisiz bir şekilde değiştirilmediğinin garantilenmesi anlamına gelir (7).

Erişilebilirlik: İhtiyaç duyulduğunda bilginin, yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olmasıdır.

Bilgi güvenliği;

- Ağ güvenliği,
- Kullanıcı güvenliği,
- Veri güvenliği,
- Uygulama güvenliği,
- Kimlik ve erişim yönetimi,
- Güvenlik yönetimi,
- Sanallaştırma ve bulut olacak şekilde 7 genel kategoride incelenebilir
(<http://gul6.bim.gantep.edu.tr>, Bilgi Güvenliği Nedir ve Nasıl Sınıflandırılır?
erişim tarihi 15 Mart 2013).

3.3.1. Bilgi güvenliğini etkileyen faktörler

Bilgi güvenliğinin sağlanmasından, bilginin sahibi, bilgiyi kullanan ve bilgi sistemini yöneten kişiler sorumludur. Bilgi güvenliği ihlali için tehdit; sistemin ya da kurumun zarar görmesine neden olabilecek istenmeyen bir olayın arkasındaki gizli sebep olarak tanımlanabilir (49).

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

İnsan faktörü

İnsanlar bilgi güvenliğinin temelini oluşturmaktadır. İnsanlar bilgi güvenliğini tasarlar, uygular ve yürütürler. Bunun yanında kurumsal sistem ve bilgilere, fiziksel ve mantıksal erişimi yönetirler ve bu sırada hatalar yapabilir, vakalar oluşturabilir ve sistemlerde büyük açıklıklara neden olabilirler. Kurulan

birçok teknolojik yapıda insana ait faaliyetler kontrol edilemez, yönetilemez ve ölçülemez olmaktadır. Bu durum ise süreçlerin sağlıklı işlememesine ve kullanıcılar tarafından yapılan hataların yol açtığı sorunların anlaşılmasına ya da giderilememesine neden olabilmektedir (72).

İç tehdit

Bilgi güvenliği tehditleri arasında, organizasyon bünyesinde çalışanların oluşturabileceği bilinçli ya da bilinçsiz tehditler olarak tanımlanabilen iç tehditler, çok önemli bir yer tutmaktadır. Bilinçli tehditler iki kategoride ele alınabilir. İlk kategori, organizasyonda yer alan kötü niyetli bir çalışanın kendisine verilen erişim haklarını kötüye kullanmasını içerir. İkinci kategori ise bir çalışanın başka birine ait erişim bilgilerini elde ederek, normalde erişmemesi gereken bilgilere erişerek, kötü niyetli bir aktivite gerçekleştirmesini kapsar. Veritabanı yöneticisinin, eriştiği verileri çıkar amacı ile başka bir işletmeye satması, ilk kategoriye verilebilecek bir örnektir. Veritabanı yöneticisi olmayan ve normalde veritabanına erişim hakkı bulunmayan birisinin, erişim bilgilerini bir şekilde elde ederek, verilere ulaşması ve onları çıkarı için kullanması, ikinci kategoriye örnek olarak verilebilir

(<http://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/bilisim-sistemleri-guvenligi-arastirmalarinin-yonu.html>, Kara M, Bahşi H. Bilgi Sistemleri Güvenliği Araştırmalarının Yönü, erişim tarihi 15 Mart 2013).

Computer Security Institute tarafından yapılan, Amerika Birleşik Devletleri'nde bazı kamu kurumlarının, finansal şirketlerin, eğitim kurumlarının ve sağlık işletmelerinin bilgi teknolojileri ve bilgi güvenliği profesyonellerinin katıldığı ankete göre, 2008 yılı içinde katılımcıların % 44'ü iç suistimal yaşamışlardı

(http://gocsi.com/forms/csi_survey.html, Richardson R. CSI Computer Crime and Security Survey 2008, erişim tarihi 19 Mart 2013).

Söz konusu oran, iç suistimallerin % 50'lik virüs tehdidinden sonra ikinci büyük tehdit olduğunu göstermektedir. Bu tür suistimallerin tespitinin zor olduğu ve çoğunlukla organizasyon dışına bu konu ile ilgili çok fazla bilgi verilmek istenemeyebileceği de düşünülürse, aslında % 44'lük oranın daha yüksek olabileceği düşünülebilir. Anket çalışmasında, suistimal tabiri ile sadece bilinçli oluşan iç

tehditlerin kastedildiği anlaşılmaktadır (http://gocsi.com/forms/csi_survey.html, Richardson R. CSI Computer Crime and Security Survey 2008, erişim tarihi 19 Mart 2013).

Yine, Pricewaterhouse Coopers şirketinin, 7000'den fazla güvenlik uzmanı ile yaptığı ve 2007 - 2008 yılının sonuçlarını açıkladığı araştırmada, mevcut ve eski çalışanların en büyük tehlikeyi oluşturduğu belirtilmiştir (72).

İç tehditler çoğunlukla uygulama seviyesinde oluşmaktadır. Bunun nedeni, iç tehditlerin önemli bir kısmını bilişim alanında detaylı teknik bilgi sahibi olmayan çalışanların oluşturmasıdır. Söz konusu kişiler, çoğunlukla teknik saldırı yöntemlerini kullanmadan, uygulamaların kendilerine verdiği yetkiler kapsamında ya da başka kişilerin erişim bilgilerini sosyal mühendislik yöntemleri ile ele geçirerek, uygulamaları suistimal ederek hedeflerine ulaşmaktadırlar

(<http://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/bilisim-sistemleri-guvenligi-arastirmalarinin-yonu.html>, Kara M, Bahşi H. Bilgi Sistemleri Güvenliği Araştırmalarının Yönü, erişim tarihi 15 Mart 2013).

Tehditlerin hedefi;

- Yazılım,
- Donanım,
- Veri,
- Depolama ortamları,
- Bilgi aktarım ortamları,
- İnsanlar olabilir.

Kişisel gizlilik

Kişisel gizlilik, bir kişinin ya da bir grubun kendilerine ait bilginin kimlere ve hangi şartlar altında iletileceğinin, bizzat o kişilerin/grubun onayı ile gerçekleştirilmesi anlamında kullanılmaktadır. Kişisel gizliliğin sağlanması iki farklı durumda da gerçekleştirilmelidir. İlk durum, kişisel verilerin kişilere ait bilgi sistemlerinde bulunduğu sırada, tüm tehditlere karşı korunmasıdır ki, bu anlamda herhangi bir bilginin korunması için geçerli tedbirler uygulanır. Bu tedbirler, erişim

denetimi, yetkilendirme, sürekliliğin sağlanması gibi konuları içerir. İkinci durum ise kişisel verinin bir başka sistem ile ihtiyaç dahilinde paylaşılmasında uygulanacak güvenlik tedbirlerini kapsar. Bu tedbirler, 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 paylaşılmasını içerir

(<http://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/bilisim-sistemleri-guvenligi-arastirmalarinin-yonu.html>, Kara M, Bahşi H. Bilgi Sistemleri Güvenliği Araştırmalarının Yönü, erişim tarihi 15 Mart 2013).

Kişisel verilerin korunmasına ile ilgili birçok tartışma yapıldıktan sonra, 2000 yılında Amerika Birleşik Devletleri ve Avrupa Birliği arasında '*Safe Harbor*' adı verilen ve kişisel verilerin korunması alanında farklı sistemler arasında bir uzlaşma örneği olan anlaşmaya varılmıştır. Bu anlaşma verilerin işlenmesi ile ilgili, bildirim, seçim, aktarım, güvenlik, doğruluk, erişim ve uygulama olmak üzere yedi temel ilkeyi içermektedir. Anlaşmaya göre, Amerikan ticari şirketleri, kapsamda kabul edilen ilkelere bağlı olacaklarını belirterek, Avrupa Birliği arasında veri aktarımı gerçekleştirebileceklerdir (38).

Türkiye'de kişisel verilerin korunması, 2010 yılından itibaren açıkça anayasal bir hak olarak düzenlenmiştir. Anayasa'nın 20. maddesine eklenen hüküm uyarınca: '*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*' (37).

Türkiye'de sağlık verilerinin gizliliğine ilişkin temel kaynak ise Hasta Hakları Yönetmeliği'dir. Yönetmeliğe göre hasta hakları, temel insan haklarının sağlık alanına yansımalarıdır. Bu kapsam içinde kişisel sağlık verilerinin korunması da yer almaktadır. Kanunlar ile izin verilen durumlar ve tıbbi zorunluluk halleri dışında, hastanın özel ve aile yaşamının gizliliğine dokunulamayacağı maddesi, ilkeler

arasında yer alır. Yönetmelik ile kişisel verilerin korunmasının temel ilkeleri büyük oranda karşılanmaktadır. Hastalar bu yönetmelikte belirtildiği üzere, kendi kişisel verilerine erişim hakkına sahiptir. Ayrıca hasta mahremiyetine saygı gösterilmesi esas olduğundan, hasta kayıtlarını yalnızca hastanın izni olur ise, hastanın tedavisi ile doğrudan ilgili olan kişiler görebilir. Hastaya ilişkin sağlık hizmeti verilmesi sonucunda edinilen bilgiler de, yasa ile izin verilen haller dışında hiçbir şekilde açıklanamaz (38).

Bilgi güvenliği ihlalleri;

- İzinsiz erişim (bilginin kopyalanması, okunması, dinlenmesi)
- Zarar verme (bilginin kaybolması, ulaşılamaz/kullanılamaz duruma gelmesi)
- Değişiklik yapma (bilgilerin/programın değiştirilmesi, veri aktarılması)
- Üretim (veri taklidi, veri eklenmesi) şeklinde olabilir (49).

Güvenlik olayları aşağıda açıklandığı üzere genel olarak 6 sınıfta gruplandırılmaktadır:

- Çalışan sahtekârlığı: Çalışanlar tarafından sahtekârlığa yönelik aktiviteleri içeren olaylar.
- Taklit: Bir kişinin/kişilerin farklı bir kişi/kişiler ya da kurum gibi tanıtılarak gerçekleştirilen olaylar.
- Kayıp: Fiziksel medyaların örneğin disklerin, ekipmanların ya da basılı materyallerin, sistemdeki bilgilerin, kaybolmasını ya da tahrip edilmesini içeren olaylar.
- Sızma/nüfuz etme: Bilgisayar yazılımına, bilgisayar sistemine ya da bilgisayar ağına sızma olayları.
- Hırsızlık: Fiziksel medyaların örneğin disklerin, ekipmanların ya da basılı materyallerin, sistemdeki bilgilerin çalınmasını içeren olaylar.
- Yetkisiz açıklama (ifşa): Bilinmeyen ve/veya yetkisiz kişilere bilginin gösterilmesini içeren olaylar (65).

3.3.2. Bilgi güvenliği sağlama araçları

Bilgi güvenliği sağlama araçları aşağıdaki şekilde sıralanabilir (49):

Fiziksel güvenlik: Fiziksel önlemler ile (güvenli ortam vb) güvenliğin sağlanması,

Kullanıcı doğrulaması yöntemleri: Akıllı kart, tek kullanımlık parola, gibi kullanıcı doğrulama araçlarının kullanılması,

Şifreleme: Güvensiz ağlar üzerinden geçen verilerin güvenliği için şifreleme yapan donanımların kullanılması,

Yönetsel önlemler: Güvenlik politikaları; kurumsal, konuya özel ve sisteme özel güvenlik politikaları oluşturulması,

Standartlar ve prosedürler: Konfigürasyon yönetimi, yedekleme ve yedekleme ortamlarını saklama, olay müdahale, iş sürekliliği ve felaket kurtarma prosedürleri,

E- imza,

Anti-virüs sistemleri,

Güvenlik duvarları,

Yedekleme,

Erişim denetimi,

Birey eğitimleri ve farkındalık yaratma.

3.3.3. Bilgi güvenliği standartları

Güvenlik süreci bir organizasyonun genel varlıklarını korumak için tasarlanmış bir genel güvenlik politikası ile başlar. Bilgi güvenliğinin yönetilmesinde bir işletme, kendi sahip olduğu kontrol araçlarını bir araya getirebilir, uygulama ilkelerini benimseyebilir, güvenlik standartlarından birini kabul edip

sertifika almak için çaba gösterebilir ya da bunların bir karışımını izleyebilir. Bütün bu faaliyetlerin amacı bilgi varlıklarının yeterli şekilde korunmasını güvence altına almaktır (64).

Bu konunun önemine dikkat çekmek ve bilgi güvenliğini geliştirecek gerekli çalışmaları yapmak üzere, bazı önemli standartlar ve yasal düzenlemeler oluşturmuştur. Bu sayede bilgi güvenliğinin sürekliliği, kaynakların doğru şekilde kullanımı ve güvenlik uygulamalarının geliştirilmesi amaçlanmıştır (<http://bilgiguvenligi.gov.tr/bt-guv.-standartlari/bilgi-guvenligi-standartlari.html>, Poşul A. Bilgi Güvenliği Standartları, erişim tarihi 19 Mart 2013).

Standartların kullanım nedenleri

Organizasyonların bilgi güvenliğinin sağlanmasında karşılaştıkları en temel zorluklar şu şekilde sıralanabilir:

- Yüksek entegrasyon gerektiren bilgi teknolojileri temelli sistemlerin geniş bir alanda kullanılmaya başlanması,
- Hızla değişen teknoloji ile temellendirilmiş bilgisayarların, uygulamaların ve ağ yapılarının yüksek tehdit altında bulunmaları,
- Teknolojik sistemlerin sürekli saldırıya maruz kalmaları,
- İşletmelerin düşük maliyetli ve yüksek verimli sistemlere ihtiyaç duymaları,
- Yasal ve düzenleyici zorunlulukların bilgi güvenliği adına getirdiği yükümlülükler,
- Kurumların kaynak, beceri ve uzmanlık bakımından bilgi güvenliğini sağlamadaki yetersizlikleri

(<http://bilgiguvenligi.gov.tr/bt-guv.-standartlari/bilgi-guvenligi-standartlari.html>, Poşul A. Bilgi Güvenliği Standartları, erişim tarihi 19 Mart 2013).

Yukarıda belirtilen bu zorluklardan dolayı, organizasyonlar, bilgi güvenliğini kapsamlı bir şekilde ele alan, faaliyet alanına göre güvenliğin sağlanmasına dair kuralları dile getiren belli başlı standartların oluşturulması ve uygulanması yoluna gitmiştir.

Yürürlükteki standartlar

HIPAA: Bireylerin sağlık bilgilerini internet uygulamaları ya da elektronik sistemler aracılığı ile aktaran organizasyonlar, HIPAA standartlarının yükümlülüklerini yerine getirmek zorundadırlar. Bu organizasyonlar, hastaneler, eczaneler, kaza ve sağlık sigortaları, tıbbi hizmet planı veren şirketler, tıbbi cihaz satan ve kiralayan şirketler, bireysel hekim klinikleri vb. organizasyonlar olabilir. HIPAA bireylerin sağlık bilgilerini korumak için, mahremiyete ve güvenliğe uygun olarak geliştirilen bir takım idari, fiziksel ve tekniksel önlemler ile ilgili standartlardır (<http://bilgiguvenligi.gov.tr/bt-guv.-standartlari/bilgi-guvenligi-standartlari.html>, Poşul A. Bilgi Güvenliği Standartları, erişim tarihi 19 Mart 2013).

İdari önlemler: Gizliliği olması gereken birimlerin denetlenmesi ve bunlar için gerekli prosedürlerin yazılması için bir yöneticinin atanması, korunması gereken sağlık bilgilerine kimlerin ulaşp kimlerin ulaşamayacağını belirlenmesi, başka bir deyişle çalışan sınıflandırmasına gidilmesi, çalışan eğitimleri ile gerekli bilgilendirmelerin yapılp farkındalık yaratılması, organizasyon ile beraber çalışan dış kaynakların da bu standartlara uyacağına dair anlaşmaların yapılması, acil durumlarda birimlerin verileri geri çekebilme ve veri düzeltme işlemlerini yapabilmeleri, zarar durumlarını görebilme ve veri üzerinde zarar tespiti yapabilmeleridir.

Fiziksel önlemler: Cihazların ağ çalışma gruplarına katılırken ya da gruplardan çıkarılırken gereken önemin gösterilmesi, sağlık bilgilerini içeren cihazlara ulaşımın kontrol edilmesi ve izlenmesi, bu cihazlara ulaşımın yetkilendirilmiş kişiler tarafından yapılmasının sağlanmasıdır.

Tekniksel önlemler: Sağlık bilgilerini içeren cihazların, siber saldırılara karşı korunması, bu bilgilerin ağ üzerinde akması halinde, şifreleme yöntemlerinin kullanılması, her birimin sağlık verilerinin değişmeyeceği ya da hareket ettirilmeyeceğine dair güvence vermesi, risk analizlerinin ve risk yönetimlerinin belgelendirilmesidir (<http://bilgiguvenligi.gov.tr/bt-guv.-standartlari/bilgi-guvenligi-standartlari.html>, Poşul A. Bilgi Güvenliği Standartları, erişim tarihi 19 Mart 2013).

Gram-Leach-Bliley Act: Bankalar, güvenlik şirketleri ve sigorta şirketlerinin güvenliği ve müşteri mahremiyeti için geliştirilmiş bir standartlar bütünüdür. Müşterilere ait gizli bilgilerin korunmasını esas almıştır. Mahremiyet ve bilgi güvenliği ile ilgili üç temel prensibi vardır (<http://bilgiguvenligi.gov.tr/bt-guv.-standartlari/bilgi-guvenligi-standartlari.html>, Poşul A. Bilgi Güvenliği Standartları, erişim tarihi 19 Mart 2013):

Mali mahremiyet kuralı: Mali organizasyonlar, müşteri mahremiyetini korumak için, onlar ile ilgili bilgilerin nerede ve nasıl kullanıldığını, bu bilgilerin nasıl korunduğunu belirten müşteri arşivlerini tutmaları, müşteri bilgilerinin korunmaması durumunda müşterinin ne gibi haklarının bulunduğu belirtilmesi, organizasyonun güvenlik ile ilgili yaptığı politika değişikliklerini müşterinin onayına sunulması zorunludur.

İhtiyat kuralı: Organizasyonlar tarafından müşterilerin gizli bilgilerini korumak için ne gibi önlemler alacağına ve hangi yöntemleri uygulayacağına dair yazılı planların oluşturulup, en azından bir çalışanı bu iş için görevlendirmesi, her birim için risk yönetim merkezinin kurulup, bilgiyi korumak adına, program geliştirilmesi, izlenmesi ve test edilmesi, bilginin toplanması, sunulması ve kullanılmasına göre politikaların değiştirilmesidir.

Veri çalınmasının engellenmesi kuralı: Erişim izni olmadan, diğer müşterilerin bilgilerine ulaşımın engellenmesidir.

BASEL: Bankaların sermaye yeterliliklerinin ölçülmesine ve değerlendirilmesine ilişkin olarak hazırlanmış standartlar bütünüdür. Amacı bankaların risk yönetimlerini etkin bir hale getirmek, piyasa disiplini geliştirmek, sermaye yeterliliği ölçümlerinin etkinliğini artırıp böylelikle etkili bir bankacılık sistemi oluşturmaktır. Bilişim sistemlerinde riskin ortadan kaldırılamayacağı ancak gerçekleşme olasılığının minimize edilebileceği felsefesine dayanır. Bilgi güvenliği sağlanması için aşağıdaki maddelere önem verir (<http://bilgiguvenligi.gov.tr/bt-guv.-standartlari/bilgi-guvenligi-standartlari.html>, Poşul A. Bilgi Güvenliği Standartları, erişim tarihi 19 Mart 2013):

Eriřim kontrolü: Bir organizasyonda, biliřim teknolojilerine kimin nasıl eriřeceęi ile ilgili belirlemelerin yapılması, kullanıcı hesaplarının oluřturulması, kaynak eriřim hakları ve ayrıcalıklı yönetici hesaplarının belirlenmesi, řifre ve kullanıcı hesapları ile ilgili standartların belirlenmesidir.

İř süreklilięinin saęlanması: Doęal afetler, yazılım ya da donanım hataları, elektrik kesintisi gibi önceden bilinemeyecek durumlar için gerekli risk tedbirlerin alınması, bu durumlar için acil risk yönetim masalarının oluřturulması, müşteri hizmetlerinin devamlılıęının saęlanması, bu süreçte yasal sorumlulukların yerine getirilmesi, organizasyona ait verinin ve her türlü bilginin korunarak verinin saklandığı sunucuların önceden farklı yerlerde kopyasının tutulmasıdır.

Deęiřiklik yöntemi: Talep edilen ve gerekli bulunan deęiřikliklerin tanımlanması, bir deęiřiklięin olası etkilerinin belirlenmesi, hangi sistemlerin hangi tarihlerde hangi sıra ile güncelleneceęinin tespit edilip bunlardan sorumlu çalışanların belirlenmesi, olumsuz durumlar için geri dönüşüm prosedürlerinin detaylıca hazırlanmasıdır.

Güvenlik yöntemi: Yetkisiz eriřimlerin engellenmesi, bilginin deęiřtirilmesinin ve bilgiye saldırılmasının engellenmesi, koruma için gereken kontrol ve ölçümlerin tespiti, bu ölçümlerin belgelendirilip kontrollerin uygulanmasıdır.

Payment Card Industry Data Security System: Organizasyonların kredi kartı işlemleri ve ödemeleri sırasında, güvenlięin saęlanması ve bilgilerin açığa çıkmaması için oluřturulmuř kurallar bütünüdür (<http://bilgiguvenligi.gov.tr/bt-guv.-standartlari/bilgi-guvenligi-standartlari.html>, Pořul A. Bilgi Güvenlięi Standartları, eriřim tarihi 19 Mart 2013).

Güvenli bir internet aęının oluřturulması ve bakımı: Kart sahibinin bilgilerini korumak adına güvenlię duvarının oluřturulması, dış kaynak organizasyonlar tarafından saęlanan güvenlię parametrelerine itibar edilmesidir.

Kart sahibi bilgilerinin korunması: Kart sahibine ait depolanmış bilgilerin korunarak dış dünyaya açık ağ üzerinde akan bu bilgilerin şifrlenmesidir.

Saldırlara karşı yönetim biriminin oluşturulması: Dış tehdite açık sistemlerin anti-virüs yazılımlarının güncellenmesi, güvenli sistemlerin ve uygulamaların geliştirilip kullanılmasıdır.

Erişim kontrol ölçütlerinin zorlaştırılması: Kart sahibinin bilinmesi gereken 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: Ağ kaynaklarına ve kart sahibi bilgilerine erişimlerin takip edilmesi, düzenli olarak güvenlik sistemlerinin ve işlemlerinin test edilmesidir.

Bilgi güvenliği politikası geliştirilmesi: Bilgi güvenliğini esas alan politikaların belirlenmesidir.

4. HASTANE BİLGİ YÖNETİM SİSTEMLERİ VE BİLGİ GÜVENLİĞİ

4.1. Hastane Bilgi Yönetim Sistemleri

Hastaneler topluma hizmet sunan, önemli nitelikte işgücünü istihdam eden, sosyal güvenlik, eğitim ve sağlık sigortası gibi başka sosyal sektörler ile çok önemli ve yakın ilişkileri bulunan ve karmaşık bir örgüt yapısına sahip kurumlardır. Aynı şekilde sağlık sektöründeki organizasyonların en çok kaynak tüketen ve bundan dolayı en fazla önem taşıyan hastanelerdir denilebilir (3).

Son yıllarda artan rekabet, hastaneleri işlerin nasıl daha etkin yapılabileceği konusunda düşünerek konuya çözüm aramaya yönlendirmekte ve çözüm olarak bilgi teknolojileri ve bilgi sistemleri kullanımı ön plana çıkmaktadır. Ayrıca hastanelerin güçlü bir finansal yapıya sahip olmasının ve elde edilen mali kaynakların en rasyonel biçimde kullanılmasının yolunun bu sistemlerden geçtiği, hastane yöneticilerinin büyük bir kısmı tarafından kabul edilmekte ve bu nedenle hastane bilgi yönetim sistemi yatırımlarına daha fazla ağırlık verilmektedir (60).

Hastaneler büyük miktarda bilgiyi toplayan, işleme tabi tutan, kullanan ve depolayan bilgi yoğun organizasyonlardır. Yüksek kaliteli sağlık bakım hizmeti ve etkin bir yönetim, hastanelerde üretilen bilgilerin kapsamlı ve dikkatli bir biçimde yönetilmesini zorunlu kılmaktadır. Günümüz hastanelerinde bilginin etkin yönetimi ise bilgi sistemi ve bunun bir uygulaması olan hastane bilgi yönetim sistemi yardımı ile gerçekleştirilmektedir (60).

Bilgi, yönetim kararlarında dikkate alınması gereken önemli beceriler olarak tanımlanabilir. Yönetim ve bilgi aslında birbirine bağlıdır. Bilginin kullanımı, maliyet, fayda ve bilginin oluşumu ile ilgilidir. Bilgi sisteminin işlevi, ait olduğu kurumun bilgi taleplerini, doğru, zamanında, tam ve uygun biçimde karşılamaktır (60).

Hastane bilgi yönetim sistemi (HBYS); hastane işletmelerinin çeşitli düzeylerindeki karar vericilere yardımcı olmak amacı ile bilgi toplama ve bilgiyi yayma fonksiyonlarını üstlenen, farklı kaynaklardan elde edilen verileri bütünleyebilen sistemdir. HBYS temel olarak, bir hastanedeki tüm tıbbi ve idari işlemlerin bilgisayar ortamında yapılması, her türlü verinin birbiri ile bütünleşik olarak çalışan çeşitli modüller yardımı ile farklı kullanıcılar tarafından ana bir veri tabanına girilmesi ve gerekli olan tüm çıktıların bu veri tabanından tekrar anlamlı bir şekilde geri alınmasını sağlayan, hastanelere zaman, işgücü, maddi kazanç ve en önemlisi doğru ve güvenilir istatistikî veri/bilgi sağlayan bir yazılımlar bütünü olarak tanımlanabilir (24).

HBYS kullanımının en temel amacı, sağlık kurumlarının zaman, insangücü, donanım, malzeme, finans gibi tüm kaynaklarının etkin bir şekilde kullanılmasına olanak vererek, gelir ve giderlerin izlenerek kaçakların önlenmesi, kaynakların verimli olarak kullanılması, verilerin hızlı ve güvenli bir ortamda değerlendirilerek tüm birimler arasında uyumlu bir çalışma ortamının sağlanmasıdır. HBYS hastanenin günlük işlerinin düzgün yürütülmesini sağlayarak, hastanenin karar ve kontrol mekanizmalarını yönlendirerek hemen her seviyede çalışanın katılımını gerektiren ve uzun bir dönemi kesintisiz olarak içine alan teknolojik ve sosyolojik bir süreçtir (2).

4.1.1. Hastane bilgi yönetim sistemlerinin kullanım alanları

Bilişim teknolojileri ile sağlık sektöründe hizmet kalitesi artarken, bu konu hastaneler açısından hayati önem taşımaya başlamıştır. Avrupa Birliği'nin 2007 raporunda, bağlı tüm ülkelerin bilişim teknolojilerini sağlıkta daha etkin kullanması ve böylece kalite artırılırken diğer taraftan da maliyetlerin düşürülmesi tavsiye edilmektedir. Yine Avrupa Birliği üye ve aday ülkeleri de sağlık hizmetlerinde "ulusal sağlık bilişimi" hedefleri koymuştur. Bu çerçevede "hastanelerin birlikte çalışılabilirliği" ve "evde bakım" kavramları önem kazanmıştır. Sağlıkta, bilişim sistemlerinin uluslararası standartlara uyması, farklı bilgi sistemleri arasında standart iletişim protokollerinin olması, bütünleşik ve birlikte çalışılabilirlik gibi konular olmazsa olmazlar olarak belirlenmiştir.

(http://www.sabiyap.org/makaleler.php?mak_id=40, Yaman Z. Teletıp ve Bilişim Altyapısı, erişim tarihi 20 Mart 2013).

Sağlık hizmetleri diğer alanlardan daha fazla bilgiye duyarlı bir alandır. Kaliteli bir sağlık hizmeti sunumu, geniş kapsamlı ve iyi planlanmış bir bilgi sürecine bağlıdır. Etkin bir yönetim, sistematik olarak bilginin elde edilmesini gerektirir. Sağlık kurumlarında bilgi sistemlerinin kullanılmasının temel amaçları ve bütünlük bir hastane bilgi sisteminin fonksiyonları şu şekilde belirtilebilir:

- Koruyucu ve tedavi edici sağlık hizmetlerinin yönetimi ve sunumu,
- Hasta kimlik bilgileri, hastanın tedavisi ve bu tedavi ile ilgili yönetsel görevleri desteklemek için hasta ile ilgili doğru, güncel ve kalıcı bilginin doğru kişiye, doğru yerde ve kullanılabilir formatta sağlanması, hastalık hakkında gelişmiş bilgi desteğinin, örneğin ilaçların, teşhis ve tedavilerin etkileri / ters etkileri hakkında bilgi sağlanması, tüm bunlar bilginin doğru olarak toplanması, saklanması, işlenmesi ve dokümanite edilmesi ile gerçekleştirilebilir,
- Gelişmiş hastane bilgi yönetim sistemlerinde farklı hastaneler ve hastanelerin ilişkide olduğu kurumlar arasında, bilgi aktarımına olanak veren bir iletişim sağlanması,
- Tedavi süreçlerinin kısılmasının sağlanması,
- Hastalara verilen hizmetin kalitesinin artırılması,
- Yatırım kararlarında giderin en aza indirilmesi için gerekli sayısal bilgilerin elde edilmesi,
- Etkin bir mali işlemler alt bilgi sisteminin kurulması,
- Hastane personelinin özlük dosyalarının tutulması ve saklanması,
- Personelin verimliliği ile ilgili bilgi sağlanması,
- Kırtasiye giderlerinin azaltılmasını sağlanması,
- Sağlık kurumlarında yaşanan sorunların en aza indirilmesi,
- Zaman, iş gücü ve tıbbi cihazların veriminin en üst düzeye çıkarılması,
- Doğru ve düzenli veriler ile bölgenin sağlık kültürünün ve gereksinimlerinin belirlenebilmesi,

- Eğitim hastanelerinde hasta tedavisine ek olarak, araştırma ve eğitim amacı ile hastanın tedavisinde özel deneyimler sonucu ortaya çıkan verileri dikkatli bir şekilde toplayıp yeni bilgiler elde edilmesinin sağlanması,
- İnsan hayatının sözkonusu olduğu bu kurumlarda hata ve risk oranının azaltılması (60).

HBYS kaliteli sağlık bakım hizmeti sunulmasında da önemli bir rol oynamaktadır. Bu sistem sayesinde daha iyi hasta bakımı sağlanmakta, bürokrasi azalmakta, bekleme süreleri kısaltılmakta, hastalara ait bilgilerin kaybolması önlenmekte, tıp eğitiminin kalitesi artmakta ve hemşirelik bakım standartları yükselmektedir (60).

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

- İnsan gücünden tasarruf edilmesi,
- Entegre bakımın sağlanması,
- İş süreçlerinde zamandan tasarruf edilmesi,
- Hataların sayısının azalması, gereksiz işlemlerin kalkması,
- Hekimler arasında bilgi paylaşımının artması, uzman hekimlerin daha iyi değerlendirilmesi,
- Kağıtsız bir hastane oluşturulabilmesi

(http://www.sabiyap.org/makaleler.php?mak_id=40, Yaman Z. Teletıp ve Bilişim Altyapısı, erişim tarihi 20 Mart 2013).

Hastane bilgi sistemleri ilk olarak faturalama, ödemeleri kontrol etme gibi idari amaçlar için kullanılmaya başlanmıştır. 1970'li yıllarda finansal bilgi sistemleri temelli birçok hastane bilgi sistemine, klinik laboratuvar sistemleri, radyoloji, eczane gibi bölümler eklenmiştir. 1990'lara doğru hastane bilgi sistemlerinde idari uygulamalardan, hekimler, hemşireler ve diğer sağlık çalışanları tarafından kullanılan klinik enformasyon sistemlerine doğru bir gelişim başlamıştır (http://www.sabiyap.org/makaleler/php?mak_id=9, Özyurt O. Hastane Bilgi Yönetim Sistemlerinin Genel Özellikleri, erişim tarihi 20 Mart 2013).

Hastane yönetiminde bilgi gereksinimi kaçınılmazdır. Sağlık sistemlerinde evrim niteliğinde değişimler olmaktadır. HBYS sağlık kurumlarının verimliliğine

yönelik en önemli araçların başında gelmektedir. Bilgi yönetim sistemlerinin hayati önem taşıdığı sektörlerin başında ise sağlık sektörünün geldiği söylenebilir. Günümüzde, yasal mevzuatların sık sık değiştiği, hastaların kalite taleplerinin arttığı, hastanelerin sunumlarının, hizmetin kendisinin önüne geçtiği, anlaşılır bir şekilde fark edilmektedir. Bununla birlikte bilginin kalitesi ve sunumu önemli bir faktör olarak karşımıza çıkmaktadır. Sağlık kurumlarının süreçlerine baktığımızda, hastaların kapıdan girdiği andan itibaren kurum içindeki her türlü hareketi ve bu hareketin paralelinde hizmet verenlerin süreçteki yerinin, hastane yönetimi açısından tıbbi ve işletimsel olarak veri bankasına eklenen bir değer olduğunu söylemek mümkündür (http://www.sabiyap.org/makaleler/php?mak_id=9, Özyurt O. Hastane Bilgi Yönetim Sistemlerinin Genel Özellikleri, erişim tarihi 20 Mart 2013).

Sağlık bakım hizmeti vermekte olan kurumlar; verimliliği artırmak, maliyetleri düşürmek ve hasta bakımının kalitesini geliştirmek, hastalara hak ettikleri bakımı zamanında ve mümkün olduğunca prosedürlerden, formalitelerden uzak bir şekilde verebilmek için, bilgisayar tabanlı bilgi sistemlerine yönelmektedirler. Günümüzde bu yöneliş, teknolojinin de hızla gelişmesi ile birlikte zorunlu hale gelmektedir (51).

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. Sağlık hizmeti sunumunun planlaması, finansmanı ve yönetimi bakımından gerekli verilerin ulaşılabilir olması, karar verme mekanizmalarının etkinliğini de artırmaktadır. Hastane yönetimi düzeyinde ise elektronik ortamdaki uygulamalar süreçlerin izlenebilirliğini, sürekliliğini ve daha anlaşılır ve açık olmasını sağlamaktadır (16).

Gerçekleşen tıbbi muayene ve tedavi, hasta bakımı, sosyal hizmet, destek hizmetleri vb. faaliyetlerin sonuçlarından elde edilen verileri değerlendirebilmek ve raporlayabilmek için, sağlık yöneticisinin tüm süreçleri kapsayan iyi bir HBYS'ne sahip olması gerekmektedir. Bu sayede sağlık kurumlarında, anlık üretilen bilgi doğrudan entegre bir HBYS üzerinden görülebilir ve kararlar daha hızlı verilebilir

olacaktır (http://www.sabiyap.org/makaleler/php?mak_id=9, Özyurt O. Hastane Bilgi Yönetim Sistemlerinin Genel Özellikleri, erişim tarihi 20 Mart 2013).

Hastane bilgi yönetim sistemleri yakın gelecekte sadece hastanelerde kullanılan sistemler olmayacak, dikey olarak entegre edilmiş, sağlık bakım sunucuları tarafından kontrol edilen, hastanın bakım aldığı çoklu ortamlara entegre edilebilen, modüler öğelerden oluşturulacak yaşam boyu hasta kayıt sisteminin bir parçası olacaklardır (http://www.sabiyap.org/makaleler/php?mak_id=6, Örengül O. Hastane Bilgi Sistemleri, erişim tarihi 20 Mart 2013).

4.1.2. Hastane bilgi yönetim sistemini oluşturan temel bileşenler

Yönetimi desteklemeye yönelik sistemler

Bu sistemler; hasta kayıt sistemi, kaynak kullanımı ve planlama sistemi, mali yönetim bilgi sistemi, malzeme ve tesis yönetim bilgi sistemi ile personel yönetim bilgi sistemi olarak sınıflandırılabilir.

Tanı ve tedaviyi desteklemeye yönelik sistemler

Bu sistemler ise; klinik bilgi sistemi, hemşirelik bilgi sistemi, eczane bilgi sistemi, laboratuvar bilgi sistemi, radyoloji bilgi sistemi ve hasta izlem sistemi olarak gruplara ayrılabilir (24).

4.1.2.1. Yönetimi desteklemeye yönelik sistemler

Yönetimi desteklemeye yönelik sistemler ile hastadan alınan ücretlerin faturalandırılmasından, malzeme takibine kadar pek çok işi takip etmek mümkündür. Günlük işlemlerin takibi yanında bilgisayarlar, yönetime bilgi sağlamak amacı ile de kullanılmaktadır (24).

Hasta kayıt sistemi

HBYS’nde yer alan bu bölüm temel bir modülde yeni hasta kaydı oluşturmak üzere, hastanın hastaneye başvurusundan itibaren ihtiyacı olan bilgileri alma ile başlayan ve taburculuğu sonrasına kadar tüm idari işlemlerini yürütmek için kullanılan

uygulamalar bütünüdür. Aşağıda açıklandığı şekilde kullanılan modüller ile detaylandırılabilir (60).

Danışma modülü

Güvenlik, gizlilik ve mahremiyet esaslarına uyulmak kaydı ile hasta ve hastane çalışanlarının oda numarası, telefon numarası, hastaların başvurduğu servis, başvuru tarihi, yattığı servis, telefon numarası, yatışını yapan hekim bilgileri gibi bilgiler konusunda, danışmaya müracaat eden hasta yakınlarına yardımcı olmak ve kısa sürede cevap verilmesini sağlamak üzere tasarlanmıştır (44).

Hasta kabul modülü

Kuruma ilk defa başvuran, veri tabanında kaydı bulunmayan hastalara ait genel bilgilerin girişinin yapıldığı, daha önceden kaydı bulunan hastalara yeni geliş kaydının açıldığı ve ilgili sosyal güvenlik kurumundan provizyon ve takip numarası alınan, belirtilen arama kriterlerine göre kayıtlı hastaların bilgilerini ekranda gösteren fonksiyondur (44)(60).

Randevu işlemleri modülü

Hasta randevularını düzenleyen modüldür. Randevu girişi, randevu arama ve görüntüleme, randevu onayı ve kapatma işlemlerini kapsar. Poliklinik, klinik, laboratuvar, fizik tedavi, radyoloji, ameliyathane vb. tüm randevu verilen birimler için tasarlanmıştır (44).

Poliklinik modülü

Hastanın başvurusundan muayene olmasına ve hastaneyi terk etmesine kadar olan süreçte, polikliniklerde ihtiyaç duyulan tüm tıbbi ve mali işlemlerin elektronik ortama aktarılarak, gerekli kayıtların tutulmasını ve bu bilgilerin gerektiğinde incelenebilmesini amaçlar (44).

Hasta yatış, yatan hasta takip ve hasta çıkış işlemleri modülü

Hastanın yatışı ile ilgili tüm işlemler (hasta bilgileri, yatış onayı bilgileri, refakatçi işlemleri, kullanılan malzemeler, verilen ilaç girişleri, tetkik sonuçları, gözlem ve epikriz notları vb.) bu modül ile gerçekleştirilebilir. Poliklinik, acil servis ya da doğumhaneden tüm servislere yatış ve refakatçi işlemleri yapılabilir. Tüm ücretler, hastanın elektronik ortamdaki mali kayıtlarına otomatik olarak yansıtılabilir. Taburcu edilen hastanın dosyası bu modülden faturalamaya hazır hale getirilir (44)(60).

Girişimsel işlemler – ameliyathane modülü

Hastanede hasta ile ilgili olarak yapılan tüm girişimsel işlemler ekrandan seçilip yapılan ameliyatlar işlenir. Doktorlar, hemşireler ve anestezi teknikerlerinden oluşan ameliyat ekibinin bilgileri kayıt edilir. Ameliyat ile ilgili tüm bilgiler girilerek, ameliyat raporu hazırlanır. Ayrıca ameliyathane ilaç ve sarf malzemelerinin izlemi de yapılır (44).

Fatura – vezne modülü

Yapılan tüm girişimsel işlemler, kullanılan bütün malzeme ve ilaç bilgisi ekrana gelir. Sosyal güvencesi olan hastalarda, hasta katkı payları belirlenir. Hastalara polikliniklerden ve servislerden istenilen tetkikler için vezneye ücret yatırılmadı ise, laboratuarda işlem yapılması önlenir. Hastanın ödeyeceği ücret vezne otomatik olarak görülür (60)(44).

Hekim modülü

Başvuran hastaların hangi hekim tarafından muayene edileceğini belirleyen alt modüldür. Hekimler kendilerine atanan hastaların listesinin görüntüleme ve raporlama yetkisine sahiptir. Hekim atanan hastalar listesinden hastasını seçerek tıbbi bilgi girişi ekranına geçebilir. Tanı girişinde ICD-10 kodları kullanılır. Hastaya ait temel tıbbi bilgilerin hekim tarafından girilebilmesi için serbest bir bölüm bulunmaktadır (44).

Elektronik order verme ve elektronik reçeteleme

Elektronik orderlar, hastaya verilen ilaçlar, laboratuvar tetkikleri, görüntüleme sonuçları, konsültasyonlar ve diğer tanı testleri için order işlemlerini içeren bilgisayar uygulamalarıdır. Elektronik reçeteleme ile sağlanan ilaç bilgi yönetim sistemlerinin asıl amacı, ilaç kullanım hatalarını azaltmak ve hasta güvenliğini artırmaktır. Birden fazla hekimin tedavi ettiği hastalarda, yan etki oluşumu ve ilaç etkileşimi ön plana çıkan önemli konulardır. Ayrıca okunaksız yazılar ile ilgili sorunların üstesinden gelmek, benzer ilaç isimleri ile ilgili daha az hata olmasını sağlamak, karar destek sistemleri ile daha kolay entegre etmek, reçeteyi yazan hekimi belirlemek, ilaç uygulama yöntemleri ile tedavi ve ilaç seçimini işaret etmek, fazla reçete yazımını önlemek, reçetelerin eczaneye daha hızlı ulaşmasını sağlamak, elektronik orderların amaçları içinde sayılabilir (60)(44).

İlaçların uygun dozda ve sürede kullanımını sağlayıp, bununla ilişkili olarak maliyetleri azaltmak da diğer bir avantajlı durumdur. İlaç seçimi sırasında karar destek sistemlerinin önerilerini dikkate almak, tıbbi personelin iş akışına yardımcı olabilir. Avantajlarının yanı sıra kurulum maliyetinin yüksek olması, iş akışının kağıda dayalı sisteme göre yavaş olması nedeni ile adaptasyon yavaş olabilir. Bu sorunları çözmek açısından iş akışı çok iyi analiz edilmeli, yeterli sayıda order set hazırlanmalı, uygulamaya geçiş için son tarih dikkatli olarak belirlenmelidir (44).

Geçiş sürecinde kısa bir süre için hem kağıt, hem de elektronik sistem bir arada uygulanmalıdır. Sistemin başarısı için uygulamalar hakkında çalışanlar çok iyi eğitilmelidir. Eğitimler belli aralıklarla tekrarlanmalı, hekimlere, eczacılara ve hemşirelere bu sistemin kullanımı ile sağlanan avantajlar yazılı olarak rapor edilmelidir. Sonuç olarak; hekimler tarafından yavaş kabul edilen bir sistem olmasına karşın bu durum zaman içinde gelişecek ve bu sistemi üreten ve satın alanlar arttıkça maliyetler de düşecektir (44).

Kaynak kullanımı ve planlama sistemi

Kaynakların gittikçe azalması ve ihtiyaçların yüksek miktarda parasal yatırım gerektirmesi, etkin kaynak kullanımını gündeme getirmektedir. Bu sistem temelde, yatak doluluk oranlarını, klinik ve acil servis faaliyetlerini, malzeme ve cihaz

kullanımını programlamak ve izlemek üzere geliştirilmiştir. Kaynak kullanımı ve programlama sistemi, kısıtlı kaynaklardan en iyi şekilde yararlanma, talebi karşılama, bütçe düzenleme, orta ve uzun dönem planlamaları yapma konularında hastane yöneticisine yol gösterici olmaktadır (24).

Mali yönetim bilgi sistemi

Mali yönetim bilgi sistemi, hastanelerde verimlilik performansının ne olduğunu görme açısından yöneticilerin vazgeçemeyecekleri bir konudur. Bir mali bilgi yönetim sisteminin amaçları aşağıdaki şekilde sıralanabilir:

- Günlük muhasebe işlemlerini yürütmek,
- Yatırım kararlarında giderin en aza indirilmesi için gerekli sayısal bilgileri elde etmek,
- Etkin bir mali işlemler alt bilgi sistemi kurmak,
- Mali işlemlerin denetim ve değerlendirilmesinde kullanılacak mali raporları hazırlamak.

Sistemin içerdiği konular:

- Personel veri sisteminden gerekli bilgileri alarak, bordro hazırlamak ve hesap çıkarmak,
- Yapılacak ödemeleri belirlemek,
- Yapılan masrafları ve borçlu kişilerin hesaplarını tahsil etmek,
- Ana defter hesabını tutmak,
- Genel giderlerin paylaştırılması için gider dağıtım sistemini çalıştırmak,
- İlgili kişi ve kuruluşlara sunulacak mali raporları hazırlamak,
- Bütçe düzenlemek ve bütçe denetimini sağlamak (24).

Malzeme ve tesis yönetim bilgi sistemi

Bu sistem malzemelerin ve tesisin daha verimli yönetimi konularında yöneticilere yardımcı olmaktadır. Örneğin satın alma, envanter denetimi, mutfak yönetimi, tesis bakımlarını izleme, enerji yönetimi, projeleri programlama ve denetim konuları, bu sistemin kapsamında yer alan bazı konulardır.

Malzeme yönetim bilgi sisteminin kullanılmasının en önemli nedenlerinden biri, hastaneye girişı yapılan ve kullanılan her tür malzemenin yönetim kademesi tarafından takip ve kontrolünün yapılabilmesini sağlamaktır. Her tür demirbaş ve sarf malzemesinin tüketimi denetlenebildiğı zaman, hastanenin gelir gider dengesini optimum düzeyde tutmak daha kolay olacaktır (24).

Personel yönetim bilgi sistemi

Tartışmasız bir şekilde personel, bir hastanenin en önemli kaynağıdır. Bu önemli kaynağın elde tutulabilmesi için bir hastane bütçesinin yaklaşık % 60 – 70'i personel giderlerine ve sosyal yardımlara ayrılmaktadır. Personel yönetim bilgi sistemi kullanılarak;

- Hastane personelinin özlük dosyalarının tutulması ve saklanması,
- Gerekli durumlarda bu dosyaların bilgi amaçlı kullanılması ve güncellenmesi,
- Görev denetiminin sistematik olarak yapılması,
- Hastanenin tüm maliyet merkezlerine ait çalışma analiz raporlarının çıkartılması,
- İşe devam, nöbet gibi personel problemlerinin oluşabileceğı konularda raporlama yapılması,
- Çalışanların özel yetenek ve belge durumlarının takip edilebilmesi,
- Bordro sistemine bağılı olarak personel giderlerinin maliyet dağılımının hesaplanması,
- Personelin verimliliğı ve kalite kontrolü ile ilgili bilgi edinilmesi sağlanabilir (24).

4.1.2.2. Tanı ve tedaviyi desteklemeye yönelik sistemler

Klinik bilgi sistemi

Klinik bilgi sistemleri (KBS), hastanedeki hasta bakımını destekleyen bilginin işlenmesini, depolanmasını ve yeniden ulaşılmasını içerir. Bu sistem hastalara ait önemli klinik bilgileri toplayıp kullanılabilir hale getiren bir sistemdir. KBS yalnızca klinik bilgi açısı ile sınıflandırılabilceğı gibi, geniş olarak tedavinin tüm yönlerini

içine alacak şekilde de sınıflandırılabilir. KBS hastanın hastalık geçmişi ve sağlık hizmeti sağlayıcıları ile etkileşimi gibi klinik verileri depolayan bir klinik veri havuzu sağlar. KBS'nin başlıca yararları şu şekilde sıralanabilir:

- Hasta verilerine kolay erişim: KBS bütün bakım noktalarında tıbbi kayıtlara uygun erişim sağlar. Bu konu özellikle mobil noktalarda önemlidir ve bu neden ile de bakımın sürekliliğini genişletmektedir. İnternet tabanlı sistemler, bu tür verilere uzaktan erişim yeteneğini geliştirir.
- Bekleme süreleri: Hastaların servis içi bekleme süreleri azalır ve daha iyi ve etkin tıbbi kayıt ve yeniden bilgiye ulaşımı sayesinde bakım kalitesi artar.
- İletişim: Hasta bakımı sağlayanlar ile hekimler arasındaki iletişim kolaylaşır.
- Standartlar: Teşhis ve tedavi için standartlar geliştirilmesi sağlanır.
- Yapısal bilgi: KBS ile toplanan bilgi ile hasta bilgileri daha çabuk araştırma ve sağlama yapmayı kolaylaştırır. Ayrıca okunaksız yazıdan kaynaklı yanlışlıkların önüne geçilebilir.
- Gelişmiş ilaç reçetesi ve hasta güvenliği: KBS ilaç dozajını kontrol etme ve daha uygun farmasötikal kullanımı desteklerken, ilaç etkileşimlerinin olumsuz yan etkilerinin azaltılmasına öncülük eder (24).

KBS tarafından sağlanan yararlar olmasına rağmen, kullanımın yaygınlaşmasına engel olabilecek bazı durumlar da mevcuttur. Bunlar:

- İlk alım masrafı: Klinik bilgi teknolojisi alt yapısının yüksek maliyeti, birçok sağlık kurumu için önemli bir engel olabilir.
- Gizlilik ve güvenlik: Bilgisayar sistemi üzerindeki hasta verilerinin gizliliği ve bu derece önemli bilgilerin nasıl korunabileceği hakkında hala ciddi endişeler bulunmaktadır. Amerika ve İngiltere'de hükümetler tarafından çıkarılan HIPAA ve Veri Koruma Kanunları bu endişeler üzerine geliştirilmiştir denilebilir.
- Hekim direnci: Hekimlerin hastalarını görmeleri için genellikle 20 dakika civarında zamanları vardır ve bu sürede herhangi bir KBS ile etkileşimleri,

gerekli olan süreden daha fazla zaman alacak olursa, sistemin kullanımında direnç oluşabilir.

- Eski sistemlerin entegrasyonu: Bu husus, özellikle önemli bazı bilgilerin kaybedilmesi riski düşünüldüğünde, birçok kurum için önemli güçlükler oluşturabilir (24).

Hemşirelik bilgi sistemi

Çeşitli sağlık bakımı ortamlarından alınan klinik verileri yöneten ve hemşirelere hasta bakımında yardımcı olmak için geliştirilen bir sistemdir. Bilgi sistemleri hemşirelik hizmetlerinde; klinik uygulamalar, yönetim hizmetleri ve eğitim olmak üzere üç alanda kullanılmaktadır. Hemşirelik bilgi sistemi iletişimin geliştirilmesi, karar vermenin desteklenmesi, yeni bilgilerin ortaya konulması, etkili ve kaliteli sağlık bakımının sunulması, hasta beklentilerinin karşılanması, elde edilen bilginin diğer sağlık çalışanları ve kurumları arasında paylaşılması yönünde kolaylıklar sağlamaktadır (24).

Eczane bilgi sistemi

Eczane bilgi sistemi ilaç etkileşimlerini, ilaçlara karşı alerjileri ve olası diğer ilaçla ilgili komplikasyonları izleyerek hasta bakımına destek sağlar. Sistem, bir reçete talebi girildiğinde, hasta tarafından aynı anda alınan iki ya da daha çok ilaç ile ya da herhangi bir gıda ile ilaca karşı bilinen alerjik etkileşimler olup olmadığını ve hastanın yaşına, ağırlığına, diğer psikolojik faktörlere dayanarak, yeterli dozun verilip verilmediğini kontrol edebilir. Yatan ve taburcu olan hastalar için reçetelerin yönetilmesinde kullanılabilir, ilaçların stoklarda bitmesini önlemek için herhangi bir ürünün miktarı, belirlenmiş bir miktarın altında olduğunda, uyarılar oluşturarak, azalan ürünün sipariş edilmesini hatırlatabilir. Birçok eczane bilgi sistemi hastanede ilaç kullanım şekline göre satın alınan ve tüketilen ilaçların maliyetine kadar raporlar oluşturabilir (60).

Laboratuvar bilgi sistemi

Laboratuvarların artan iş yükü ve sorumluluğu, çok büyük miktarda laboratuvar bilgisini toplamayı, özet halinde ve belli bir biçimde hazırlanmasını ve olabildiğince hızlı bir şekilde bu bilgilerin hekimlere ulaşmasını sağlamayı zorlaştırmaktadır. Bu gibi problemleri gidermek için bilgisayarlı sistemlere olan talep artmaktadır.

Laboratuvar test işlemleri bağımsız olarak kullanılabileceği gibi, laboratuvar bilgi sistemine bağlı olarak da kullanılabilir. Laboratuvar bilgi sistemi; test istemlerinin kayıtları, örneklerin alınma zamanları ve test süreçleri, tamamlanan test sonuçlarının kayıtları, istemi yapan bölümlere test sonuçlarının iletilmesi, hastalara verilen bütün test sonuçlarının periyodik raporlarının alınması, istatistiklerin hazırlanması, laboratuvar işlemlerinin yönetimi ve kalite kontrol süreçleri için kayıtların tutulması işlevlerini içermektedir (http://www.sabiyap.org/makaleler.php?mak_id=6, Örengül O. Hastane Bilgi Sistemleri, erişim tarihi 20 Mart 2013).

Günümüzde birçok sağlık kurumunda test sonuçlarının sisteme daha hızlı ve güvenilir kayıt edilebilmesi için, cihazlar ile entegre yazılımlar kullanılmaktadır. Entegrasyonlar ile kullanıcı hataları ortadan kaldırılarak test sonuçlarının güvenli ve hızlı bir şekilde sisteme girilmesi sağlanmaktadır.

Radyoloji bilgi sistemi

Radyoloji bilgi sistemi diğer birimlerde olduğu gibi iş yönetimini geliştirmekte, bölümler arasında iletişimi artırmakta ve hastanın bekleme zamanını kısaltmaktadır. Hastanın tetkik istemleri hekim tarafından sisteme girilebilir ya da manuel olarak yapılan istemler sisteme aktarılabilir. Radyoloji bölümünde elektronik depolamaya izin veren görüntü arşivleme ve iletişim sistemleri (PACS) gibi tıbbi görüntülerin yansıtılması ve aktarılmasına olanak veren sistemler giderek yaygınlaşmaktadır (http://www.sabiyap.org/makaleler.php?mak_id=6, Örengül O. Hastane Bilgi Sistemleri, erişim tarihi 20 Mart 2013).

PACS sistemleri, tıbbi görüntülerin elektronik olarak elde edildiği, ayrıldığı, aktarıldığı, depolandığı ve görüntülendiği filmsiz bilgi sistemidir. Sistemin amaçları; bütün hekimlerin yeni ve eski filmlere ulaşımını kolaylaştırmak, geniş fiziksel alan

gerektiren filmlerin saklanması kolaylaştırmak, personel maliyetini en aza indirmek ve pahalı olan gümüşe dayalı filmleri ortadan kaldırmak olarak sayılabilir. Teknolojik zorluklar ve yüksek maliyet dezavantajlarına rağmen PACS kurulması ve kullanımı son on yıl içerisinde artmıştır

(http://www.sabiyap.org/makaleler.php?mak_id=6, Örengül O. Hastane Bilgi Sistemleri, erişim tarihi 20 Mart 2013).

Hasta izlem sistemleri

Hasta takip sistemlerinde bilgisayarlar, hastanede yatarak tedavi gören ya da evde bakım hizmetlerinden yararlanan hastaların, yaşam fonksiyonlarını sürekli olarak izlemek ve periyodik olarak fizyolojik verilerini göstermek görevlerini yürütmektedir (60)(24).

4.2. Hastane Bilgi Yönetim Sistemlerinde Bilgi Güvenliği

Sağlık işletmeciliği bilgi temeline dayanan bir sektör olduğundan, sağlık hizmetleri faaliyetleri ile ilgili işlemlerin her aşamasında ihtiyaç duyulan bilgiyi sağlayacak bir bilgi yönetim sisteminin varlığı, günümüzde kaçınılmaz hale gelmiştir. Sağlık hizmetleri için gereksinim duyulan bilgiler zamanında, eksiksiz olarak ve güvenilir bir şekilde sağlanmadığında, ortaya çıkabilecek sorunlar insan sağlığını doğrudan etkileyebildiği için sağlık kurumları açısından bilginin etkin yönetimi oldukça önemli bir konudur. Sağlık hizmetlerinde bilgi yönetimi, sağlık hizmetleri içinde var olabilecek eksiklikleri ele almayı ve gidermeyi amaçlar (4).

Sağlık hizmetleri, hastanın teşhis, tedavi ve bakımı ile ilgili oldukça karmaşık prosedürleri içermektedir. Teşhis, tedavi planlaması ve hasta bakımı sırasında yapılan tetkikler, ilaç kullanımı, ameliyat endikasyonu ve sonuçları, girişimsel müdahaleler, hasta taburcu etme, taburcu olduktan sonraki bakımlar sırasında, hasta güvenliğini tehdit eden bazı istenmeyen olaylar meydana gelebilir. Dolayısı ile günümüzde bakım ve taburcu aşamasında hasta güvenliğini sağlayacak önlem ve uygulamalar büyük bir önem kazanmıştır (4).

Sağlık hizmetlerinde bilgi, tanı ve tedavi döneminin her aşamasında, özellikle de karar verme konusunda merkezdir. Sağlık hizmetlerinde bilgiye, doğru ve eksiksiz bir karar vererek ve etkili tedavi yöntemini belirlemek için başvurulur. Bu süreçte hastalar için iyi sonuç verecek ya da başarılı olacak tedavi girişimlerini sağlamak ve hastanın sağlık durum değerlendirmesinde doğru yorumu yapmak için, gereken zamanda, eksiksiz ve doğru bilgilerin kullanımına ihtiyaç duyulur (1).

Sağlık hizmeti veren kurumlar, hasta tedavilerinin kalitesinin geliştirilmesi için de bilgi yönetimine gereksinim duymaktadır. Özellikle bilgi yönetimi en iyi uygulamaları gerçekleştirmek için karar destek sistemlerine, hastaların tanı ve tedavisindeki hataların azaltılarak hasta güvenliğini artırmak için temel bilgi faaliyetlerine gereksinim duyar. Bununla birlikte sağlık profesyonellerinin isteği sadece bilgiye kolayca ulaşmak değil, daha çok karar vermeyi desteklemek için güncel ve mevcut bilginin iş akışlarına kesintisiz olarak dahil edilmesidir. Aynı şekilde hastalar, kendilerinin sağlık hizmet alım süreci ile başa çıkmak ve bu süreci anlamaya yardım edecek kişisel bakım haritalarını öğrenmeyi ve bakımla ilişkili eğitim almayı isterler. Sağlık hizmetlerinde elde edilen bilgi yalnızca bir kaynak değil, aynı zamanda ve asıl olarak bir hizmettir. Sağlık hizmeti organizasyonları içinde, hasta bakımlarını iyileştirmek amacına ek olarak, tıbbi hataları azaltmak için de bilgi yönetimi uygulamaları başlamıştır (26).

Bilgi yönetimi, doğru ve güncel bilgiyi doğru yerde, gereken zamanda ve en uygun biçimde sağlamayı amaçlar. Böylece bilginin kullanılabilirliğini sağlamaya ve güven altına alınmasına olanak verir (26).

Sağlık hizmetlerinde bilgi yönetiminin amacı, hasta bakım sonuçlarını ve klinik uygulamaları iyileştirmek, sağlık hizmetlerine etkinlik ve yenilik getirmektir. Daha iyi bir sağlık hizmet bilgisi, kurum içinde işbirliğinin yaygınlaştırılması, iç kaynakların etkin kullanımının sağlanması ve bilgi yönetiminin bir kaynak olarak hizmet etmesi ile mümkündür (57).

Sağlık hizmetlerinde bilgi yönetiminin rolü, hem klinik hem de idari uygulamalarda önemli olabilmektedir. Klinik uygulamalarda, tıbbi bilginin paylaşımının artması ve kanıta dayalı tecrübelerin organizasyon içinde ve organizasyonlar arasında dağıtımı ile daha etkili uygulamalar ortaya çıkabilir. Nihayetinde bilgi yönetiminin rolü, klinik ve idari fonksiyonlar arasındaki bağlantılarda özellikle önemlidir. Genellikle bu iki kategorinin faaliyetleri, mesleki uzmanlaşma, organizasyonun rolü, uygulama standartları ve amaçları gibi farklılıklar ile ayrılır (69).

Bilgi teknolojileri yaygınlaşmadan önce, bilginin büyük çoğunluğu basılı dokümanlarda iken, günümüzde bilgi teknolojileri tarafından işlenir duruma gelmiştir. Buna paralel olarak bilgiye erişim olanakları geçmiş ile kıyaslanamayacak derecede artmıştır. Aslında bu durum, birçok dezavantajı da beraberinde getirmektedir. Bilgi teknolojileri üzerinde bilinçli ya da bilinçsiz yapılan hataların çok ciddi sonuçlar ortaya çıkarması olasıdır. Bilgi teknolojilerindeki dikkatsiz yapılandırmalar ve açıklar bilgiye yetkisiz erişime yol açabilir. Bu durumda bilginin yetkisiz kişilerce değiştirilmesi, görülmesi ve yok edilmesi söz konusu olabilir. Geçmişte sadece fiziksel güvenliğin tesis edilmesi ile sağlanan bilgi güvenliği, günümüzde organizasyonların en çok zorlandıkları ihtiyaçların başında gelmektedir (http://www.sabiyap.org/makaleler.php?mak_id=18, Hülür Ü. Bilgi Güvenliği ve Sağlık, erişim tarihi 21 Mart 2013).

Birçok akademik kaynakta, bilgi güvenliğinin teknik ve teknolojik bir kavram olmadığı vurgulanmakta, bilgi güvenliğinin sağlanması için kurum kültürünün değiştirilmesi, kurum üst yöneticilerinin bilgi güvenliği ile ilgili süreçlerde aktif olarak rol alması gibi sosyal çalışmalara değinilmektedir.

Günümüzde kurumlar ve bireylerin sahip olduğu en değerli varlıkları olan bilginin, gizlilik, bütünlük ve erişilebilirlik nitelikleri bakımından sürekli korunması gerekmektedir. Koruma bazı fiziksel ve sistemsal önlemlerin alınmasının yanında, çalışanların bilgi güvenliğine ilişkin tehdit ve risklerden, kurum bilgi güvenlik politika ya da kurallarından haberdar olması, bu tehditlere nasıl karşı koyabileceği, olası risklerin mümkün olabilecek en düşük seviyede nasıl tutabileceği konusunda bilgilenmesi ile mümkün olabilir

(http://www.sabiyap.org/makaleler.php?mak_id=18, Hülür Ü. Bilgi Güvenliği ve Sağlık, erişim tarihi 21 Mart 2013).

Bilginin gizliliği, bütünlüğü ve erişilebilirliğinin sağlanması olarak ifade edebileceğimiz “bilgi güvenliği” konusunda ISO 27000 serisi oldukça kapsamlı süreçler öngörmektedir. Bu seri içerisinde yer alan; ISO/IEC 27001:2005 bir Bilgi Güvenliği Yönetim Sistemi için spesifikasyonları belirlerken, ISO/IEC 27002:2005 ise Bilgi Güvenliği Yönetimi için uygulama kodu niteliğindedir. ISO 27799:2008 standardı ise, sağlık bilişimi ile ilgili olup, ISO/IEC 27002 kullanılarak sağlık sektöründe bilgi güvenliği yönetiminin nasıl gerçekleştirileceğini düzenlemektedir (http://www.sabiyap.org/makaleler.php?mak_id=18, Hülür Ü. Bilgi Güvenliği ve Sağlık, erişim tarihi 21 Mart 2013).

Konu ile ilgili uluslararası düzenlemelerde 2008 yılında yayımlanan ve sağlık sektörü için bilgi güvenliği esaslarını sunan yeni ISO standardı; ISO 27799:2008 (Sağlık Bilgileri – Sağlıkta ISO/IEC 27002 bilgi güvenliği yönetimi) oldukça önemlidir. Bu standart son derece hassas olan kişisel sağlık bilgileri konusu ve bu bilgilere hem sağlık hizmetleri çalışanlarının erişiminin garanti edilmesi, hem de bilgilerin gizliliğinin ve bütünlüğünün en iyi şekilde korunması konusunu değerlendirmekte ve bunu mümkün kılmak için bir hareket planı oluşturmaktadır. ISO 27799:2008, sağlık bilgilerinin şekillendirilmesi, saklanması ve paylaşılması aşamalarında gerekli olan tüm tedbirlerin alınması ve güvenlik altında tutulması için detaylı standartlar da içermektedir. Aynı zamanda, ilgili uluslararası standartları uygulayarak, sağlık hizmetleri organizasyonları ve sağlık bilgileri koruyucularına, boyutlarına ve durumuna göre gerekli görülen güvenlik şartlarını da sağlayabilmektedir (http://www.sabiyap.org/makaleler.php?mak_id=18, Hülür Ü. Bilgi Güvenliği ve Sağlık, erişim tarihi 21 Mart 2013).

Sağlık sektöründe çalışan bilgi güvenliğinden sorumlu personeli ve kurumun tüm çalışanlarını ilgilendiren bu standart, bütün sağlık kurumlarına uygulanabilmektedir. Standartta hastaların sağlık durumları ile ilgili bilgilerin çeşitli durumlar altında gizliliğinin, bütünlüğünün ve erişilebilirliğinin nasıl korunabileceği anlatılmaktadır. ISO 27799, ISO 27001 bilgi güvenliği yönetim sistemine ek olarak, sağlık sektöründe bu standardın nasıl yorumlanması gerektiğini açıklar

(<http://gelisim.ogr/index.php?bolum=makale&mno=98>, Sağlık Kurumlarında Bilgi Güvenliği Yönetim Sistem Standardı, erişim tarihi 21 Mart 2013).

Bilgi hangi biçimde olursa olsun (konuşulan bilgi, ses kayıtları, çizimler, video görüntüleri, tıbbi tahlil sonuçları vb.), hangi ortamda bulunursa bulunsun (basılı ya da elektronik ortamda) ya da bilginin transferi için hangi araçlar kullanılırsa kullanılsın (fax, bilgisayar ağları, posta vb.) mutlaka çok iyi bir şekilde korunmalıdır (<http://gelisim.ogr/index.php?bolum=makale&mno=98>, Sağlık Kurumlarında Bilgi Güvenliği Yönetim Sistem Standardı, erişim tarihi 21 Mart 2013).

ISO 27799 standardına uyum sağlamanın yararları aşağıdaki şekilde sıralanabilir (<http://www.27000.org/iso-27799.htm>, erişim tarihi 21 Mart 2013):

- Hastaya ait tüm bilgilerin gizliliğinin korunması ve sadece erişim yetkisi olan kişiler tarafından erişilebilmesinin sağlanması,
- Hasta sağlığına ilişkin kritik bilgilerin bütünlüğünün korunması yani bilgilere tam ve doğru olarak erişilebilmesi için gerekli kontrollerin yapılmasının sağlanması,
- Sağlık kurumlarında yeni teknolojik sistemlerin adapte edilmesi sırasında kesintisiz hizmet sunulmasına katkıda bulunulması,
- Sağlık sektörüne ilişkin bilgilerin yok olması, yetkisiz kişilerin eline geçmesi gibi bilgi güvenliği ihlali olarak sayılabilecek durumların azalmasının sağlanması,
- Kaynakların etkili ve verimli bir şekilde kullanılmasının sağlanması.

ISO 27799 Standardı;

- Sağlık terimleri,
- Bilgi güvenliği terimleri,
- Sağlık bilgi güvenliği,
- Sağlık bilgi güvenliğinin amaçları,
- Sağlık kurumlarında bilgi güvenliği,
- Korunması gereken sağlık bilgisi,
- Sağlık sektörüne yönelik korunulması gereken tehditler ve zayıflıklar,

- ISO 27002 nin kurulması için hareket planı,
- ISO 27002 nin sađlık sektöründe yorumlanması,
- Bilgi güvenliđi politikası,
- Bilgi güvenliđi organizasyonu,
- Varlık yönetimi,
- İnsan kaynakları güvenliđi,
- Fiziksel ve çevresel güvenlik,
- Haberleşme ve işletim yönetimi,
- Erişim kontrolü,
- Bilgi sistemleri edinim, geliştirme ve bakımı,
- Bilgi güvenliđi ihlal olay yönetimi,
- İş sürekliliđi,
- Uyum,
- Sađlık sektörüne ilişkin tehditleri içermektedir (<http://www.27000.org/iso-27799.htm>, erişim tarihi 21 Mart 2013).

Sađlık kurumları ISO 27799 uygulayarak şunları elde edebilir:

- Etkin bilgi güvenliđi sistemi oluşturulması ve takip edilmesi,
- Bilgi kaçakları oluşumunun azaltılması ve engellenmesi,
- Yasal yükümlölük doğurabilecek risk noktalarının azaltılması,
- Hastaların kuruma karşı güveninin artırılması,
- Çalışanların yetki ve sorumluluklarının netleşmesi,
- Kurum yatırımının korunması

(http://www.sabiyap.org/dergi/2009/sabiyap_dergisi_03_2009.pdf, Aydınllı C. Bilgi Güvenliđi Yönetim Sistemi Standardı, erişim tarihi 25 Mart 2013).

Kişisel sađlık verileri, kişisel veri kategorisi içinde “hassas” ya da “özel niteliđi olan” veriler kategorisinde yer almaktadır. Bu gizliliđi korumak tıbbi verilerin sahibi olan kişilerin mahremiyet hakkının korunması bakımından gereklidir. Hasta güvenliđini sađlamak için sađlık bilgisinin bütünlüğü mutlaka korunmalıdır ve bu korumanın en önemli bileşeni de sađlık bilgisinin tüm yaşam döngüsü boyunca denetlenebilirliđini sađlamaktır. Sađlık bilgisinin erişilebilir olması, etkili bir sađlık hizmeti sunulması

bakımından hayati öneme sahiptir. Sağlık bilişim sistemlerinin bu neden ile doğal afetler, sistem çökmeleri ve olası saldırılar karşısında kullanılabilir şekilde olmaları son derece önemlidir. Sağlık bilgisinin gizlilik, bütünlük ve erişilebilirliği bu neden ile sağlık sektörüne özgü uzmanlığı gerektirmektedir

(http://www.sabiyap.org/makaleler.php?mak_id=20, Keser Berber L. Kişisek Sağlık Verilerinin Elektronik İletişim Yönetimleriyle İletimi, Standartları ve Çözüm Yolları, erişim tarihi 25 Mart 2013).

Gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması gereken birçok bilgi çeşidi mevcuttur. Bunlar:

- Kişisel sağlık bilgileri,
- Kişisel sağlık bilgilerinden, kimlik bilgileri arındırma yöntemleri ile elde edilmiş olan veriler,
- Kişisel sağlık bilgilerinden elde edilen anonimleştirilmiş veriler de dahil olmak üzere, istatistiksel ve araştırma verileri,
- Klinik karar destek sistemleri de dahil olmak üzere, herhangi bir spesifik tedavi öznesine ilişkin olmayan klinik/tıbbi bilgiler (ilaç etkileşimine ilişkin veriler gibi),
- Sağlık uzmanları ve çalışanlara ait bilgiler,
- Kamu sağlığı gözlemlerine ilişkin bilgiler,
- Sağlık bilgi sistemleri tarafından üretilen kişisel sağlık bilgilerini içeren ya da bu bilgilerden türetilen kimlik bilgilerinden arındırılmış veriler ya da kişisel sağlık bilgilerine ilişkin olarak kullanıcı hareketlerine ilişkin işlem geçmiş verileri,
- Erişim kontrol verileri ve güvenlik ile ilişkili diğer sistem konfigürasyon verileri de dahil olmak üzere, sağlık bilgi sistemleri için sistem güvenliği verileri olarak sayılabilir

(http://www.sabiyap.org/makaleler.php?mak_id=20, Keser Berber L. Kişisek Sağlık Verilerinin Elektronik İletişim Yönetimleriyle İletimi, Standartları ve Çözüm Yolları, erişim tarihi 25 Mart 2013).

Organizasyon içinde kişisel sağlık bilgileri ne kadar iyi korunursa korunsun, çalışanlar tarafından elektronik iletişim yöntemleri (e-posta, sms gibi) ile paylaşıldığında, sağlık bilişimi standartlarında öngörülen ancak uygulamada çok da fazla dikkat edilmeyen, çok önemli bir bilgi güvenliği açığı ortaya çıkmaktadır. Teknolojik önlemler alınmadan gerçekleştirilen elektronik iletişim, hem teknik hem de hukuki açıdan güvensiz bir paylaşım platformu olduğu için, sağlık kurumlarının bilgi güvenliği standartlarına ve düzenlemelerine uyumlarında sorun yaratabilir. Kişisel sağlık bilgilerini elektronik iletişim yöntemleri ile ileten sağlık kurumlarının, bu mesajların gizliliğini ve bütünlüğünü sağlayacak önlemleri almış olmaları gereklidir (http://www.sabiyap.org/makaleler.php?mak_id=20, Keser Berber L. Kişisel Sağlık Verilerinin Elektronik İletişim Yönetimleriyle İletimi, Standartları ve Çözüm Yolları, erişim tarihi 25 Mart 2013).

Yine, yazılım firmaları gerek sahada personel bulundurarak gerekse ihtiyaç duyulduğunda uzaktan HBYS'ne erişerek problem giderme, sürüm yükseltme gibi işlemleri gerçekleştirmektedir. Bu işlemler için ister istemez hasta bilgilerinin bulunduğu veri tabanlarına erişim olanakları olmaktadır. Her ne kadar yapılan sözleşmelerde yazılım firmalarını bağlayan maddeler bulunsun da, kurum haricinde kişi ya da kuruluşların hastanın bütün ya da dönemsel bilgilerine ulaşabilmesi, bilgi güvenliği açısından önemli bir tehdittir

(http://www.sabiyap.org/makaleler.php?mak_id=10, Türk H. Neden Hastaneler HBYS Yazmak İster?, erişim tarihi 25 Mart 2013).

Başka bir örnek olarak, hastanelerin araştırma projeleri için araştırma merkezleri ile hasta verilerini paylaşabilmesi verilebilir. Burada paylaşılan bilgilerden, özellikle belirli bir kişinin hangi hastalığa sahip olduğunun, araştırma merkezine ulaşmaması beklenmektedir. Bu soru, sadece veri içerisinde kişiyi tekil olarak belirleyebilen kimlik numarası, isim ve soyisim gibi bilgilerin çıkarılması ile çözülememektedir. Kişilere ait cinsiyet, adres gibi veriler de çoğunlukla spesifik olarak bir kişiyi tespit etmede yardımcı olmaktadır. Yapılan çalışmalarda, bu tip veri kısımlarının da kişisel gizliliği sağlayacak şekilde genelleştirilmesi ya da silinmesi sağlanmaktadır (<http://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/bilisim-sistemleri-guvenligi->

arastirmalarinin-yonu.html, Kara M, Bahşı H. Bilgi Sistemleri Güvenliđi Arařtırmalarının Yönu, erişim tarihi 15 Mart 2013).

Biliřim sistemleri güvenliđi konusunda yapılan arařtırmalar ve projeler, internetin e-devlet, e-sađlık, e-ticaret, e-öđrenme, gibi konularda tüm dünyada yaygın olarak kullanılmaya başlaması ile birlikte hız kazanmıřtır. Günümüzde de biliřim sistemleri güvenliđi alanındaki arařtırmalar devam etmektedir. Elektronik ortamda taşınan, işlenen ve saklanan bilgilerin artmıř olması, güvenliđin dolayısı ile de güvenlik arařtırmalarının önemini daha da artırmıřtır.

5. GEREÇ VE YÖNTEM

Kamu hastanelerinde bilgi teknolojileri ile ilgili uygulamalar, Sağlık Bakanlığı tarafından öngörülen düzenlemeler ve standartlar ile gerçekleşmektedir. Özel hastanelerde ise daha farklı uygulamaların yapılabilmesi mümkündür. Bu neden ile tanımlayıcı tipteki bu araştırma için özel bir hastane tercih edilmiştir.

Araştırmanın evreni Türkiye'deki özel hastanelerdir. Araştırmacının İstanbul'da ikamet etmesi ve İstanbul'daki herhangi bir özel hastanenin sağlık hizmetleri ve bilgi yönetimi konusunda, Türkiye'deki özel hastaneleri temsil edebilecek nitelikte olması sebebi ile İstanbul'da seçilen bir özel hastane örneklemini oluşturmuştur. Belirlenen hastanenin yönetiminden çalışma yapılabilmesi için gerekli izin alınmıştır. Bu kurumda HBYS'ni kullanan tıbbi ve idari birim çalışanlarının tümüne ulaşılması amaçlanmıştır.

Araştırmanın saha uygulaması 15 Şubat 2013 – 28 Mayıs 2013 tarihleri arasında yapılmıştır.

Hastanede günlük çalışması sırasında HBYS'ni kullanmayan çalışanlar araştırma kapsamı dışında yer almıştır. Günlük çalışma sırasında HBYS'ni kullanan 489 çalışandan, araştırmaya katılmayı kabul eden 424 çalışan ile anket formu kullanılarak yüz yüze görüşme yapılmıştır.

Araştırmada kullanılan anket; bilgi güvenliği ölçeği (64) 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 (64) tarafından geliştirilen, sağlık alanı dışında kullanılan bir ölçek ile çalışılmıştır. Ölçeğin kullanımı konusunda geliştiriciden gerekli izin alınmıştır. Ankette yer alan diğer sorular ise kaynaklardan yararlanılarak araştırmacı tarafından oluşturulmuştur.

Bilgi güvenliği ölçeği öncelikle İngilizce'den Türkçe'ye çevrilmiştir. Elde edilen Türkçe ölçek başka bir grup tarafından tekrar İngilizce'ye çevrilmiş ve orijinal metin ile uyumlu olduğu belirlenmiştir.

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.

Yapılandırılmış anket formu pilot değerlendirme olarak 10 kişiye uygulanmış ve anketin anlaşılması ile ilgili bir sorunun olmadığı görülmüştür.

Anket formu iki kısımdan oluşmaktadır. Birinci kısımdaki 1-11 numaralı sorular, katılımcının kişisel özelliklerine yöneliktir. İkinci kısımda bulunan 12-53 numaralı sorular ise bilgi güvenliğine yönelik sorulardır. Ölçekte yer alan 4 soru diğer sorular ile uyumlu olması açısından olumlu ifadeye döndürülmüştür. Ölçeğe ek olarak iki yeni soru araştırmacı tarafından eklenmiştir.

Örnekleme ölçekteki madde sayısının 5 katı yer almıştır. Bu bakımdan faktör analizine uygun olduğuna karar verilmiştir (15). Ölçme aracının geçerliliğini saptamak amacı ile açıklayıcı faktör analizi kullanılmıştır. Yapılan faktör analizi sonucu KMO örneklem yeterliliği değeri 0.90 olarak bulunmuştur. Buna göre faktör analizi için örneklem büyüklüğü “çok iyi” sınıflaması içinde yer almaktadır. Barlett küresellik testi sonucunda ise $p = 0.000$ olarak saptanmıştır. Buna göre verilerin faktör analizine uygun olduğu söylenebilir.

Faktör analizi sonucunda birden fazla faktörlü yapı oluşmuştur. Oluşan 5 faktör yapısı toplam varyansın % 63,26'sını yansıtmaktadır.

Faktör analizi ile elde edilen ölçek, güvenlik politikası, örgütsel güvenlik, güvenlik uygulamaları, erişim ve yetkilendirme ile hizmet sunumu alt boyutlarında değerlendirilmiştir.

Araştırmanın hipotezleri

1.Hipotez: Hastanede farklı meslek grupları arasında bilgi güvenliğinin korunması konusunda fark yoktur.

2.Hipotez: Yöneticiler ile diğer çalışanlar arasında bilgi güvenliğinin korunması konusunda fark yoktur.

3.Hipotez: Tıbbi birim çalışanları ile idari birim çalışanları arasında bilgi güvenliğinin korunması konusunda fark yoktur.

4.Hipotez: Farklı yaş, cinsiyet, eğitim durumu, kıdem ve HBYS eğitimi olan çalışanlar arasında bilgi güvenliğinin korunması konusunda fark yoktur.

Araştırma verilerinin tez danışmanı tarafından değerlendirmesi ile oluşturulan analiz yönergesi doğrultusunda analizler aşağıdaki gibi yapılmıştır. Hipotezlere yönelik testler, yeni oluşturulan faktör yapıları ile değerlendirilmiştir. Her faktörün ortalama değeri hesaplanmış ve analizde bu değerler kullanılmıştır.

Araştırmaya katılan çalışanların sosyo-demografik özelliklerine ilişkin bulgular yaş, cinsiyet, eğitim düzeyi, kurumda çalışma süresi değişkenlerine göre tablolar düzenlenmiştir.

Araştırmanın verileri elektronik ortama aktarılmış ve paket istatistik programında analizler yapılmıştır. Tanımlayıcı türde olan bu araştırmada verilerin bir kısmı ‘n’ ve ‘%’ olarak sunulmuştur. Analizde Ki-kare testi kullanılmıştır. Ölçümsel değerlerin analizinde, Eşleşmemiş T testi ve Pearson korelasyon testleri kullanmıştır. Dağılımın normal olmadığı ya da örnek sayısının 30’un altında kaldığı durumlarda non-parametrik Mann-Whitney U testi kullanılmıştır.

Araştırmada kullanılan ölçeğin güvenilirliği için iç tutarlılık analizi olan Cronbach alpha değeri hesaplanmıştır. Bu değer oluşan 5 faktör yapısında sırası ile 0.8157, 0.8185, 0.8017, 0.9019 ve 0.8963 olduğu saptanmıştır. Buna göre ölçeğin iç tutarlılığının olduğunu söylemek mümkündür.

Tablo 1: Bilgi güvenliği ölçeğine ait maddelerin faktör analizi ile dağılımı

İfadeler	Faktörler				
	1(n=9) Erişim ve Yetkilendirme	2(n=5) Güvenlik Uygulamaları	3(n=4) Hizmet Sunumu	4(n=5) Örgütsel Güvenlik	5(n=4) Güvenlik Politikası
Çalışanlar, kendi kullanıcı hesaplarıyla yetkilendirilip tanımlamaları yapılmadan, sistemlerimizde oturum açamaz/ sistemlerimize erişim sağlayamazlar.	0,790				
Bilgi işlem uygulamaları sadece yetkilendirilmiş iş amaçları doğrultusunda kullanılır.	0,732				
Hastanede, kullanıcıların hangi verilere erişebileceğini belirleyen bir yetkilendirme prosedürü vardır.	0,699				
Halka açık ağlara bağlı olmasına rağmen, sistemlerimiz internet hizmeti sağlayıcısının güvenliği ve/veya kendi güvenlik sistemlerimiz tarafından yeterince korunmaktadır.	0,680				
Sistemlerimiz herhangi bir sorun oluşması beklenmeden, önceden oluşturulmuş bir plan doğrultusunda güncellenmektedir.	0,663				
Anti-virüs sistemimiz günceldir ve bir virüs saldırısı durumunda, sistemlerimizi mümkün olan en iyi şekilde korumaktadır.	0,608				
Bir güvenlik ihlalinin meydana gelmesi durumunda, yapılacaklar ve yardım için kimin aranacağı bilinmektedir.	0,581				
Şifre değiştirme sıklığını belirleyen ve şifre karmaşıklığını engelleyen bir şifre yönetim sistemi bulunmaktadır.	0,547				
Kullanıcıların sistemlerimizde oturum açmalarına yetki verecek uygun mekanizmalar bulunmaktadır.	0,460				
Güvenlik politikalarımızı ve süreçlerimizi ihlal eden çalışanlarımıza yönelik disiplin uygulamaları vardır.		0,761			
Çalışanlar kendi çalışma alanlarından uzaklaştığında, bilgisayarlarını daima güvenli şekilde bırakmaları konusunda eğitilmiştir.		0,701			
Çalışanlar, güvenlik ihlali olaylarının derhal yönetime bildirilmesi gerektiğinden haberdardır.		0,629			
Bilgi güvenliği uzmanı bulunmadığında dışarıdan danışmanlık hizmeti alınmaktadır.		0,550			
Sistem arızası, çökmesi ya da hırsızlık gibi durumlarda, veri yedeklerimiz işimizde kesintiye yol açmayacak şekilde bilgilerimizi geri kazanmamızı sağlar.		0,521			
Bilgisayar kullanımı ile iş akışında olan değişimler bilgi güvenliğine gereken önemi vermeyi engellemez.			0,907		
Bilgi güvenliği süreçleri, hizmet kalitesini olumsuz yönde etkilemez.			0,888		
Bilgi güvenliği gün içinde yaptığımız işleri düşününce öncelikli bir konudur.			0,881		
Hastanedeki iş yükünün fazla olması, bilgi güvenliğine gereken önemin verilmesini engellemektedir.			0,876		
Yöneticiler bilgi güvenliğinin uygulanması konusunda sorumluluk sahibidirler.				0,799	
Hastanedeki yöneticiler bilgi güvenliğine gereken özeni gösterir.				0,780	
Hastane içinde bilgi güvenliği konusunda bir uzman bulunmaktadır.				0,606	
Bilgi güvenliğinin sağlanması için çalışanlar gerekli özeni gösterir.				0,532	
Çalışanlar bilgi sisteminde izin verilen ve onaylanmayan uygulamalar konusunda yeterince bilgilidir.				0,429	
Çalışanlar bilgi güvenliği politikalarından haberdardır.					0,738
Hastanede, bilgi güvenliğine ilişkin yazılı politikalar vardır.					0,737
Hastanede bilgi güvenliğinin sağlanması için görevler ve sorumluluklar net olarak belirlenmiştir.					0,723
Tüm personele yeterli ve uygun bilgi güvenliği eğitimi verilmektedir.					0,715
Varyans açıklama oranları (%)	35,03	11,81	6,96	5,09	4,35
Cronbach Alpha değerleri	0.8157	0.8185	0.8017	0.9019	0.8963

6. BULGULAR

Araştırmaya katılan tıbbi birim çalışanlarının % 57,4'ü (n=148), idari birim çalışanlarının % 71,1'i (n=118) kadın, tıbbi birim çalışanlarının % 53,1'i (n=137), idari birim çalışanlarının % 75,3 ü (n=125) 21-30 yaş arasında, tıbbi birim çalışanlarının % 53,5'i (n=138), idari birim çalışanlarının % 36,7'si (n=61) lisans ya da lisansüstü düzeyde eğitim almışlardır (Tablo 2).

Tablo 2: Araştırmaya katılan tıbbi ve idari birim çalışanlarının sosyo-demografik özellikleri

Değişkenler		Tıbbi birimler		İdari birimler	
		n	%	n	%
Cinsiyet	Kadın	148	57,4	118	71,1
	Erkek	110	42,6	48	28,9
	Toplam	258	100	166	100
Yaş (yıl)	20 ve altı	11	4,3	2	1,2
	21 - 30	137	53,1	125	75,3
	31 - 40	74	28,7	23	13,9
	41 - 50	25	9,7	6	3,6
	51 ve üzeri	5	1,9	0	0
	Cevapsız	6	2,3	10	6
	Toplam	258	100	166	100
Eğitim durumu	Lise	79	30,6	77	46,4
	Ön Lisans	41	15,9	28	16,9
	Lisans / Lisansüstü	138	53,5	61	36,7
	Toplam	258	100	166	100

Araştırmaya katılan tıbbi ve idari birim çalışanlarının çalışma durumları ve HBYS kullanımları karşılaştırıldığında, HBYS kullanım becerisi puanı ile hastane bilgi güvenliği puanının, idari birimlerde tıbbi birimlere göre daha yüksek olduğu belirlenmiştir ($p = 0.016$ ve $p = 0.004$). Kurumda çalışma süresi, HBYS kullanımı deneyim süresi, HBYS kullanımı için alınan eğitim süresi ve bilgisayar kullanım becerisini değerlendirme açısından ise, gruplar arasında anlamlı bir fark tespit edilememiştir ($p>0.05$) (Tablo 3).

Tablo 3: Araştırmaya katılan tıbbi ve idari birim çalışanlarının çalışma durumları ve HBYS kullanımları

	Tıbbi birimler		İdari birimler		p*
	Ortalama puan	Standart sapma	Ortalama puan	Standart sapma	
Kurumda çalışma süresi (ay)	27,4	18,39	25,53	19,67	0.321
HBYS kullanımı deneyim süresi (ay)	37,74	41,05	37,02	46,01	0.873
HBYS kullanımı için alınan eğitim süresi (saat)**	3,97	8,04	4,62	7,26	0.511
Bilgisayar kullanım becerisini değerlendirme (0-100 puan)	81,5	17,6	79,79	18,24	0.342
HBYS kullanım becerisini değerlendirme (0-100 puan)	71,68	20,01	76,39	18,23	0.016
Hastane bilgi güvenliği puanı değerlendirme (0-100 puan)	58,69	16,77	65,01	23,52	0.004

* Eşleşmemiş T testi kullanılmıştır.

** Mann-Whitney U testi kullanılmıştır.

Araştırmaya katılan tıbbi ve idari birim çalışanlarının HBYS kullanımı için eğitim alma durumu karşılaştırıldığında, anlamlı farklılık bulunmuştur ($p = 0.005$). Gruplar arasında eğitim alma durumunun, tıbbi birimde idari birime göre daha yüksek olduğu belirlenmiştir ($p = 0.005$) (Tablo 4).

Tablo 4: Araştırmaya katılan tıbbi ve idari birim çalışanlarının HBYS kullanımı için eğitim alma durumları

		Tıbbi birimler		İdari birimler		p*
		n	%	n	%	
HBYS kullanım eğitimi	Almış	203	78,7	109	65,7	0.005
	Almamış	49	19	50	30,1	
	Cevapsız	6	2,3	7	4,2	
	Toplam	258	100	166	100	

* Ki-kare testi kullanılmıştır.

Araştırmaya katılan tıbbi ve idari birim çalışanlarının HBYS kullanımları incelendiğinde, HBYS kullanımı sırasında ulaşılabilen bilgi türleri açısından; sigorta şirket bilgilerinin % 75 oranında ve sosyal güvence bilgilerinin % 65,8 oranında idari birimlerce, süreçsel raporların % 70,5 oranında ve hastaya ait bilgilerin % 62,4 oranında tıbbi birimlerce ulaşılabilir olduğu görülmektedir.

HBYS’nde günlük işleyiş sırasında kullanılan bilgiler açısından; süreçsel raporların % 70,3 oranında ve kurum prosedürlerinin % 65,7 oranında tıbbi birimlerce, sosyal güvence bilgilerinin % 69,2 ve hastaneye ait mali bilgilerin % 61,8 oranında idari birimlerce ulaşılabilir olduğu görülmektedir.

HBYS’nde koruma altında olduğu düşünülen bilgiler değerlendirildiğinde, tüm parametrelerde grupların kendi içlerinde benzer şekilde değerlendirme yaptığı görülmektedir (Tablo 5).

Tablo 5: Araştırmaya katılan tıbbi ve idari birim çalışanlarının HBYS kullanımları

		Tıbbi birimler		İdari birimler		Toplam	
		n	%	n	%	n	%
HBYS kullanımı sırasında ulaşılabilen bilgi türleri*	Hastaya ait bilgiler	247	62,4	149	37,6	396	100
	Çalışanlara ait bilgiler	66	44,3	83	55,7	149	100
	Hastaneye ait mali bilgiler	35	46,1	41	53,9	76	100
	Yönetimsel raporlar	24	58,5	17	41,5	41	100
	Süreçsel raporlar	98	70,5	41	29,5	139	100
	Kurum prosedürleri	91	60,3	60	39,7	151	100
	Sigorta şirketi bilgileri	16	25	48	75	64	100
	Sosyal güvence bilgileri	26	34,2	50	65,8	76	100
HBYS’nde günlük işleyiş sırasında kullanılan bilgiler*	Hastaya ait bilgiler	243	62	149	38	392	100
	Çalışanlara ait bilgiler	50	41,7	70	58,3	120	100
	Hastaneye ait mali bilgiler	29	38,2	47	61,8	76	100
	Yönetimsel raporlar	17	43,6	22	56,4	39	100
	Süreçsel raporlar	104	70,3	44	29,7	148	100
	Kurum prosedürleri	88	65,7	46	34,3	134	100
	Sigorta şirketi bilgileri	14	23	47	61	61	100
	Sosyal güvence bilgileri	24	30,8	54	69,2	78	100
HBYS’nde koruma altındaki bilgiler*	Hastaya ait bilgiler	179	58,5	127	41,5	306	100
	Çalışanlara ait bilgiler	120	56,1	94	43,9	214	100
	Hastaneye ait mali bilgiler	119	53,6	103	46,4	222	100
	Yönetimsel raporlar	116	55	95	45	211	100
	Süreçsel raporlar	112	63,3	65	36,7	177	100
	Kurum prosedürleri	106	63,5	61	36,5	167	100
	Sigorta şirketi bilgileri	66	59,5	45	40,5	111	100
	Sosyal güvence bilgileri	68	58,1	49	41,9	117	100

* Bu sorularda araştırma grubu tarafından birden fazla seçenek işaretlenmiştir.

Araştırma grubu tarafından, HBYS kullanımı sırasında hasta verilerine erişimin % 18,86 oranında bilgi işlem departmanı tarafından denetlendiğinin düşünüldüğü görülürken, bu soruya grubun % 54,48'inin cevap vermediği görülmektedir (Tablo 6).

Tablo 6: Araştırmaya katılan tıbbi ve idari birim çalışanlarına göre HBYS kullanımında erişim denetimi

		n	%
HBYS üzerinden hasta verilerine erişim kimler tarafından denetleniyor	Bilgi işlem departmanı	80	18,86
	Üst yönetim	24	5,67
	Sorumlu ve müdürler	40	9,43
	Merkez yönetim	31	7,32
	Hemşirelik hizmetleri	18	4,24
	Cevapsız	231	54,48
	Toplam	424	100

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 % 69,3 oranında ve 8765... şeklindeki şifrelerin % 67,7 oranında tıbbi birimlerce, şifrede hastane adı kullanımının ve kullanıcı adı ile şifrenin aynı olmasının % 50 oranlarında idari birimlerce kullanıldığı görülmektedir (Tablo 7).

Hasaya ait bilgilerin paylaşımı için onam formu alınması uygulamasında, her grubun kendi içinde benzer sonuçlar gösterdiği belirlenmiştir (Tablo 7).

HBYS'nde hasta bilgileri için yapılabilen işlemler için; yazma % 63,1 oranında, okuma % 62,8 oranında, silme % 55 oranında ve değiştirme % 53,3 oranında tıbbi birimlerce, gönderme % 50,9 oranında, ekleme % 48,7, değiştirme % 46,7 oranında ve silme % 45 oranında idari birimlerce olduğu tespit edilmiştir (Tablo 7).

HBYS'nde erişilebilen hasta bilgilerinin; tıbbi raporların % 69,2 oranında ve önceden aldığı tıbbi hizmet bilgilerinin % 65,5 oranında tıbbi birimlerce, ödeme

bilgilerinin % 66,7 oranında ve sigorta bilgilerinin % 61,2 oranında idari birimlerce olduğu görülmektedir.

Bilgi güvenliğini artırmak için alınabilecek önlemler konusunda, tüm parametrelerde grupların kendi içlerinde benzer özellikler gösterdiği görülmektedir (Tablo 7).

Tablo 7: Araştırmaya katılan tıbbi ve idari birim çalışanlarının bilgi güvenliği uygulamaları

		Tıbbi birimler		İdari birimler		Toplam	
		n	%	n	%	n	%
Bilgi güvenliğinin sağlanması için kullanılan kimlik belirleme yöntemleri*	Kullanıcı adı	232	63,2	135	36,8	367	100
	Şifre	239	63,1	140	36,9	379	100
Kullanılan şifre yapıları*	1234....	116	67,1	57	32,9	173	100
	8765....	21	67,7	10	32,3	31	100
	Kullanıcı adı ve şifrenin aynı olması	19	50	19	50	39	100
	Şifrede kişisel isim kullanımı	106	69,3	47	30,7	153	100
	Şifrede bölüm adı kullanımı	20	64,5	11	35,5	31	100
	Şifrede hastane adı kullanımı	15	50	15	50	30	100
	Sayı ve harfin bir arada kullanımı	153	66,2	78	33,8	231	100
Hastaya ait bilgilerin paylaşımı için onam formu alınması	Onam formu alınıyor	162	60,7	105	39,3	267	100
	Onam formu alınmıyor	75	67	37	33	112	100
	Cevapsız	21	46,7	24	53,3	45	100
HBYS de hasta bilgileri için yapılabilen işlemler*	Okuma	225	62,8	133	37,2	358	100
	Yazma	183	63,1	107	36,9	290	100
	Silme	66	55	54	45	120	100
	Gönderme	53	49,1	55	50,9	108	100
	Değiştirme	64	53,3	56	46,7	120	100
	Kopyalama	48	53,9	41	46,1	89	100
	Ekleme	59	51,3	56	48,7	115	100

HBYS’nde erişilebilen hasta bilgileri*	Kimlik bilgileri	239	60,7	155	39,3	394	100
	İletişim bilgileri	230	61,5	144	38,5	374	100
	Hastalık bilgileri	220	65,5	116	34,5	336	100
	Tıbbi raporlar	200	69,2	89	30,8	289	100
	Tetkik sonuçları	213	63,6	122	36,4	335	100
	Önceden aldığı tıbbi hizmet bilgileri	163	65,5	86	34,5	249	100
	Ödeme bilgileri	48	33,3	96	66,7	144	100
	Sigorta bilgileri	52	38,8	82	61,2	134	100
Bilgi güvenliğini artırmak için alınabilecek önlemler*	Anti-virüs programlarının kullanımı	171	65,8	89	34,2	260	100
	Yazılım ve donanımın ihtiyaca göre güncellenmesi	154	66,7	77	33,3	231	100
	Şifre kullanımı	191	62,2	116	37,8	307	100
	Bilgisayarda kişisel usb kullanımının engellenmesi	116	69	52	31	147	100
	Bilgisayarı çalışanlar dışında kişilerin kullanmaması	157	64,1	88	35,9	245	100
	Çalışanın birimden ayrılırken bilgisayarını kapatması	172	66,9	85	33,1	257	100
	Şifrenin kesinlikle paylaşılmaması	202	64,7	110	35,3	312	100
	Şifrenin uygun kalitede seçiminin sağlanması	135	62,8	80	37,2	215	100

* Bu sorularda araştırma grubu tarafından birden fazla seçenek işaretlenmiştir.

Araştırmaya katılan tıbbi ve idari birim çalışanlarının bilgi güvenliği kazalarına bakışı değerlendirildiğinde, bilgi güvenliği ile ilgili yaşanan kazaların nedenlerinin duyurulmasını isteme konusunda, tıbbi ve idari birim çalışanları arasında anlamlı bir farklılık olduğu görülmektedir. İdari birimde bilgi güvenliği kazalarının duyurulmasını isteme oranının daha yüksek olduğu belirlenmiştir ($p = 0.02$) (Tablo 8).

Tablo 8: Araştırmaya katılan tıbbi ve idari birim çalışanlarının bilgi güvenliği kazalarına bakışları

		Tıbbi birimler		İdari birimler		p*
		n	%	n	%	
Bilgi güvenliği ile ilgili yaşanan kazaların nedenlerinin duyurulmasını isteme durumu	Duyurulmasını isteyen	187	72,5	140	84,3	0,02
	Duyurulmasını istemeyen	61	23,6	25	15,1	
	Cevapsız	10	3,9	1	0,6	
	Toplam	258	100	166	100	

* Ki-kare testi kullanılmıştır.

Tablo 9: Araştırmaya katılan tıbbi ve idari birim çalışanlarına göre bilgi güvenliği kazalarının duyurulma ve farkındalık sağlama yöntemleri

		Tıbbi birimler		İdari birimler		Toplam	
		n	%	n	%	n	%
Bilgi güvenliği konusunda yaşanan kazaların duyurulma yöntemlerinin tercihi	Sms ile mesaj gönderilmesi	120	71	49	29	169	100
	E-posta gönderilmesi	71	49,3	73	50,7	144	100
	E-konferans ile bildirilmesi	34	68	16	32	50	100
	Haber verilmemesi	11	61,1	7	38,9	18	100
Bilgi güvenliği konusunda farkındalığı artırmak için yapılabilecek uygulamalar	Eğitici poster hazırlanması	92	60,5	60	39,5	152	100
	Sms ile hatırlatıcı mesaj gönderilmesi	45	69,2	20	30,8	60	100
	HBYS üzerinden hatırlatıcı e-posta gönderilmesi	72	59,5	49	40,5	121	100
	E-konferans düzenlenmesi	32	58,2	23	41,8	55	100

Araştırmaya katılan tıbbi ve idari birim çalışanlarının bilgi güvenliği kazalarının duyurulma ve farkındalığına bakışları açısından değerlendirildiğinde, tıbbi birimler tarafından, bilgi güvenliği kazalarının duyurulması için sms ile mesaj gönderilmesi (% 71) ve e-konferans ile bildirilmesi (% 68), idari birimler tarafından ise e-posta gönderilmesi ise (% 50,7) öncelikli yöntemler olarak tercih edilmiştir. Bilgi güvenliği konusunda farkındalığı artırmak için yapılabilecek uygulamalarda, tüm parametrelerde grupların kendi içlerinde benzerlik gösterdiği görülmektedir (Tablo 9).

Araştırmaya katılan tıbbi ve idari birim çalışanlarına göre güvenlik politikası boyutu değerlendirildiğinde, tıbbi ve idari birim çalışanları arasında bilgi güvenliğinin sağlanması için görev ve sorumlulukların net olarak tanımlanması ile ilgili maddenin, tıbbi birimlere ait puanın idari birimlere göre anlamlı şekilde yüksek olduğu görülmektedir ($p = 0.047$). Bilgi güvenliğine ilişkin yazılı politikalar vardır ifadesine, tıbbi birim çalışan puanının idari birim çalışan puanına göre daha yüksek olmasına rağmen anlamlı farklılığa ulaşamamıştır ($p = 0.054$). Diğer maddelerde de anlamlı farklılık tespit edilememiştir (Tablo 10).

Tablo 10: Araştırmaya katılan tıbbi ve idari birim çalışanlarına göre güvenlik politikası boyutu

	Tıbbi birimler		İdari birimler		p*
	Ortalama puan	Standart sapma	Ortalama puan	Standart sapma	
Bilgi güvenliğinin sağlanması için görev ve sorumluluklar net olarak tanımlanmıştır.	3,49	0,82	3,31	0,97	0.047
Bilgi güvenliğine ilişkin yazılı politikalar vardır.	3,45	0,85	3,28	0,99	0.054
Çalışanlar bilgi güvenliği politikalarından haberdardır.	3,25	0,93	3,22	1,04	0.803
Çalışanlara yeterli ve uygun bilgi güvenliği eğitimi verilmektedir.	3,16	0,92	3,09	1,08	0.472

* Eşleşmemiş T testi kullanılmıştır.

Araştırmaya katılan tıbbi ve idari birim çalışanlarına göre örgütsel güvenlik boyutu değerlendirildiğinde, tıbbi ve idari çalışanlar arasında arasında anlamlı bir farklılık bulunamamıştır ($p > 0.05$) (Tablo 11).

Tablo 11: Araştırmaya katılan tıbbi ve idari birim çalışanlarına göre örgütsel güvenlik boyutu

	Tıbbi birimler		İdari birimler		p*
	Ortalama puan	Standart sapma	Ortalama puan	Standart sapma	
Yöneticiler bilgi güvenliğinin uygulanması konusunda sorumluluk sahibidir.	3,71	0,83	3,6	0,98	0.212
Hastane içinde bilgi güvenliği konusunda bir uzman vardır.	3,46	0,91	3,27	1,04	0.500
Bilgi güvenliğinin sağlanması için çalışanlar gerekli özeni gösterir.**	3,37	0,83	3,34	1,07	0.189
Yöneticiler bilgi güvenliğine gereken özeni gösterir.**	3,56	0,89	3,63	0,93	0.477
Çalışanlar sistemde izin verilen ve onaylanmayan uygulamalar konusunda bilgilidir.	3,44	0,96	3,45	1,03	0.885

* Eşleşmemiş T testi kullanılmıştır.

** Araştırmacı tarafından bilgi güvenliği ile ilgili eklenen sorulardır.

Araştırmaya katılan tıbbi ve idari birim çalışanlarına göre güvenlik uygulamaları boyutu değerlendirildiğinde, tıbbi ve idari çalışanlar arasında, çalışanlar çalışma alanlarından uzaklaştıklarında bilgisayarlarını güvenli bir şekilde bırakmaları konusunda eğitilmişlerdir görüşünde idari birimlere ait puanın tıbbi birimlere göre ($p = 0.036$), bilgi güvenliği uzmanı olmadığında dışarıdan danışmanlık hizmeti alındığı görüşünde ise tıbbi birimlere ait puanın idari birimlere göre anlamlı şekilde yüksek olduğu görülmektedir ($p = 0.038$) (Tablo 12).

Tablo 12: Araştırmaya katılan tıbbi ve idari birim çalışanlarına göre güvenlik uygulamaları boyutu

	Tıbbi birimler		İdari birimler		p*
	Ortalama puan	Standart sapma	Ortalama puan	Standart sapma	
Çalışanlar güvenlik ihlali olaylarının derhal yönetime bildirilmesi gerektiğini bilirler.	3,54	0,95	3,62	1,04	0.411
Çalışanlar çalışma alanlarından uzaklaştıklarında bilgisayarlarını güvenli bir şekilde bırakmaları konusunda eğitilmişlerdir.	3,53	0,97	3,75	1,07	0.036
Güvenlik ihlalleri için çalışanlara yönelik disiplin uygulamaları vardır.	3,38	0,99	3,41	1,22	0.828
Bilgi güvenliği uzmanı olmadığında dışarıdan danışmanlık hizmeti alınır.	3,27	1,05	3,04	1,13	0.038
Sistem arızalarında ya da hırsızlık durumlarında veri yedekleri bilgilerin geri kazanılmasını sağlar.	3,63	0,94	3,52	1,1	0.303

* Eşleşmemiş T testi kullanılmıştır.

Araştırmaya katılan tıbbi ve idari birim çalışanlarına göre erişim ve yetkilendirme boyutu değerlendirildiğinde, tıbbi ve idari çalışanlar arasında anlamlı bir farklılık bulunamamıştır ($p > 0.05$) (Tablo 13).

Tablo 13: Araştırmaya katılan tıbbi ve idari birim çalışanlarına göre erişim ve yetkilendirme boyutu

	Tıbbi birimler		İdari birimler		p*
	Ortalama puan	Standart sapma	Ortalama puan	Standart sapma	
Sistemler herhangi bir arıza oluşmadan, belli bir plan doğrultusunda sürekli güncellenir.	3,59	0,9	3,42	1,04	0.088
Bir güvenlik ihlali oluştuğunda yapılacaklar ve yardım için kimin aranacağı bilinir.	3,67	0,94	3,52	1,03	0.142
Anti-virüs sistemi günceldir ve sistemi en iyi şekilde korur.	3,59	0,9	3,67	0,95	0.397
Halka açık ağlara bağlı olmasına rağmen sistemler yeterince korunmaktadır.	3,65	0,89	3,53	0,99	0.205
Kullanıcıların sistemde oturum açmasına yetki verecek uygun mekanizmalar vardır.	3,96	3,32	3,67	1,04	0.266
Çalışanlar, yetkilendirme yapılmadan sisteme erişemez.	3,87	0,93	3,95	0,98	0.408
Şifre yönetim sistemi bulunmaktadır.	3,54	1,07	3,6	1,07	0.566
Kullanıcıların hangi verilere erişebileceğini belirleyen bir yetkilendirme prosedürü vardır.	3,7	0,98	3,74	0,97	0.750
Bilgi işlem uygulamaları sadece yetkilendirilmiş iş amaçları için kullanılır.	3,8	0,94	3,78	1,07	0.884

* Eşleşmemiş T testi kullanılmıştır.

Araştırmaya katılan tıbbi ve idari birim çalışanlarına göre hizmet sunumu boyutu değerlendirildiğinde, tıbbi ve idari çalışanlar arasında, iş yükünün fazla oluşunun bilgi güvenliğine gereken önemin verilmesini engellemediği görüşünde, idari birimlere ait puanın tıbbi birimlere göre anlamlı şekilde yüksek olduğu görülmektedir ($p=0.010$). Bilgi güvenliği süreçlerinin sunulan hizmet kalitesini olumsuz yönde etkilemediği ($p=0.000$), bilgi güvenliğinin öncelikli bir konu olduğu ($p=0.023$) ve iş akışındaki değişikliklerin bilgi güvenliğine gereken önemi vermeyi engellemediği görüşlerinde de ($p=0.007$) idari birimlere ait puanın tıbbi birimlere göre anlamlı şekilde yüksek olduğu görülmektedir (Tablo 14).

Tablo 14: Araştırmaya katılan tıbbi ve idari birim çalışanlarına göre hizmet sunumu boyutu

	Tıbbi birimler		İdari birimler		p*
	Ortalama puan	Standart sapma	Ortalama puan	Standart sapma	
İş yükünün fazla oluşu bilgi güvenliğine gereken önemin verilmesini engellemez.	2,87	1,36	3,21	1,27	0.010
Bilgi güvenliği süreçleri hizmet kalitesini olumsuz etkilemez.	2,49	1,24	2,95	1,22	0.000
Bilgi güvenliği öncelikli bir konudur.	2,46	1,27	2,76	1,32	0.023
İş akışındaki değişiklikler bilgi güvenliğine gereken önemi vermeyi engellemez.	2,59	1,28	2,92	1,14	0.007

* Eşleşmemiş T testi kullanılmıştır.

Bilgi güvenliği alt boyutlarına ait ortalama puanlar incelendiğinde en yüksek ortalamanın erişim ve yetkilendirme boyutunda, en düşük ortalamanın ise hizmet sunum boyutunda olduğu görülmektedir (Tablo 15).

Tablo 15: Araştırma grubunda bilgi güvenliği alt boyutlarına ait puan ortalamaları

	Ortalama puan	Standart sapma
Erişim ve yetkilendirme boyutu puanı (n=424)	3,675	0,727
Örgütsel güvenlik boyutu puanı (n=424)	3,503	0,714
Güvenlik uygulamaları boyutu puanı (n=424)	3,468	0,771
Güvenlik politikası boyutu puanı (n=424)	3,294	0,754
Hizmet sunumu boyutu puanı (n=424)	3,254	1,118
Toplam puan (n=424)	3,486	0,572

Alt boyut puanlarının hem birbirleri ile hem de toplam puan ile ilişkili olduğu belirlenmiştir. Erişim ve yetkilendirme boyutunun, güvenlik uygulamaları boyutu, hizmet sunumu boyutu, örgütsel güvenlik boyutu, güvenlik politikası boyutu ve toplam puan ile ilişkili olduğu belirlenmiştir. En kuvvetli ilişkinin ise toplam puan ile arasında olduğu tespit edilmiştir. Güvenlik uygulamaları boyutunun, örgütsel güvenlik boyutu, güvenlik politikası boyutu ve toplam puan ile, hizmet sunumu boyutunun güvenlik politikası boyutu ve toplam puan ile, örgütsel güvenlik boyutunun güvenlik politikası boyutu ve toplam puan ile, güvenlik politikası boyutunun da toplam puan ile ilişkili olduğu görülmüştür. Toplam puanı ise en çok, erişim ve yetkilendirme boyutunun etkilediği tespit edilmiştir. Ancak erişim ve yetkilendirme boyutu ile hizmet sunumu boyutu arasında ($r = 0.137$) ve hizmet sunumu boyutu ile güvenlik politikası boyutu arasında ($r = 0.103$) anlamlı kabul edilemeyecek düzeyde zayıf korelasyon ilişkisi tespit edilmiştir (Tablo 16).

Tablo 16: Araştırma grubunda bilgi güvenliği alt boyut puanları arasındaki ilişkiler

	r	p
Erişim ve yetkilendirme boyutu puanı –		
Güvenlik uygulamaları boyutu puanı	0,653	0.000
Erişim ve yetkilendirme boyutu puanı -		
Hizmet sunumu boyutu puanı	0,137	0.005
Erişim ve yetkilendirme boyutu puanı -		
Örgütsel güvenlik boyutu puanı	0,574	0.000
Erişim ve yetkilendirme boyutu puanı -		
Güvenlik politikası boyutu puanı	0,522	0.000
Erişim ve yetkilendirme boyutu puanı -		
Toplam puan	0,860	0.000
Güvenlik uygulamaları boyutu puanı -		
Hizmet sunumu boyutu puanı	0,064	0.187
Güvenlik uygulamaları puanı - Örgütsel		
güvenlik boyutu puanı	0,643	0.000
Güvenlik uygulamaları boyutu puanı -		
Güvenlik politikası boyutu puanı	0,537	0.000
Güvenlik uygulamaları boyutu puanı -		
Toplam puan	0,790	0.000
Hizmet sunumu boyutu puanı -		
Örgütsel güvenlik boyutu puanı	0,086	0.078
Hizmet sunumu boyutu puanı -		
Güvenlik politikası boyutu puanı	0,103	0.034
Hizmet sunumu boyutu puanı -		
Toplam puan	0,400	0.000
Örgütsel güvenlik boyutu puanı –		
Güvenlik politikası boyutu puanı	0,594	0.000
Örgütsel güvenlik boyutu puanı –		
Toplam puan	0,770	0.000
Güvenlik politikası boyutu puanı -		
Toplam puan	0,710	0.000

Bilgi güvenliği alt boyutları ile araştırma grubunun yaşları arasındaki ilişki değerlendirildiğinde, anlamlı bir farklılık bulunamamıştır ($p > 0.05$) (Tablo 17).

Tablo 17: Araştırma grubunda bilgi güvenliği alt boyutları ile yaş arasındaki ilişki

	Yaş	Ortalama puan	Standart sapma	p
Erişim ve yetkilendirme boyutu puanı	30 yaş ve altı (n=275)	3,685	0,679	0.483
	31-40 yaş (n=97)	3,757	0,797	
	41 yaş ve üzeri (n=36)	3,694	0,718	
Güvenlik uygulamaları boyutu puanı	30 yaş ve altı (n=275)	3,493	0,730	0.376
	31-40 yaş (n=97)	3,480	0,838	
	41 yaş ve üzeri (n=36)	3,305	0,768	
Hizmet sunumu boyutu puanı	30 yaş ve altı (n=275)	3,213	1,130	0.067
	31-40 yaş (n=97)	3,510	1,103	
	41 yaş ve üzeri (n=36)	3,166	1,062	
Örgütsel güvenlik boyutu puanı	30 yaş ve altı (n=275)	3,512	0,677	0.965
	31-40 yaş (n=97)	3,534	0,803	
	41 yaş ve üzeri (n=36)	3,511	0,721	
Güvenlik politikası boyutu puanı	30 yaş ve altı (n=275)	3,308	0,729	0.596
	31-40 yaş (n=97)	3,350	0,768	
	41 yaş ve üzeri (n=36)	3,201	0,859	
Toplam puan	30 yaş ve altı (n=275)	3,492	0,529	0.294
	31-40 yaş (n=97)	3,567	0,652	
	41 yaş ve üzeri (n=36)	3,404	0,601	

Bilgi güvenliği alt boyutları ile araştırma grubunun kurumda çalışma süreleri arasındaki ilişki değerlendirildiğinde, yalnızca hizmet sunumu boyutunda anlamlı bir farklılık bulunmuştur ($p = 0.007$). Bu farkın kurumda 12 ay ve altı çalışanlar ile 13 – 48 ay arası çalışanlar arasında olduğu belirlenmiştir ($p = 0.006$) (Tablo 18).

Tablo 18: Araştırma grubunda bilgi güvenliği alt boyutları ile çalışma süresi arasındaki ilişki

	Çalışma süresi	Ortalama puan	Standart sapma	p
Erişim ve yetkilendirme boyutu puanı	12 ay ve altı (n=128)	3,721	0,713	0.307
	13-48 ay (n=224)	3,627	0,722	
	49 ay ve üzeri (n=71)	3,755	0,767	
Güvenlik uygulamaları boyutu puanı	12 ay ve altı (n=128)	3,539	0,750	0.242
	13-48 ay (n=224)	3,469	0,792	
	49 ay ve üzeri (n=71)	3,346	0,741	
Hizmet sunumu boyutu puanı	12 ay ve altı (n=128)	2,998	1,112	0.007*
	13-48 ay (n=224)	3,377	1,132	
	49 ay ve üzeri (n=71)	3,345	1,012	
Örgütsel güvenlik boyutu puanı	12 ay ve altı (n=128)	3,571	0,787	0.443
	13-48 ay (n=224)	3,476	0,681	
	49 ay ve üzeri (n=71)	3,470	0,679	
Güvenlik politikası boyutu puanı	12 ay ve altı (n=128)	3,429	0,786	0.052
	13-48 ay (n=224)	3,245	0,722	
	49 ay ve üzeri (n=71)	3,211	0,779	
Toplam puan	12 ay ve altı (n=128)	3,509	0,599	0.873
	13-48 ay (n=224)	3,476	0,559	
	49 ay ve üzeri (n=71)	3,485	0,568	

* ≤ 12 ay - 13-48 ay $p = 0.006$

Bilgi güvenliği alt boyutları ile araştırma grubunun eğitim durumları arasındaki ilişki değerlendirildiğinde, anlamlı bir farklılık bulunamamıştır ($p > 0.05$) (Tablo 19).

Tablo 19: Araştırma grubunda bilgi güvenliği alt boyutları ile eğitim durumu arasındaki ilişki

	Eğitim durumu	Ortalama puan	Standart sapma	p
Erişim ve yetkilendirme boyutu puanı	Lise (n=156)	3,616	0,714	0.423
	Ön lisans (n=69)	3,684	0,730	
	Lisans / Lisansüstü (n=199)	3,718	0,737	
Güvenlik uygulamaları boyutu puanı	Lise (n=156)	3,494	0,738	0.400
	Ön lisans (n=69)	3,553	0,741	
	Lisans / Lisansüstü (n=199)	3,419	0,806	
Hizmet sunumu boyutu puanı	Lise (n=156)	3,128	1,171	0.098
	Ön lisans (n=69)	3,184	1,106	
	Lisans / Lisansüstü (n=199)	3,376	1,071	
Örgütsel güvenlik boyutu puanı	Lise (n=156)	3,528	0,702	0.666
	Ön lisans (n=69)	3,542	0,706	
	Lisans / Lisansüstü (n=199)	3,470	0,728	
Güvenlik politikası boyutu puanı	Lise (n=156)	3,298	0,769	0.874
	Ön lisans (n=69)	3,333	0,717	
	Lisans / Lisansüstü (n=199)	3,278	0,759	
Toplam puan	Lise (n=156)	3,458	0,536	0.738
	Ön lisans (n=69)	3,507	0,576	
	Lisans / Lisansüstü (n=199)	3,501	0,600	

Bilgi güvenliği alt boyutları ile araştırma grubunun HBYS eğitimi alma durumları arasındaki ilişki değerlendirildiğinde, tüm boyutlarda eğitim almayanlara göre puanların daha yüksek olduğu belirlenmiştir ($p < 0.05$) (Tablo 20).

Tablo 20: Araştırma grubunda bilgi güvenliği alt boyutları ile HBYS eğitimi alma durumu arasındaki ilişki

	HBYS eğitimi alma durumu	Ortalama puan	Standart sapma	P
Erişim ve yetkilendirme boyutu puanı	Eğitim almış (n=312)	3,789	0,676	0.000
	Eğitim almamış (n=99)	3,344	0,771	
Güvenlik uygulamaları boyutu puanı	Eğitim almış (n=312)	3,576	0,739	0.000
	Eğitim almamış (n=99)	3,155	0,796	
Hizmet sunumu boyutu puanı	Eğitim almış (n=312)	3,347	1,156	0.001
	Eğitim almamış (n=99)	2,964	0,981	
Örgütsel güvenlik boyutu puanı	Eğitim almış (n=312)	3,603	0,698	0.000
	Eğitim almamış (n=99)	3,236	0,704	
Güvenlik politikası boyutu puanı	Eğitim almış (n=312)	3,379	0,731	0.000
	Eğitim almamış (n=99)	3,053	0,798	
Toplam puan	Eğitim almış (n=312)	3,589	0,538	0.000
	Eğitim almamış (n=99)	3,190	0,580	

Bilgi güvenliği alt boyut puanlarında HBYS eğitimi alma durumuna göre, tıbbi ve idari birimlerde farklılık olup olmadığına bakıldığında, tıbbi birimlerde tüm alt boyut puanları ve toplam puan ortalamalarının, HBYS eğitimi alanlarda yüksek olduğu görülmektedir ($p < 0.05$). İdari birimlerde ise hizmet sunumu boyutu ve güvenlik politikası alt boyut puanlarında bu farklılık görülmemiştir ($p > 0.05$). Ancak diğer boyutlarda farklılık gözlemlenmiştir ($p < 0.05$) (Tablo 21).

Tablo 21: Tıbbi ve idari birimlerde bilgi güvenliği alt boyutları ile HBYS eğitimi alma arasındaki ilişki

Çalışma pozisyonu		HBYS eğitimi alma durumu	Ortalama puan	Standart sapma	p
Tıbbi birim	Erişim ve yetkilendirme boyutu puanı	Eğitim almış (n=203)	3,788	0,64879	0.000
		Eğitim almamış (n=49)	3,337	0,73070	
	Güvenlik uygulamaları boyutu puanı	Eğitim almış (n=203)	3,553	0,70136	0.001
		Eğitim almamış (n=49)	3,167	0,72841	
	Hizmet sunumu boyutu puanı	Eğitim almış (n=203)	3,525	1,15302	0.000
		Eğitim almamış (n=49)	2,862	0,99224	
	Örgütsel güvenlik boyutu puanı	Eğitim almış (n=203)	3,609	0,68151	0.001
		Eğitim almamış (n=49)	3,265	0,57211	
	Güvenlik politikası boyutu puanı	Eğitim almış (n=203)	3,428	0,671	0.000
		Eğitim almamış (n=49)	2,994	0,802	
	Toplam puan	Eğitim almış (n=203)	3,619	0,514	0.000
		Eğitim almamış (n=49)	3,171	0,531	
İdari birim	Erişim ve yetkilendirme boyutu puanı	Eğitim almış (n=109)	3,792	0,728	0.001
		Eğitim almamış (n=50)	3,351	0,816	
	Güvenlik uygulamaları boyutu puanı	Eğitim almış (n=109)	3,620	0,806	0.001
		Eğitim almamış (n=50)	3,144	0,864	
	Hizmet sunumu boyutu puanı	Eğitim almış (n=109)	3,016	1,094	0.787
		Eğitim almamış (n=50)	3,065	0,969	
	Örgütsel güvenlik boyutu puanı	Eğitim almış (n=109)	3,592	0,733	0.004
		Eğitim almamış (n=50)	3,208	0,819	
	Güvenlik politikası boyutu puanı	Eğitim almış (n=109)	3,286	0,828	0.208
		Eğitim almamış (n=50)	3,110	0,797	
	Toplam puan	Eğitim almış (n=109)	3,533	0,578	0.002
		Eğitim almamış (n=50)	3,2081	0,629	

Bilgi güvenliği alt boyutları ile araştırma grubunun cinsiyetleri arasındaki ilişki değerlendirildiğinde, anlamlı bir farklılık bulunamamıştır ($p > 0.05$) (Tablo 22).

Tablo 22: Bilgi güvenliği alt boyutları ile cinsiyet arasındaki ilişki

	Cinsiyet	Ortalama puan	Standart sapma	P
Erişim ve yetkilendirme boyutu puanı	Erkek (n=158)	3,725	0,760	0.281
	Kadın (n=266)	3,646	0,707	
Güvenlik uygulamaları boyutu puanı	Erkek (n=158)	3,503	0,740	0.473
	Kadın (n=266)	3,448	0,790	
Hizmet sunumu boyutu puanı	Erkek (n=158)	3,371	1,079	0.095
	Kadın (n=266)	3,184	1,136	
Örgütsel güvenlik boyutu puanı	Erkek (n=158)	3,526	0,698	0.606
	Kadın (n=266)	3,489	0,724	
Güvenlik politikası boyutu puanı	Erkek (n=158)	3,321	0,746	0.586
	Kadın (n=266)	3,279	0,760	
Toplam puan	Erkek (n=158)	3,535	0,579	0.178
	Kadın (n=266)	3,457	0,567	

Bilgi güvenliği alt boyutları ile araştırma grubunun yer aldıkları kadro arasındaki ilişki değerlendirildiğinde, anlamlı bir farklılık bulunamamıştır ($p > 0.05$) (Tablo 23).

Tablo 23: Bilgi güvenliği alt boyutları ile kurumdaki kadro türleri arasındaki ilişkiler

	Kadro türü	Ortalama puan	Standart sapma	p
Erişim ve yetkilendirme boyutu puanı	Tıbbi kadro (n=249)	3,707	0,739	0.425
	İdari kadro (n=157)	3,616	0,726	
	Yönetici kadro (n=18)	3,675	0,554	
Güvenlik uygulamaları boyutu puanı	Tıbbi kadro (n=249)	3,517	0,786	0.303
	İdari kadro (n=157)	3,397	0,757	
	Yönetici kadro (n=18)	3,422	0,664	
Hizmet sunumu boyutu puanı	Tıbbi kadro (n=249)	3,305	1,132	0.289
	İdari kadro (n=157)	3,149	1,070	
	Yönetici kadro (n=18)	3,458	1,306	
Örgütsel güvenlik boyutu puanı	Tıbbi kadro (n=249)	3,522	0,721	0.504
	İdari kadro (n=157)	3,493	0,723	
	Yönetici kadro (n=18)	3,322	0,509	
Güvenlik politikası boyutu puanı	Tıbbi kadro (n=249)	3,277	0,795	0.646
	İdari kadro (n=157)	3,305	0,713	
	Yönetici kadro (n=18)	3,444	0,489	
Toplam puan	Tıbbi kadro (n=249)	3,514	0,593	0.406
	İdari kadro (n=157)	3,437	0,553	
	Yönetici kadro (n=18)	3,522	0,407	

Bilgi güvenliği alt boyutları ile araştırma grubunun meslekleri arasındaki ilişki değerlendirildiğinde, anlamlı bir farklılık bulunamamıştır ($p > 0.05$) (Tablo 24).

Tablo 24: Bilgi güvenliği alt boyutları ile meslek grupları arasındaki ilişkiler

	Meslek grubu	Ortalama puan	Standart sapma	p
Erişim ve yetkilendirme boyutu puanı	Hekim (n=63)	3,673	0,665	0.314
	Hemşire (n=87)	3,624	0,714	
	Diğer sağlık çalışanları (n=99)	3,801	0,799	
	Operasyonel birimler (n=131)	3,586	0,745	
	Diğer idari çalışanlar (n=26)	3,765	0,609	
	Yöneticiler (n=18)	3,753	0,554	
Güvenlik uygulamaları boyutu puanı	Hekim (n=63)	3,507	0,734	0.111
	Hemşire (n=87)	3,370	0,746	
	Diğer sağlık çalışanları (n=99)	3,652	0,835	
	Operasyonel birimler (n=131)	3,381	0,760	
	Diğer idari çalışanlar (n=26)	3,476	0,752	
	Yöneticiler (n=18)	3,422	0,664	
Hizmet sunumu boyutu puanı	Hekim (n=63)	3,591	1,052	0.136
	Hemşire (n=87)	3,186	1,011	
	Diğer sağlık çalışanları (n=99)	3,227	1,255	
	Operasyonel birimler (n=131)	3,171	1,088	
	Diğer idari çalışanlar (n=26)	3,038	0,986	
	Yöneticiler (n=18)	3,458	1,306	
Örgütsel güvenlik boyutu puanı	Hekim (n=63)	3,457	0,586	0.49
	Hemşire (n=87)	3,471	0,700	
	Diğer sağlık çalışanları (n=99)	3,610	0,810	
	Operasyonel birimler (n=131)	3,473	0,752	
	Diğer idari çalışanlar (n=26)	3,592	0,558	
	Yöneticiler (n=18)	3,322	0,509	
Güvenlik politikası boyutu puanı	Hekim (n=63)	3,226	0,657	0.484
	Hemşire (n=87)	3,209	0,837	
	Diğer sağlık çalışanları (n=99)	3,368	0,835	
	Operasyonel birimler (n=131)	3,276	0,749	
	Diğer idari çalışanlar (n=26)	3,451	0,479	
	Yöneticiler (n=18)	3,444	0,489	
Toplam puan	Hekim (n=63)	3,524	0,465	0.263
	Hemşire (n=87)	3,422	0,556	
	Diğer sağlık çalışanları (n=99)	3,589	0,685	
	Operasyonel birimler (n=131)	3,420	0,562	
	Diğer idari çalışanlar (n=26)	3,525	0,508	
	Yöneticiler (n=18)	3,522	0,407	

Bilgi güvenliği alt boyutları ile araştırma grubunda yöneticiler ve diğer çalışanlar değerlendirildiğinde, anlamlı bir farklılık bulunamamıştır ($p > 0.05$) (Tablo 25).

Tablo 25: Bilgi güvenliği alt boyutları ile yöneticiler ve diğer çalışanlar arasındaki ilişkiler

		Ortalama puan	Standart sapma	p
Erişim ve yetkilendirme boyutu puanı	Diğer çalışanlar (n=406)	3,672	0,734	0.493
	Yöneticiler (n=18)	3,753	0,554	
Güvenlik uygulamaları boyutu puanı	Diğer çalışanlar (n=406)	3,470	0,776	0.531
	Yöneticiler (n=18)	3,422	0,664	
Hizmet sunumu boyutu puanı	Diğer çalışanlar (n=406)	3,245	1,110	0.303
	Yöneticiler (n=18)	3,458	1,306	
Örgütsel güvenlik boyutu puanı	Diğer çalışanlar (n=406)	3,511	0,721	0.208
	Yöneticiler (n=18)	3,322	0,509	
Güvenlik politikası boyutu puanı	Diğer çalışanlar (n=406)	3,288	0,764	0.372
	Yöneticiler (n=18)	3,444	0,489	
Toplam puan	Diğer çalışanlar (n=406)	3,484	0,579	0.536
	Yöneticiler (n=18)	3,522	0,407	

Bilgi güvenliği alt boyutları ile araştırma grubunun HBYS kullanım becerisi arasındaki ilişki değerlendirildiğinde, yalnızca erişim ve yetkilendirme boyutu ile anlamlı kabul edilemeyecek düzeyde zayıf korelasyon ilişkisi tespit edilmiştir ($r = 0.14$ $p = 0.004$). Diğer boyutlarda anlamlı bir ilişki tespit edilememiştir.

Araştırma grubunun bilgisayar kullanım becerisi ile HBYS kullanım becerisi arasındaki ilişki değerlendirildiğinde ise, orta dereceli korelasyon ilişkisi gözlemlenmiştir ($r = 0.59$ $p = 0.000$).

7. TARTIŞMA

Bilginin gizliliği, güvenilirliği ve her an kullanıma hazır halde güncel olması; günümüzde tartışmasız olarak kabul edilen rekabet gücünü, yasal yükümlülükleri, verimliliği, kurumsal ve ticari imajı etkin bir şekilde sürdürebilmek ve korumak için gereklidir. Bilgisayar ve internet kullanımının hızla yaygınlaşması sonucu, kurumlar için artan tehditler ve beraberinde getirdiği riskler yüzünden bilgi güvenliği kavramı, bilgi sistemleri alanında günümüzün en önemli konularından biri haline gelmiştir. Önümüzdeki yıllarda da bu konunun öneminin artarak süreceği düşünülmektedir. Kurum ve kişisel bilgiler ölçeğinde bilgi güvenliğinin sağlanması; iş kesintilerinden ve bilgi kayıplarından kaçınma, iş sürekliliğinin sağlanması, kurumsal prestijin korunması, kişisel bilgilerin gizliliği ve maddi kayıpların önlenmesi bakımından çok büyük önem taşımaktadır. Bir kurumun sadece teknik önlemler ile bilgi güvenliğini ve iş sürekliliğini sağlamasının mümkün olmadığı, bu teknik önlemlerin yanısıra bilgi güvenliği yönetim sistemi kapsamında kavramsal ve prosedürel bir takım önlem ve denetimlerin sağlanması gerektiği konusu, tüm dünyada kabul edilmiş bir yaklaşımdır (22). Araştırmalar bir kurumun hassas bilgilerini korumaya almada, teknik olmayan sorunların da teknik olanlar kadar önemli olduğunu göstermiştir. Teknik çözümler bilgiyi sadece belli bir yere kadar korur ve bu nedenle güvenliğin insani yönü, tartışılacak büyük bir odak haline gelir (23).

Türkiye’de sağlık bilgilerinin saklanması ve gizliliği ile ilgili çeşitli düzeylerde önemli düzenlemeler yürürlüktedir. Sağlık Hizmetleri Temel Kanunu’nun 3/f hükmüne göre *‘Herkesin sağlık durumunu takip edebilmek için gerekli kayıt ve bildirim sistemi kurulur’*. Sağlık Bakanlığı’nın Sağlık.net uygulaması ve elektronik sağlık kaydı sistemleri bu kapsamda yer alır. Ayrıca Sağlık Hizmetleri Temel Kanunu’nda da, hekimlerin ve diğer sağlık çalışanlarının sorumlulukları ile ilgili hükümler yer alır (38).

Bilgi güvenliği sağlık hizmetlerinin her alanında sağlanması ve korunması gereken bir unsurdur (46).

Hastane bilgi yönetimi sistemi, hastanenin idari ve tıbbi bilgilerinin yönetimini kolaylaştırmak ve verilen hizmetlerin kalitesini artırmak amacı ile düzenlenmiş bir bilgi sistemi olarak tanımlanmaktadır

(http://www.sabiyap.org/makaleler/php?mak_id=9, Özyurt O. Hastane Bilgi Yönetim Sistemlerinin Genel Özellikleri, erişim tarihi 20 Mart 2013).

Bu araştırmada, sağlık hizmetlerinin sunumunda yaygın olarak kullanılan hastane bilgi yönetim sisteminde bilgi güvenliğinin çalışanlar tarafından değerlendirilmesi amaçlanmıştır.

Araştırma grubunun kurumda çalışma süreleri, HBYS kullanımı deneyim süreleri, HBYS eğitimi alma süreleri ve bilgisayar kullanım becerileri değerlendirildiğinde, tıbbi ve idari grupların standart olarak seçildiği görülmektedir. İdari birim çalışanlarında, hem HBYS kullanım becerisi puanının hem de hastane bilgi güvenliği puanının, tıbbi birim çalışanlarına göre daha yüksek olduğu görülmüştür. İdari birim çalışanları süreçlerini yönetebilmeleri için bilgi teknolojilerini aktif olarak kullanmak zorundadırlar. Tıbbi birim çalışanları için ise bu konu, ikincil öneme sahiptir. Bilgi sistemlerinin uygulamaya konulmasında en büyük engel, tıbbi çalışanların, özellikle klinisyenlerin direnç göstermesidir. Bu durum, teknik, kurumsal ya da bireysel nedenlerden dolayı olabilir. Klinik gereksinimleri karşılamada eğer bir sistem başarısız olursa ya da klinisyenler, bilgi teknolojilerini kullandıklarında işlerinin kötüleşeceğine inanırlarsa, yeni teknoloji kullanımına direnç gösterebilir ya da bunu tamamen reddedebilirler (8). Sistemin başarısı kullanıcıların kabulüne bağlıdır. Özellikle tıbbi birim çalışanlarının kullanacağı sistemlerin çoğu ne yazık ki kullanılabilirlik düşüncesi üzerine tasarlanmadığında, kullanıcılar yaşadıkları hayal kırıklığı sonucu, bilgi teknolojileri kullanımını ve sistemi öğrenmeyi ikincil iş olarak görmekte ve bununla bağlantılı olarak da onların güvenlik konusuna gereken önemi de vermedikleri düşünülmektedir (10).

Tıbbi birimde HBYS eğitimi alma durumunun daha yüksek olduğu belirlenmiştir. Tıbbi birim çalışanları için HBYS kullanımı ikincil görev olduğu için, eksikliklerin tamamlanması daha çok önem taşımaktadır. Bu anlamda HBYS kullanımı için eğitime, idari birim çalışanlarına oranla daha çok ihtiyaç

duymaktadırlar. İdari birim çalışanları ise rutin iş süreçlerini bilgisayar üzerinden yürüttükleri için, görevlerini yaparken sistemi kullanmayı da öğrenmektedirler. HBYS kullanımında kullanıcı memnuniyetinin özellikle tıbbi birim çalışanları bakımından sağlanması için bazı önlemler alınabilir. HBYS kullanıcı eğitimlerinin öncelikli konu olarak görülmesi ve erken dönemde başlatılması, kullanıcıların stresini azaltıp sistemin kullanım kabulünü kolaylaştırmaktadır. Sistem kullanıcı dostu oldukça, kullanıcı ihtiyaçlarını daha fazla karşıladıkça, kullanıcı memnuniyeti oluşur (32). Kullanıcı memnuniyetinin artması sonucu iş akış süreçlerinin kalitesi yükselerek, daha etkili sağlık hizmeti sunulabilir (10).

Etkili sağlık hizmeti sunumunda bilgi teknolojileri sayesinde hasta verilerine hızlı ve güvenli şekilde erişilebilmesi de, hasta güvenliğini olumlu yönde etkilemektedir (47).

HBYS’nde erişilen bilgi türlerinde, sigorta şirket bilgilerine ve sosyal güvence bilgilerine ağırlıklı olarak idari birim çalışanları tarafından ulaşıldığı, hastaya ait bilgilerin yanı sıra süreçsel raporlara ulaşımın ise tıbbi birim çalışanlarınca daha yüksek oranda olduğu görülmektedir. Erişim kontrolü ile sadece yetkili kişilerin sisteme girmesi, kişilerin yalnızca kendi iş süreçleri ile ilgili bilgilere ulaşması ve gerektiğinde kullanması sağlanmalıdır (23). Tıbbi birim çalışanlarının iş süreçlerinde kullanacağı tıbbi bilgilerin dışındaki bilgi türlerine de erişimlerinin olduğu belirlenmiştir. Benzer oranlar günlük işleyiş sırasında kullanılan bilgi türlerinde de görülmektedir. Bu durum da, kuruma ait bilgilerin özellikle tıbbi birim çalışanlarından yeterince korunmadığını düşündürmektedir.

Bilgi güvenliği, farkında olunarak ya da olunmadan meydana gelebilecek bilgi kayıplarının, mevcut bilgilerde değişiklik yapılmasının engellenmesi şeklinde tanımlanabilir (23).

Bir kurumda hangi verilere erişimin sağlanacağı ve bu erişimin hangi seviyede olacağı önemlidir. Erişim kriteri olarak en yaygın kullanılan yöntem, rol tabanlı erişim kontrolüdür (56). Sağlık çalışanlarının ise, iş süreçleri dışında bilgilere erişimi üzerinde düşünülmesi gereken bir konudur. Düşünülmesi gereken sorular; ‘sistemde veriye kimlerin erişim yetkisi vardır? sağlık çalışanları ihtiyaç duyduğu verilere erişebilmekte midir?’ olarak belirlenebilir (9). Acil durumlarda kullanıcı verilerine

erişimin nasıl olacağı doğru tanımlanmalıdır (56). Bu noktada idari birim çalışanlarının iş süreçleri ile bağlantılı uygulamalara erişimleri istenilen bir durum iken, sağlık çalışanlarının daha geniş bir erişim platformuna sahip olmaları, bilgi güvenliği açısından ciddi bir sorun oluşturabilir. Bu açıdan sorunların çözümüne yönelik verinin değeri bilinmeli ve verilere erişim açık şekilde tanımlanmalıdır (9).

HBYS üzerinden hasta verilerine erişimin kimler tarafından denetlendiği konusunda cevap vermeyenlerin oranının % 50'nin üzerinde oluşu, HBYS kullanımı, bilgiye erişim ve standart politikalar konusunda çalışanlara gerekli bilginin verilmediğini düşündürmektedir. Bilgi işlem bölümü cevabının % 20'nin altı gibi düşük bir değerde olması da, bu konuda net bir durumun olmadığını göstermektedir. Kurum içinde bir bilgi güvenliği politikasının varlığı, hastane bilgi teknolojileri donanımlarının, bilişim sistemlerinin ve yeni prosedürlerin kullanımı hakkındaki kuralları, bilgi güvenliği ve gizliliği ile ilgili olarak kendi çalışma koşullarını ve kendi yükümlülüklerini tüm çalışanlara hatırlatan dahili bildirim sistemi kurulmalıdır. Bu sistem hastane hakkındaki kısa haber mesajlarını içeren, intranetten ya da basılı olarak dağıtılan dökümanlardan oluşabilir (70).

Bilgi güvenliğinin sağlanması için kimlik belirleme yöntemleri olarak, kullanıcı adı ve şifrenin kullanıldığı görülmüştür. Kullanılan şifre yapıları incelendiğinde, Şifrelerde sayı ve harfin bir arada kullanımı olduğu görülmekle birlikte, özellikle tıbbi birim çalışanlarının büyük oranda birbirini takip eden numaralar, kişisel isim ya da bölüm adı gibi kolay tahmin edilebilecek şifreler kullandığı görülmektedir. Tıbbi birim çalışanlarının karmaşık şekilde şifre kullanmamalarının, karşılıklı olarak duyulan yüksek güvenin sonucu olduğu açıklanmıştır. Her tıbbi çalışanın kendine ait bir şifresi olmasına rağmen, bunların diğer çalışanlardan birinde toplandığı ve ardından ofis alanına asılan bir parça kağıt üzerine yazıldığı da bildirilmiştir (55). Veri koruması ile ilgili temel alanlar; kullanıcı kimliğinin onaylanması, verilerin şifreleme yolu ile güvenlik altına alınması, elektronik verilerin bölümlere ayrılması ve internet güvenliği olarak tanımlanmıştır. Özellikle basit şifreli oturum açma uygulamasının oluşu ciddi bir sorundur. Uzun ve sayı harf kombinasyonundan oluşan şifreler uygulama açısından daha güvenlidir (43).

Elektronik sistemler kimlikleri üç biçimde denetlemektedir: birincisi kişinin bildiği parola ya da kişisel kimlik numarası aracılığı ile denetleme yapılması, ikincisi sistemin manyetik kart gibi bir araç ile denetleme yapması, üçüncüsü ise yeni gelişen bir alan olarak kişinin özellikleri aracılığı ile yani biyometrik yöntemler kullanılarak denetlenmesidir (21).

Yetkili olmayan bir kişi şifrelenmiş dosyaya erişim sağlamak için, kullanıcı adı, şifre ve biyometrik oturum açma basamaklarını geçememelidir. İşin devamlılığı açısından verilere farklı kullanıcıların erişimi gerekiyorsa, uygun yetki seviyeleri düzenlenerek yeni kullanıcı tarafından okunabilir hale getirmek için, dosyanın şifresini açabilen bir yapılanmanın olması uygundur (43).

Hastaya ait bilgilerin paylaşımı için onam formu alınması konusunda araştırma grubunun üçte birinden fazlasının, formun alınmadığını söylediği ya da soruya cevap vermediği görülmüştür. Bu oranın yüksekliği de konuya gereken önemin verilmediğini düşündürmektedir. Hastalara ait bilgilerin paylaşılabilmesi için, hastalardan bilgilendirilmiş onam alınması gereklidir (18). Geleneksel hasta-hekim ilişkisi modelinde bilgilendirilmiş onam, sağlık çalışanının kontrolü altındadır ve sadece bilgi ve bilginin hekim tarafından nasıl açıklandığı ile ilgili değildir. Onamın aynı zamanda hasta kayıtlarına erişim ve bu kayıtların kullanımının onayını da içerdiği unutulmamalıdır (33).

HBYS'nde bulunan hasta bilgilerini silme ve değiştirme yetkilerinin % 50'den fazla bir oranda tıbbi birim çalışanlarında olması, verilerin güvenli saklanması konusunda sıkıntılar olabileceğini düşündürmektedir. Aynı yetkilerin idari birim çalışanlarının yaklaşık üçte birinde olması da, hem hastanedeki mali ve hukuki süreçler açısından, hem de doğru veriye erişim noktasında sorunlar yaratabilir. Bilgi kaynaklarının güvenliğinin sağlanması ile ilgili olarak, bilginin korunmasına dair teknolojik yöntemler etkili olabilir. Bununla birlikte birçok kayıp temelde, teknolojinin eksikliğinden ya da hatalı olmasından dolayı değil, bunun yerine bu teknolojileri kullananlardan ve insanların hatalı davranışlarından dolayı ortaya çıkar (23). Tıbbi bilgi hırsızlığı rahatsız edici ve giderek daha yaygınlaşan bir eğilimdir ve hastaların mali bilgilerini korumakta başarısız olan uygulamalar,

kuruluşların itibarını riske atmakta ve büyük oranda ciddi yasal sorunlara yol açmaktadır (14).

Tıbbi birim çalışanlarının HBYS üzerinde hasta tedavisi ile birebir ilişkili olmayan bazı bilgilere, idari birim çalışanlarına göre daha yüksek oranda ulaştıkları gözlemlenmektedir. Bu durum çalışanların görevlerine uygun olan yetkilendirmenin yapılmadığı anlamına gelebilir. Klinik veri tabanları giderek daha yaygın şekilde geliştirilip uygulamaya konulduğundan, veri gizliliğini koruyan engelleri güçlendirmek için de, klinik veri tabanlarını açan çeşitli teknik, yasal ve siyasi mekanizmaları kapsayan bir dizi öneri benimsenmelidir (42). Amaç; istenmeyen erişimi engellemek, bununla birlikte çalışanların güvenlik engelleri etrafında kısayollar kullanabilmesini sağlayacak kadar da ulaşımı kolaylaştırmaktır (14).

İdari birim çalışanlarının bilgi güvenliğini artırmak için farklı önlem kombinasyonlarını, tıbbi birim çalışanlarının da hem teknik hem de kullanıcı boyutunu düşündükleri görülmüştür. Özellikle şifre kullanımı ve şifrenin kesinlikle paylaşılmaması ilk akla gelen önlemler arasındadır. Önlemlere yönelik verilen cevaplara bakıldığında, tıbbi birimde oranların idari birime göre daha yüksek olduğu görülmüştür. Bilginin korunması gerekliliğindeki bu yüksek oranlar, tıbbi birim çalışanları için hasta mahremiyetini koruma açısından da önemli olabileceği düşünüldüğünde, beklenen bir sonuçtur. Sağlık bilgilerinin gizliliği ve güvenliği kamu, hastalar ve hizmet sağlayıcılar açısından önemli kaygı unsurları olarak bildirilmiştir. Çeşitli çalışmalarda hastalar ve hekimler, yanlış kullanım (suistimal) potansiyelini azaltmak amacı ile sağlık hizmeti çalışanlarının tıbbi kayıtlara erişimini sınırlandırma isteklerini belirtmişlerdir (50).

Bilgi güvenliği ile ilgili yaşanan kazaların nedenlerinin duyurulması konusunu, idari birim çalışanlarının daha yüksek oranda desteklediği görülmektedir. Kuruma ait bilgilerin paylaşılma istenmemesi, öncelikli bilgilerde kurumun mali bilgilerinin de olduğu düşünülürse, kabul edilebilir bir sonuç olabilir. Bilgi güvenliği olayları sıklıkla, kurumsal süreçleri ve operasyonları doğrudan etkilemektedir. Bilgi güvenliği kazalarının sayısı artıp etkisi yaygınlaştıkça, şirketler teknik karşıt önlem sistemlerinden (dahili ağı koruyan güvenlik duvarları) güvenlik yönetimine uzanan geniş bir yelpazede birçok önlemi uygulamaya koymuşlardır

(<http://www.yumpu.com/en/document/view/9533455/information-security-governance-framework-jhu-department-of->, Ohki E, Harada Y, Kawaguchi S, Shiozaki T, Kagawa T. Information Security Governance Framework, erişim tarihi 25 Kasım 2013).

Yaşanan kazaların duyurulması için, farklı iletişim kanallarının kullanılması konusunda bir eğilim olduğu görülmektedir. Tıbbi birim çalışanları hasta bakımı nedeni ile bilgisayar başında daha az vakit geçirebildikleri için, e-posta yerine sms ile duyurulmasını daha fazla tercih etmektedirler. Bu durum sağlık çalışanlarının iş süreçleri düşünüldüğünde beklenebilen bir durumdur.

Bilgi güvenliği konusunda farkındalığı artırmak için çeşitli uygulamalar yapılmasını, tıbbi birim çalışanlarının idari birim çalışanlarına göre daha fazla desteklediği belirlenmiştir. Hasta mahremiyetinin korunması ve etik problemler yaşanmasının önlenmesi konularının, tıbbi birimlerce mesleki açıdan daha öncelikli olduğu düşünülürse, bu beklenen bir sonuçtur.

HBYS kurulumu ile birlikte medikal hataların azaldığı, teşhis doğruluğunun arttığı, sağlık çalışanları arasındaki iş birliğinin artarak verimli hale geldiği ve gereksiz masrafların azaldığı gözlemlenmiştir

(http://www.sabiyap.org/makaleler.php?mak_id=40, Yaman Z. Teletıp ve Bilişim Altyapısı, erişim tarihi 20 Mart 2013).

Sağlık sektörüne özel olarak gizlilik, hasta doktor ilişkisinin temel bir yol göstereni olarak görülür ve doğru tanı konulması, tedavinin kolaylaşması ve ters ilaç etkilerinden kaçınılması için, hastaların kendi doktorları ile bilgi paylaşması gerekmektedir (23).

Yapılan çalışmalarda elektronik sağlık kayıtlarının hastanın, durumu ile ilgili eksiksiz bir özet oluşturduğu, bilgilerine rahatça ulaşılabilirdiği, sistemin hekimlere uygun geri bildirimler sağladığı, bilgi ve iletişim teknoloji sistemlerinin hekimlerin hemşirelere verdiği orderların görüntülenmesine yardım ettiği, hastane bilgi yönetim sistemlerinin hasta kabul çalışanlarının üretkenliğini geliştirdiği ve çalışanların operasyonel ihtiyaçlarını karşıladığı tespit edilmiştir. Tüm bunlar hizmet sunum kalitesini etkileyen önemli unsurlardır (45).

Bir kuruluşun bilgi güvenliği yaklaşımı çalışanın davranışına odaklanmalıdır çünkü kuruluşun başarısı ya da başarısızlığı büyük oranda çalışanlarının gerçekleştirdiği ya da gerçekleştiremediği unsurlara bağlıdır. Bilgi güvenliği farkındalığı kültürü, bilgi varlıkları üzerindeki riskleri minimum seviyeye indirecek ve özellikle bir çalışanın hatalı davranış riskini ve bilgi varlıklarına zarar verici etkileşimini azaltacaktır. Kuruluşlar bilgi güvenliği farkındalığının oluşturulmasında ya da kabul edilebilir bir bilgi güvenliği kültürünün uygulanmasında rehberliğe ihtiyaç duyarlar. Kullanıcılar, güvenlik farkındalığı ve tedbirli davranışları yolu ile kuruluşların, bilgi güvenliği performansında önemli bir rol oynarlar. Kullanıcının bilgi güvenliği deneyimi ve bilgi güvenliği işindeki kişisel rolü değerlendirilebilmektedir (59).

Bilgi güvenliği politikası boyutu değerlendirilirken, tıbbi birim çalışanlarının bilgi güvenliğinin sağlanması için görev ve sorumlulukların net olarak tanımlanmış olması görüşüne verdikleri puanın, idari birim çalışanlarının puanına göre daha yüksek olduğu görülmüştür. Bilgi güvenliğine ilişkin yazılı politikalar olması konusunda da benzer eğilim olmasına rağmen iki grup arasında anlamlı bir farklılık tespit edilmemiştir. Çalışanların bilgi güvenliği politikalarından haberdar oluşu ve çalışanlara yeterli ve uygun bilgi güvenliği eğitiminin verilmesi görüşlerinde de benzer bir dağılım olduğu görülmüştür. Bilgi güvenliği politikası boyutunda, tıbbi birim çalışanlarının farkındalığının idari birim çalışanlarına göre daha fazla olduğu anlaşılmaktadır. Bir modern işletmede, bilgi sistemlerinin ve teknolojilerinin etkili şekilde uygulamaya konulduğunu güvence altına alacak en önemli belgelerden ikisi, stratejik bilgi sistemleri planı ve bilgi güvenliği politikasıdır. Bilgi güvenliği politikası, sistemlerin güvenli bir şekilde geliştirilip çalıştırılmasını sağlayacak bir çerçeve sunar. Çalışanların bilgi teknolojileri güvenlik politikalarına riayet etme niyeti, süreci önemli ölçüde etkiler. Uyumu artırmak amacı ile çalışanların geçmişte sergiledikleri ve otomatik olarak gösterdikleri davranışlarının ele alınması gerekir (59).

Bilgi güvenliği davranışı; bilgi güvenliği politikalarında tanımlanan bilgi güvenliğinin sürdürülmesi için, son kullanıcıların riayet etmesi gereken, ana bilgi güvenliği faaliyetlerinin oluşturduğu bir kümeyi ifade eder (59). Hasta ile ilişkili sağlık hizmeti verilerinin alınmasını, işlenmesini, değiştirilmesini, dağıtımını,

gönderilmesini, depolanmasını ve açıklanmasını yönetecek politikalara ihtiyaç duyulmaktadır (44). Bilgi güvenliği sadece basit bir teknik ya da yasal bir konu değildir. Bu yönergelere uygunluk, büyük oranda sahip oldukları verilerin değerini anlayan sağlık hizmeti çalışanlarına bağlıdır. Bir güvenlik kültürü, sağlık çalışanlarını uygun bilgi teknolojileri politikaları ve prosedürlerini geliştirme konusunda cesaretlendirebilir (55).

Etkili bir sağlık kuruluşu yönetiminde, işletmeyi ve kararları etkileyen en önemli öge kaynağı bilgidir. Bir hastane yönetiminin ve yöneticisinin hedeflerini oluşturabilmesi için gerekli olan bilgi; ölçme, raporlama, değerlendirme ve iyileştirmeyi planlamaktır. Organizasyonlar ancak bu sayede standartlarını geliştirebilir ve iyileştirici faaliyetlerin sürekliliğini mümkün kılabilir (http://www.sabiyap.org/makaleler/php?mak_id=9, Özyurt O. Hastane Bilgi Yönetim Sistemlerinin Genel Özellikleri, erişim tarihi 20 Mart 2013).

Yöneticilerin bilgi teknolojileri kullanımı için değerlendirme yaparak, sistemin kurum kültürüne ve iş akışına uyumlu olduğunu belirtmesi, hem sistemin kabulünü, hem de kullanımını artırır. Tıbbi birim çalışanlarından özellikle hekimlerin, uzmanlık alanlarından kaynaklanan farklı uygulama kültürleri, bilgi teknolojilerini kullanımlarında da farklılık göstermelerine yol açabilir. Yöneticilerin, proaktif yaklaşım içinde süreci yönetme ve hekim kullanıcı kaynaklı problemleri çözebilme açısından, bu farklılıkları göz önünde bulundurmaları yararlı olabilir (35).

Örgütsel güvenlik boyutu değerlendirilirken, yöneticilerin bilgi güvenliğinin uygulanması konusunda sorumluluk sahibi olması, hastanede bilgi güvenliği uzmanı olması, çalışanların ve yöneticilerin bilgi güvenliğine gereken özeni göstermesi ve çalışanların sistemde izin verilen ve onaylanmayan uygulamalar konusunda bilgili olmaları parametrelerinde, grupların görüşlerinin benzer olduğu görülmüştür. Önemli bilgi güvenliği sorunlarının aşağıdakileri içerdiği ileri sürülmüştür: özel bir bilgi teknolojileri güvenliği koordinatörüne duyulan ihtiyaç, felaketten kurtarma planını da içeren yazılı bilgi teknolojisi politikaları, farklı seviyelerdeki elektronik verilere erişimin kontrolü, yedeklerin alınması ve test edilmesi, virüsler ve diğer zararlı yazılımlara karşı korunma, güvenlik duvarının kurulması, donanım ve yazılımın rutin bakımının yapılması, elektronik iletişimin güvenliğinin sağlanması. Bu bilgiler, tek

sayfalık özet kontrol listesini içeren bilgisayar güvenliği yönergelerinin oluşturulmasına yol açmıştır (55).

Bilgi güvenliğinde güvenlik uygulamaları boyutu değerlendirildiğinde, idari birim çalışanlarının çalışma alanlarından uzaklaştırıldığında bilgisayarların güvenli şekilde bırakılması konusunda eğitim alma görüşünü, daha fazla destekledikleri görülmüştür. Araştırma yapılan hastanenin uluslararası akreditasyon sertifikası almış olması, çalışanların bu konuda eğitim almış olduğunu, bununla beraber korumanın gerçekçi olmaktan çok şekilsel olabileceğini düşündürmektedir. Bilgi güvenliği uzmanı olmadığında dışarıdan danışmanlık hizmeti alınması konusunda, tıbbi birim çalışanlarının daha olumlu bir görüşe sahip oldukları görülmektedir. Taşınabilir cihazlar (elde kullanılan cihazlar ve dizüstü bilgisayarlar) ev ya da işte kullanılan masaüstü bilgisayarlardan daha az korunmaktadır, çünkü bu cihazların ameliyathanede, soyunma odasında ya da hasta odasında kaybedilmesi, çalınması ya da kullanıma açık şekilde bırakılması daha olasıdır (43). Birçok bilgi güvenliği uzmanı, iyi kullanıcı davranışlarını desteklerken, son kullanıcıların istenmeyen davranışlarını engellemenin, kuruluşlar içerisinde bilgi güvenliğini etkili kılmak için önemli bir yöntem olabileceğine inanmaktadır. Son kullanıcının güvenlik ile ilgili davranışlarının önemi nedeni ile sergiledikleri farklı türdeki davranışlara odaklanan sistematik bir bakış açısı, yöneticilere, denetçilere, bilgi teknolojisi uzmanlarına ve son kullanıcı davranışlarının değerlendirilmesi ve/veya etkilenmesi ile ilgilenen diğer uzmanlara fayda sağlayabilir (59).

Çalışanlara göre bilgi güvenliğinde erişim ve yetkilendirme boyutu değerlendirildiğinde, sistemlerin herhangi bir arıza oluşmadan belirli plan içinde sürekli güncellenmesi, bir güvenlik ihlali oluştuğunda yapılacakların ve kimin aranacağını bilmesi, anti-virüs sisteminin güncel olması, sistemlerin yeterince korunması, kullanıcıların sistemde oturum açmasına yetki verecek uygun mekanizmaların oluşu, yetkilendirme yapılmadan sisteme erişilememesi, şifre yönetim sisteminin bulunması, kullanıcıların hangi verilere erişebileceğini belirleyen bir yetkilendirme prosedürünün oluşu ve bilgi işlem uygulamalarının yalnızca yetkilendirilmiş iş amaçları için kullanıldığı görüşlerinde, tıbbi ve idari birim çalışan grupları arasında fark bulunamamıştır.

Genel uygulama anlamında, bilgisayar güvenliğindeki en önemli konu verilerin yedeklenmesidir. Ortaya çıkan önemli sorunlar içerisinde, fiziksel güvenlik ve internet güvenliği (güvenlik duvarları, anti-virüs çözümleri ve şifreleme) ile hasta kayıtlarının gizliliği yer almaktadır. Bilgisayar sistemi çöktüğünde uygulamaya konulacak felaket planlarına gereksinim duyulmaktadır. Yine yapılan çalışmalar, bir felaket planının bulunmamasının önemli bir risk oluşturduğunun düşünüldüğünü göstermektedir. Hasta randevularının alınması, kayıtların yapılması ve hastaların tedavi edilmesine olanak sağlayacak bir alternatif sistemin hazırda tutulmasının, hayati öneme haiz olduğu düşünülmektedir. Ayrıca çalışmalar yedeklerin başarısız kalma olasılığının bulunduğuna inanıldığını göstermektedir. Ölçülmesi zor olsa da, hastaların ve işletmenin karşı karşıya olduğu risklerin büyük önem taşıdığı düşünülmüştür. Etkili veri yedekleme stratejilerinin bulunmaması, kayda değer mali yansımalarla neden olabilir. Bilgisayarların virüsler gibi zararlı yazılımlar karşısında korunmamasının, yüksek risk oluşturduğu düşünülmektedir. Bu durum özellikle tıbbi çalışanlar ile uygulama personelinin düzenli olarak internet erişimine sahip olduğu koşullarda geçerlidir. Bilgisayar sistemlerinin çökmesi gibi oluşan sorunların düzeltilmesi, maliyetlidir, zaman israfına yol açar ve günlük operasyonları kesintiye uğratır (55).

Tıbbi veriye erişim değerlendirmesine yönelik temel gereksinim veriye kimin eriştiğinin (ya da erişmeye çalıştığının) kaydedilmesidir. Netice itibari ile her kullanıcı doğrulanması mümkün olan, kendisine özgü bir kimlik tanımlayıcısına sahip olmalıdır. Günümüzde, sağlık kuruluşu içerisindeki birçok sistemde erişim, kullanıcılara kısıtlıdır. Dolayısıyla, bir dosya belirli erişim haklarının tanımlanmış olduğu kullanıcılar tarafından tutulmaktadır. Kullanıcılar sıklıkla kendilerini bir kullanıcı adı ile tanıtır ve kendilerine verilen kişisel bir şifre ile kimlik doğrulaması yaparlar. Şifre korumasının zayıf yönleri bilinmekte ve bunun yerine ya da buna ilave olarak kişisel anahtar kullanımı önerilmektedir. Erişim yetkileri standart olmayıp bunların bazıları kullanıcının mesleğini esas alırken, diğerleri kullanıcının rolü ve hasta ile ilişkisini göz önünde bulundurmaktadır (9). Hangi verilere kimlerin erişebileceğini gösteren anlaşılabilir bir prosedürün bulunması, hem

linik hem de finansal bilgilere, uygun olmayan erişim riskinin azaltılması için önemlidir (55).

Bilgi güvenliğinde hizmet sunumu boyutuna ait parametrelerde, iş yükünün fazla oluşunun bilgi güvenliğine gereken önemin verilmesini engellemediği, bilgi güvenliği süreçlerinin hizmet kalitesini olumsuz etkilemediği, bilgi güvenliğinin öncelikli bir konu olduğu ve iş akışındaki değişikliklerin bilgi güvenliğine gereken önemi vermeyi engellemediği görüşlerinde, idari birim puanlarının tıbbi birim puanlarına göre daha yüksek olduğu gözlemlenmiştir. Tıbbi birim çalışanları için HBYS kullanımı ikincil bir görev olduğu için bilgi güvenliğinin sağlanması da bir yük olarak görülüyor olabilir. Bazı çalışmalar, sağlık bilgi teknolojileri uygulamalarının hastanelerde, hekimlerin çalışma pratikleri üzerine (hızlı yanıt, hataların önlenmesi) bir etkiye sahip olduğunu göstermektedir. Sağlık bilgi teknolojileri uygulaması, sağlık çalışanlarından oluşan bir grubun yerine getirdiği görevlerin doğasını değiştirebilir, örneğin bazı rutin görevlerin gerçekleştirilmesinde hemşirelerin harcadıkları süre, hasta merkezli bakıma daha iyi odaklanması gerekirken, diğer görevlere yönlendirilebilir. Geçmişte mesleki uzmanlık gerektiren bazı görevler (reçetelerin eczacı tarafından onaylanması) kısmen otomasyona bağlanmış olup bu, mesleklerin sergiledikleri rolleri önemli ölçüde değiştirmektedir. Sağlık bilgi teknolojileri uygulaması mesleklerin, kendilerine atanmış rollerini ve sorumluluklarını planlı ya da beklenmedik şekilde değiştirebilir (40).

Bilgi güvenliği alt boyutlarına ait puanlar değerlendirildiğinde, en yüksek puanın erişim ve yetkilendirme boyutunda, en düşük puanın ise hizmet sunumu boyutunda olduğu görülmektedir. Bilgi güvenliği alt boyut puanları arasındaki ilişkiye bakıldığında, birbirleri ile ve toplam puan ile farklı derecelerde ilişkili olduğu belirlenmiştir. Toplam puanı ise en çok, erişim ve yetkilendirme boyutunun etkilediği tespit edilmiştir. Bilgi güvenliğine ilişkin alt boyutların bir bütün olarak değerlendirilmesi gerekliliği, biri yokken diğerinin de olamayacağı ve toplamın her biri ile benzer bir ilişkide olduğu görülmüştür. Bu durum kurum yöneticisi için oldukça önemlidir. Sağlık bilgi teknolojileri sağlık sektöründe, verimliliği, sağlık kalitesini ve/veya sistem verimliliğini artırmanın, bakım kalitesini iyileştirmenin ana yollarından biri olarak sunulmaktadır. Ayrıca tıbbi uygulamaları iyileştirebilirler, iyi

uygulama yönergelerine erişimi kolaylaştırarak karar verme sürecini destekleyebilirler, tanı işlemlerinin istenmesini kolaylaştırabilirler ve önemli parametreleri hatırlatan uyarılar üretebilirler (40). Günümüzde sağlık çalışanları, günlük iş akışları içinde bilgisayar teknolojilerini yoğun olarak kullanmaktadırlar. Böylece elektronik ortama taşınan tüm verilerin kurum içinde ve kurumlar arasında paylaşımı sağlanabilmektedir (52).

Bilgi güvenliği alt boyutları ile yaş arasında anlamlı bir ilişki tespit edilememiştir. Bilgi teknolojileri kullanımı, genç nesilde sisteme kolay adapte olunması nedeni ile daha yüksektir. Ancak bilgi güvenliği ile ilgili böyle bir durum ortaya çıkmamıştır. Aynı şekilde bilgi güvenliği alt boyut puanları açısından, eğitim durumunun, cinsiyetin, kişinin görev yaptığı kadronun, dahil olduğu meslek grubunun ve yönetici olup olmamasının, bilgi güvenliği algısı ve bilgi güvenliğini sağlama açısından belirleyici olmadığı gözlemlenmiştir.

Bilgi güvenliği hizmet sunumu boyutunda, kurumda 12 ay ve altındaki sürede çalışanların puanının, 13-48 ay arasında çalışanlara oranla oldukça düşük olduğu belirlenmiştir. Sürece yeni başlayan bir çalışan için, bilgi güvenliği politikalarına hakim olup süreci yürütebiliyor olması öncelikli bir konu olarak görülmeyebilir. Ayrıca çalışan kuruma başladığında gerekli ve yeterli oryantasyon programını almamış ise, bilgi güvenliğinin önemini yeterince kavrayamayabilir. Kuruma yeni başlayanlarda mutlaka kullanıcı eğitimlerinin tamamlanması, süreç içinde de ihtiyaç halinde ya da yılda bir kez eğitimlerin tekrarlanması oldukça önemlidir.

Araştırmanın hipotezleri içinde bilgi güvenliği ile ilgili en temel parametrenin eğitim olduğu tespit edilmiştir. HBYS eğitimi alanların bilgi güvenliği alt boyut puanlarının eğitim almayanlara göre daha yüksek olduğu belirlenmiştir. Kurum içinde eğitimlerin verilmesinin, bilgi güvenliğini sağlamada en temel ve etkili yaklaşım olduğu görülmektedir. Çünkü eğitim, bilgi güvenliğinin başarılı şekilde yönetilmesinde oldukça önemli bir öğedir (39). Yapılan bazı araştırmalar bilgi güvenliği konusunda farkındalığın önemli bir sorun olduğunu göstermektedir. Çalışanlar arasında en çok dile getirilen problemlerden birisi, sistem kullanım eğitimi almayanların, bilgi güvenliği ile ilgili yeterli farkındalığı gösteremiyor oluşudur (70).

Hem tıbbi hem de idari birim çalışanları için, HBYS eğitimi alındığında, bu eğitimi almayanlara göre bilgi güvenliği alt boyut ve toplam puanlarının daha yüksek olduğu belirlenmiştir. Yalnızca idari birim çalışanları için, bilgi güvenliği hizmet sunumu boyutu ile güvenlik politikası boyutunda, HBYS eğitimi alma durumu arasında anlamlı bir ilişki saptanmamıştır. Bilgi güvenliği açısından HBYS eğitiminin, tüm çalışanlar için kritik önem taşıdığı belirlenmiştir. Bununla beraber tıbbi ve idari birim açısından bir miktar farklılığın olabileceği de görülmektedir.

Bilgisayarlara alışamama ile ortaya çıkan stresi azaltmaya yardımcı olmak üzere, eğer ilave eğitim programları düzenlenirse kullanıcı memnuniyeti artırılabilir. Bazı araştırmalarda, erken zamanda elektronik order giriş eğitimini alan tıbbi görevlilerde, stres azalmış, kullanıcı memnuniyeti yükselmiş ve hasta güvenliği ve sağlık hizmeti etkinliği artmıştır (10).

Araştırmalar çalışanların, sistemin yaptıkları işlere olumlu bir etki yaratacağına inandıklarında, o sistemi kullanacaklarını göstermiştir. Benzer şekilde klinisyenlerin süreçlere müdahil olmaları, sistemin amacı, potansiyel faydaları ve etkileri ile kendi iş akışlarındaki beklenen değişiklikler hakkında bilgilendirilmeleri, sistemin nasıl kullanılacağı konusunda yapılan başlangıç ve tekrar eğitimleri, sistemin kabul edilmesini ve güvenli bir şekilde kullanımının artırılmasını etkilemeye yardımcı olur (8).

Günümüzde sağlık kuruluşlarında hastaların randevuları, sağlık geçmişleri ile ilgili bilgiler, tahlil sonuçları, tanıları ve aldıkları tedaviler dijital ortamda yer almaktadır. Kişilerin sağlık bilgileri, hekimlerin kişisel notlarından bilgisayar ortamına, hastane arşivlerinden sanal koridorlara taşınmıştır. Böylelikle hastanın geçmiş bilgilerine ulaşım da kolaylaşmıştır. Bu durum yeni tanıların doğru şekilde konulmasını, müdahalenin daha çabuk ve daha az riskli gerçekleştirilmesini sağlayabilir. Ancak bu faydaları ile birlikte diğer taraftan, bir kişinin sağlık durumu ile ilgili bilgiler kişiseldir ve yanlış kullanımı sonucu kişiye ciddi zararlar verebilir. (38). Bu konuda önemle dikkat edilmesi gereken husus, yetkilerin kötüye kullanımını engellemek için önlem alınmasının gerekliliğidir. Elektronik sağlık kayıtlarının tutulması ve kullanılması bakımından tartışılacak önemli bir konu da, kayıtların ne amaçla ve ne kadar süre ile tutulması gerektiğinin doğru olarak belirlenmesidir.

Avrupa İnsan Hakları Mahkemesi de, kişisel verilerin özel hayatın gizliliği kapsamında değerlendirilmesi gerektiği görüşündedir. Mahkemenin bazı kararlarında, kamu kurumlarının ve devletin mahrem olarak saklanması gereken verileri, bu şekilde saklamakta başarısız oldukları takdirde, Avrupa İnsan Hakları Sözleşmesi'ni ihlal eder duruma düştükleri belirtilmiştir (20).

Sonuç olarak; bilgi günümüzde kurumlar için önemi tartışılmaz bir unsur olmakla beraber, güvenliği en fazla ihmal edilen varlıktır. Bu ihmal nedeni ile bilgi güvenliği konusunda oluşabilecek bir açık, başta yasal sorunlar olmak üzere, finansal kayıp, çalışan ve hasta memnuniyetsizliği ile beraber, kurumun ciddi zarar görmesine ve hatta yok olmasına kadar gidebilecek büyük sorunlara yol açabilir. Kurumsal prestijin korunması ve artırılmasında bilgi güvenliği oldukça kritik bir öneme sahiptir. Yöneticilerin anlayışı, işbirliği ve gerektiğinde duruma müdahalesi olmadan, politikaların yürürlükte tutulması olanaksızdır. Yöneticiler, çalışanların bu konudaki farkındalıklarını ve duyarlılıklarını artırarak, bilgi güvenliğini oluşturan ve destekleyen bir kurum kültürünün oluşmasını sağlamalıdır.

8. SONUÇ VE ÖNERİLER

1. Sağlık kurumlarında, bilgi güvenliğinin sağlanması için teknik koruma sağlayabilecek, uluslararası standartlara uyum sağlayan, bilgi ve iletişim teknolojileri altyapısı uygulamaya konmalıdır. Bilgi güvenliğini sağlamak için kimlik belirleme, şifre yapısı oluşturma, hasta bilgileri ile ilgili yapılabilecek işlemler ve bilgi paylaşımı için onam alınması konularında, süreçlerin uygun şekilde belirlenmesi gereklidir. Kimlik denetimi için biyometrik yöntemlerin daha yaygın şekilde kullanılabileceği de unutulmamalıdır.
2. Hastanedeki bilgi varlıkları için tüm sorumluluğu alabilecek özel bir kişi ya da ekip görevlendirilmelidir. Kurumda uzman olmadığı durumlarda dışarıdan destek alınmalıdır.
3. Kurumun bilgi varlıklarının korunması için, bilgi güvenliği politika ve prosedürleri oluşturulmalıdır. Süreçler, görev ve sorumluluklar açık ve net bir şekilde tanımlanmalıdır. Bunlara paralel olarak yetkilendirme ve erişim denetimi prosedürleri oluşturulmalıdır. Çalışanlara rehberlik edecek bilgi güvenliği temel kuralları bulunmalıdır. Kurum içindeki temel gereksinimlere göre gerektiğinde politikalar uygun şekilde güncellenmeli ve politika/prosedürlere uyum da takip edilmelidir.
4. Bilgi güvenliğinin sağlanmasında, tehditler ve riskler iyi bir şekilde tanımlanmalı, uygun koruma yöntemleri seçilmeli ve periyodik olarak denetlenmelidir. Acil durumlar için, mutlaka önceden belirlenmiş eylem planları hazır tutulmalıdır.
5. Sadece teknik alt yapı oluşturmakla bilgi güvenliğinin sağlanamayacağı unutulmamalıdır. Gerçekte güvenlik başarısı çalışanlara aittir. Çalışanların güvenlik konusundaki özeninin, süreçleri önemli ölçüde etkileyeceği unutulmamalıdır. Bilgi güvenliği bilincine sahip davranışlar elde etmek için, bilgi güvenliği farkındalığı eğitim programları uygulanmalıdır. Çalışanlar

sorunların farkına vardıklarında, konuya katılım göstermeyi isteyebilirler. Düzenli eğitim ve son kullanıcı farkındalığı, en iyi uygulamalar ve yöntemler konusunda bilginin yayılmasına olanak sağlar. Sürekli farkındalık da daha iyi anlamının ve katılımın temelini oluşturur. Bilgi güvenliği kazalarının kurumda farklı yöntemler ile duyurulması ile bu konuya verilmesi gereken önem hatırlatılmalıdır.

6. Çalışanların bilgisayar kullanım becerileri bilgi güvenliği açısından önemlidir. HBYS kullanım eğitimi, bilgi güvenliğine verilen önemi artırmaktadır. Tüm çalışanların ulaşabildikleri ve iş akışları içinde ihtiyaç duydukları bilgilerin, doğru tespit edilmesi ve kullanıcı yetkilendirmelerinin ona göre yapılması gerekmektedir. Çalışanlar da özellikle erişim denetimi konusunda bilgilendirilmelidir.
7. Bilgi güvenliğinin tüm boyutları birbirleri ile ilişkili olduğu için bunların uygun şekilde değerlendirilmesi oldukça önemlidir. Biri olmadan diğerinin olamayacağı göz ardı edilmemelidir.
8. Bilgi güvenliğinin sağlanması açısından yaş, cinsiyet, çalışma pozisyonu, yönetici olma gibi faktörlerin ilişkili olmadığı, ancak kurumda görev yapma süresinin süreçte etkili olabileceği göz ardı edilmemelidir.
9. Yöneticiler çalıştıkları kurumlarda bilginin gizliliğini, bütünlüğünü ve kesintisiz kullanımını sağlamalıdır. Yönetim desteği olmadan, bilgi güvenliği programları yalnızca bir öneri olarak kalabilir. Gerekli destek ve teşvik sunulmaz, kaynaklar sağlanmaz ise, ne program etkin olabilir ne de çalışanlar tarafından kabul edilir.
10. Bilgi güvenliğinin sağlanması dinamik bir olaydır ve çalışanların işbirliğine dayalıdır. Politikaların etkin olmasını sağlamak için, yöneticiler ve tüm çalışanlar arasında işbirliği oluşturulmalı, tüm birimlerin aktif olarak görev almaları sağlanmalıdır.

9. KAYNAKLAR

1. Abidi SSR. Healthcare Knowledge Management: The Art of The Possible, Knowledge Management For Healthcare Procedures. From Knowledge to Global Care, 2008; p.1-20.
2. Akkoç L. Hastane Bilgi Yönetim Sistemi (HBYS)'nin Isparta'da Bulunan Sağlık Kuruluşları Üzerindeki Etkililiğinin Araştırılması. S.D.Ü. Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, 2009, Isparta (Danışman: Yrd. Doç. Dr. Mehmet Aktel).
3. Alpagun O. Hastanelerde Verimlilik Sorunu. MPM Yayınları, 1999.
4. Altındış S, Kurt M. Bilgi yönetim uygulamalarının hasta güvenliğine etkisine ilişkin bir araştırma: Afyonkarahisar İli'nde bir uygulama. Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 2010; 24, s.45-61.
5. Amarasingham R. Hospital characteristics associated with highly automated and usable clinical information systems in Texas, United States. BMC Med Inform Decis Mak, 2008; 8:39.
6. Asaro PV, Land GH, Hales JW. Making public health data available to community-level decision makers-goals, issues and a case report. Journal of Public Health Management and Practice, 2001; 7(5):58.
7. Aslandağ K. Bilgi Güvenliği Kavramı ve Bilgi Güvenliği Yönetim Sistemleri ile Şirket Performans İlişkisine Dair Bir Uygulama. Gebze Yüksek Teknoloji Enstitüsü Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, 2010, Gebze (Danışman: Prof. Dr. Halit Keskin).
8. Ayatollahi H, Bath PA, Goodacre S, Lo SY, Draegebo M, Khan FA. What factors influence emergency department staff attitudes towards using information technology?. Emergency Medicine Journal, 2013; 30:303-307.
9. Bakker AR. The need to know the history of the use of digital patient data, in particular the EHR. International Journal of Medical Informatics, 2007; 76:438-441.

10. Bey HY, Wai TJ, Marcelo C, Jong MH, Chieh YL, Ting TL. Evaluation of computerized physician order entry system – A satisfaction survey in Taiwan. *Journal of Medical Systems*, 2012; 36:3817-3824.
11. Blazona B, Koncar M. HL7 and DICOM based integration of radiology departments with healthcare enterprise information systems. *International Journal of Medical Informatics*. 2007; 76(3): p.425-432.
12. Borzekowski R. Measuring the cost impact of hospital information systems: 1987-1994. *Journal of Health Economics*, 2009; 28(5):938-949.
13. Canberk G, Sarioğlu Ş. Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi*, 2006; 3:165-174.
14. Civelek AC. Patient safety and privacy in the electronic health information aera: Medical and beyond. *Clinical Biochemistry*, 2009; 42:298-299.
15. Çokluk Ö, Şekercioğlu G, Büyüköztürk Ş. Sosyal Bilimler İçin Çok Değişkenli İstatistik (SPSS ve LISREL Uygulamaları). Pegem Yayınları, Ankara; 2010; s.206.
16. Çolak HE, İnan H. Türkiye için Konumsal Veri Tabanlı Sağlık Bilgi Sistemi Önerisi. Ankara; 2011.
17. Dodge CR, Carver C, Ferguson JA. Phishing for user security awareness. *Computer & Science*, 2007; 26(1):73.
18. Dokholyan RS, Muhlbaier LH, Falletta JM, Jacobs JP, Shaian D, Haan CK, Peterson ED. Regulatory and ethical considerations for linking clinical and administrative databases. *American Heart Journal*, 2009; 157(6):971-982.
19. Edward H. Shortliffe JJC. *Biomedical Informatics: Computer Applications in Health Care and Biomedicine*. 2006, p. 475-511.
20. Er C. Avrupa İnsan Hakları Sözleşmesi kapsamında elektronik sağlık kayıtları. *Bilişim ve Hukuk*, 2009; 10(1):22-28.
21. Er C. *Biyometrik Yöntemler Ve Özel Hayatın Gizliliği Hakkı*. Yetkin Yayınları, 2007.

22. Ersoy EV. ISO/IEC 27001 Bilgi Güvenliği Standardı Tanımlar ve Örnek Uygulamalar. ODTÜ Geliştirme Vakfı Yayıncılık ve İletişim Yayınları, 2012; s.7-8.
23. Gebrasilase T, Lessa LF. Information security culture in public hospitals: The case of Hawassa Referral Hospital. The African Journal of Information Systems, 2011; 3(3):72-86.
24. Güleş HK, Özata M. Sağlık Bilişim Sistemleri. Nobel Yayın Dağıtım, 2005.
25. Hamill JT, Deckro RF. Evaluating information assurance strategies. Decision Support Systems. 2005, p.39.
26. Hirakis O, Karakounos S. Goals and benefits of knowledge management in healthcare. Knowledge Management: Concept Methodologies, Tools and Applications, 2008; p.2232-2239.
27. International Medical Informatics Association Working Group 1: Health and Medical Informatics Education. Recommendations of the International Medical Informatics Association (IMIA) on Education in Health and Medical Informatics. Method Inform Med, 2000; 39:267-277.
28. Jaana M. Clinical information technology in hospitals: a comparison between the state of Iowa and two provinces in Canada. International Journal of Medical Informatics, 2005; 74(9):719-31.
29. Kağnıcıoğlu H, Sevim A. Yönetim Bilgi Sistemi. Anadolu Üniversitesi Yayınları, 2005.
30. Karahoca A. Information system design for a hospital emergency department: a usability analysis of software prototypes. Journal of Biomedical Informatics, 2010; 43(2): 224-232.
31. Kavuncubaşı Ş. Hastane ve Sağlık Kurumları Yönetimi. Siyasal Kitabevi, 2000; s.235-266.
32. Khaujouei R, Wierenga PC, Hasman A, Jaspers MWM. Clinicians satisfaction with CPOE ease of use and effect on clinicians' workflow, efficiency and medication safety. International Journal of Medical Informatics, 2011; 80:297-309.

33. Kluge EW. Ethical and legal challenges for health telematics in a global world:Telehealth and the technological imperative. International Journal of Medical Informatics, 2011; 80:1-5.
34. Köksal L. “Teletıp ve Telekomünikasyon”, İçinde Sağlık Hizmetlerinde Bilişim Teknolojisinin Uygulama Alanları”. Şelimen D, Mumcu G. (Eds), Bedray Yayıncılık, Ankara; 2011; s.167-178.
35. Kralewski JE, Dowd BE, Adeniyi TC, Gans D, Malakar L, Elsin B. Factors influencing physician use of clinical electronic informtion technologies after adoption by their medical group practices. Health Care Management Review, 2008; 33(4):361-367.
36. Krogh VG, Ichijo K. Bilginin Üretimi. Dışbank Yayınları, 2007.
37. Küzeci E. Kişisel Verilerin Korunması. 2011, [Elektronik Dergi], <http://www.bilisimdergisi.org/s128>.
38. Küzeci E. Kişisel Verilerin Korunması. Turhan Kitabevi, Ankara; 2010.
39. Landolt S, Hirschel J, Schlienger T, Businger W, Zbinden AM. Assessing and comparing information security in Swiss hospitals. Interactive Journal of Medical Research, 2012; 1(2):1-11.
40. Lapointe L, Mignerat M, Vedel I. The IT productivity paradox in health: A stakeholder’s perspective. International Journal of Medical Informatics, 2011; 80:102-115.
41. Lucas HC. Information Systems Concepts for Management. New York McGraw Hill Book Company, 1990; s:442.
42. Malin B, Karp D, Scheuermann RH. Technical and policy approaches to balancing patient privacy and data sharing in clinical and translational research. Journal of Investigative Medicine, 2010; 58(1):11-18.
43. Mole DJ, Fox C, Napolitano G. Electronic patient data confidentiality practices among surgical trainees: questionnaire study. Annals of the Royal Collage of Surgeons of England, 2006; 88(6):550-553.

44. Mumcu G. Elektronik Sağlık Kayıt Sistemi: Sağlık Hizmetlerinde Bilişim Teknolojisinin Uygulama Alanları. Bedray Yayıncılık, Ankara; 2011.
45. Mumcu G, Köksal L, Kopmaz B, Gök MM, Bulu B, Şişman N, Kılıç Aksu P, Tarım M. Sağlık hizmetleri kalitesi ve hastane bilgi yönetim sistemi: Türkiye’den bir örnek. Acıbadem Sağlık Bilimleri Dergisi, 2014; 5(1):31-37.
46. Mumcu G, Köksal L, Şişman N, Çatar RÖ, Tarım M. The effect of pharmacy information management system on safety medication use: A study from private hospitals in İstanbul. Marmara Pharmaceutical Journal, 2014; 18:1-4.
47. Mumcu G, Köksal L, Şişman N, Çatar RÖ. The effectiveness and outcomes of computerized provider order entry in emergency care department of private hospitals. Journal of Marmara University Institute of Health Sciences, 2013; 3(2):83-90.
48. Özata M. Sağlık Bilişim Sistemlerinin Hastane Etkinliğinin Araştırılmasında Yeri ve Önemi. S.Ü. Sosyal Bilimler Enstitüsü Doktora Tezi, 2004, Konya (Danışman: Doç. Dr. Hasan Kürşat Güleş).
49. 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>.
50. Perera G, Holbrook A, Thabane L, Foster G, Willison DJ. Views on health information sharing and privacy from primary care practices using electronic medical records. International Journal of Medical Informatics, 2011; 80:94-101.
51. Rigby M. Evaluation: 16 Powerful reasons why not to do it -and 6 over-riding imperatives. Studies in Health Technology and Informatics. 2001; 2:1198-1202.
52. Robertson M, Callen J. The educational needs of health information managers in an electronic environment: what information technology and health informatics skills and knowledge are required?. HIM J, 2004; 32(3):95-101.
53. Ruotsalainen P. Privacy and security in teleradiology. European Journal of Radiology, 2010; 73:30-35.
54. Sağlık Bakanlığı, Türkiye Sağlıkta Dönüşüm Programı, 2008.

55. Schattner P, Pleteshner C, Bhend H, Brouns J. Guidelines for computer security ingeneral practice. *Informatics in Primary Care*, 2007; 15:73-82.
56. Senor C, Aleman JL, Toval A. Are personel helathcare records safe? A review free web-accessible personal health record privacy policies. *Journal of Medical Internet Research*, 2012; 14(4): 1-14.
57. Sharma SK. *Knowledge Management In Healthcare. Creating Knowledge Based Healthcare Organizations*, 2005; p.1-13.
58. Singh D, Spiers S, Beasley BW. Characteristics of CPOE systems and obstacles to implementation that physicians believe will affect adoption. *South Med J*, 2011; 104(6): 418-421.
59. Stanton JM, Stam KR, Mastrangelo P. Analysis of end user security behaviors. *Computers & Security*, 2005; 24(2):124-133.
60. Suntay Y. *Hastane Bilgi Sistemlerinde Entegrasyon Sorunları ve Çözüm Önerileri*. K.Ü. Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, s.16-63, 2010, Kocaeli (Danışman: Prof. Dr. Nurullah Genç).
61. T.M.H. Turkish Ministry of Health, *Statistical yearbook of health care institutions in 2006*.
62. Tengilimoglu D, Çelik Y, Ulgu M. Comparison of computing capability and information system abilities of state hospitals owned by Ministry of Labor and Social Security and Ministry of Health. *J Med Syst*, 2006; 30(4):269-275.
63. Türkiye Bilişim Şurası. 2. E-Sağlık Çalışma Grubu Final Raporu, 5 Nisan 2004.
64. Upfold CT, Sewry DA. An investigation of Information Security in Small and Medium Enterprises (SMEs) in the Eastern Cape, In: Venter HS, Eloff JHP, Labuschagne L, Eloff MM.(Eds.), *Proceedings of the ISSA 2005 new knowledge today conference*, 29 June–1 July 2005, South Africa, Article 082, 1–17. Available from URL: [http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/082 Article.pdf](http://icsa.cs.up.ac.za/issa/2005/Proceedings/Research/082%20Article.pdf).
65. Vardal N. *Yükseköğretimde Bilgi Güvenliği: Bilgi Güvenlik Yönetim Sistemi İçin Bir Model Önerisi ve Uygulaması*. G.Ü. Eğitim Bilimleri Enstitüsü, Doktora Tezi, 2009, Ankara (Danışman: Prof. Dr. Halil İbrahim Yalın).

66. Vural Y. Kurumsal Bilgi Güvenliđi ve Sızma Testleri. G.Ü. Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 2007, Ankara (Danışman: Doç. Dr. Şeref Sağırođlu).
67. Westerheim A. Telemedicine leverages power of clinical information. Health Management Technology, 1999; 20(9):8.
68. Whitman M, & Mattord H. Principles of information security. 1st. ed, Thomson Learning Course Technology, Boston; 2003.
69. Wickramasinghe N, Geisler E. The adoption and implementation of knowledge management in healthcare operations. Managing Worldwide Operations & Communications with Information Technology, 2007; p.91-95.
70. Wirken G. Information Security in Dutch Hospitals. Master thesis Content and Knowledge Engineering Faculty of Science, 2012; p.41-53.
71. Wood CC. Information security policies made easy, USA. Information Shield Publications; 2005, p.35-36.
72. Yıldız Ç. Telekomünikasyon Sektöründe Firma İçindeki Bilgi Güvenliđini Etkileyen Faktörler ve Bu Faktörlerin Çalışanlar Üzerine Etkileri. Gebze Yüksek Teknoloji Enstitüsü Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, 2009, Gebze (Danışman: Doç. Dr. Salih Zeki İmamođlu).
73. Zaim H. Bilginin Artan Önemi ve Bilgi Yönetimi. İşaret Yayınları, 2005; s.122-134.

EK 1



T.C.
MARMARA ÜNİVERSİTESİ
Sağlık Bilimleri Enstitüsü
Girişimsel Olmayan Klinik Araştırmalar Etik Kurulu

PROJENİN ADI: Hastane Bilgi Yönetim Sisteminin Bilgi Güvenliği Açısından Değerlendirilmesi
PROJE YÜRÜTÜCÜSÜ: Doç.Dr.Gonca MUMCU
PROJEDEKİ ARAŞTIRICILAR: Pınar Kılıç AKSU
ONAY TARİHİ VE ONAY SAYISI: 21.12.2012-3

Sayın Doç. Dr. Gonca MUMCU

152 protokol nolu "Hastane Bilgi Yönetim Sisteminin Bilgi Güvenliği Açısından Değerlendirilmesi" isimli projeniz Enstitümüzün Girişimsel Olmayan Klinik Araştırmalar Etik Kurulu tarafından incelenmiş ve etik yönden uygunluğuna karar verilmiştir.

F. Arıcıoğlu

Prof. Dr. Feyza ARICIOĞLU
Komisyon Başkanı

Serap Şirvanci

Doç. Dr. Serap ŞİRVANCI
Komisyon Başkan Yardımcısı

Akyüz

Prof. Dr. Serap AKYÜZ

Levent Kabasakal

Doç. Dr. Levent KABASAKAL

Prof. Dr. Aysel PEHLİVAN

Neşe Bahçecik

Doç. Dr. Neşe BAHÇECİK

Doç. Dr. Oğuzhan DEYNELİ

Asım Cingir

Doç. Dr. Asım CİNGİR

Doç. Dr. Pınar AY

Murat Çekin

Yrd. Doç. Dr. Murat ÇEKİN

Zübeyir Sarı

Yrd. Doç. Dr. Zübeyir SARI

Tolga Güven

Yrd. Doç. Dr. Tolga GÜVEN

EK 2

HASTANE BİLGİ YÖNETİMİ SİSTEMİNİN BİLGİ GÜVENLİĞİ AÇISINDAN DEĞERLENDİRİLMESİ

Hastanemizde “Hastane Bilgi Yönetimi Sisteminin Bilgi Güvenliği Açısından Değerlendirilmesi” konusu ile ilgili olarak yürüttüğümüz çalışmada size bazı sorular sorulacaktır. Bu anket tamamen bilimsel çalışma amaçlı olup sizin ya da kurumun adı kullanılmayacaktır. Gerekli desteği sağlayabilmeniz hususunu arz ve rica ederiz.

Dt. Pınar Kılıç Aksu	Prof.Dr. Gonca Mumcu
Hastane İşletmeciliği Doktora Programı Öğrencisi	Tez Danışmanı Marmara Üniversitesi Sağlık Bilimleri Fakültesi

I-Kişisel Bilgiler

- Çalışma pozisyonunuz aşağıdakilerden hangisidir?
 - Tıbbi Birimler** 1)Uzman hekim 2)Pratisyen hekim 3)Eczacı 4)Hemşire 5)Ebe 6)Acil tıp teknisyeni 7)Laboratuar teknisyeni 8)Radyoloji teknisyeni 9)Anestezi teknisyeni 10)Biyolog 11) Fizyoterapist 12)Sağlık memuru 13)Diyetisyen 14)Diğer.....
 - İdari Birimler** 1)Hasta Hizmetleri 2)Destek Hizmetler 3)Muhasebe/Faturalama 4)Teknik Hizmetler 5)Satınalma 6) İnsan Kaynakları 7)Kalite 8)Pazarlama 9) Biyomedikal 10)Arşiv 11) Hasta ilişkileri 12) Üst Yönetim 13)Diğer.....
- En son mezun olduğunuz okul?
- Yaşınız:
- Cinsiyetiniz: 1)Erkek 2)Kadın
- Kurumda çalışma süreniz:yıl ay
- Hastane bilgi yönetimi sistemi kullanımı deneyim süreniz: ay
- Hastane bilgi yönetimi sistemini kullanmak için eğitim aldınız mı? 1)Evet 2)Hayır
- Hastane bilgi yönetimi sistemini kullanmak için aldığınız eğitim ne kadar sürdü?saat
- Aldığınız eğitimi nasıl değerlendirirsiniz? 1)Yetersiz 2)Kararsızım 3)Yeterli
- Genel olarak bilgisayar kullanım becerinizi nasıl değerlendirirsiniz?
(Çok yetersiz) 0 _____ 100 (Çok yeterli)
- Genel olarak hastane bilgi yönetimi sistemi kullanım becerinizi nasıl değerlendirirsiniz?
(Çok yetersiz) 0 _____ 100 (Çok yeterli)

II-Bilgi Güvenliği İle İlgili Genel Sorular

12. Hastanedeki hangi tür bilgilere kolaylıkla ulaşabiliyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)
- 1)Hastaya ait bilgiler 2)Çalışanlara ait bilgiler 3)Hastaneye ait mali bilgiler 4)Yönetimsel raporlar
5)Süreçsel raporlar 6)Kurum prosedürleri 7)Sigorta şirketi bilgileri 8)Sosyal güvence bilgileri
9)Diğer.....
13. Hastanedeki günlük çalışma düzeninizde hangi tür bilgileri kullanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)
- 1)Hastaya ait bilgiler 2)Çalışanlara ait bilgiler 3) Hastaneye ait mali bilgiler 4)Yönetimsel raporlar
5)Süreçsel raporlar 6)Kurum prosedürleri 7)Sigorta şirketi bilgileri 8)Sosyal güvence bilgileri
9)Diğer.....
14. Hastanedeki hangi tür bilgiler koruma altındadır? (Birden fazla seçenek işaretleyebilirsiniz)
- 1)Hastaya ait bilgiler 2)Çalışanlara ait bilgiler 3) Hastaneye ait mali bilgiler 4)Yönetimsel raporlar
5)Süreçsel raporlar 6)Kurum prosedürleri 7)Sigorta şirketi bilgileri 8)Sosyal güvence bilgileri
9)Diğer.....
15. Hastane bilgi yönetimi sistemi üzerinden hasta verilerine erişiminiz kim/kimler tarafından denetleniyor?
16. Bilgi güvenliğinin sağlanması için sisteme girişte kimlik belirleme yöntemi olarak aşağıdakilerden hangisini /hangilerini kullanıyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)
- 1)Kullanıcı adı 2)Şifre 3)Akıllı kart 4)Parmak izi 5)Diğer
17. Aşağıdaki şifre yapılarından herhangi birini kullanıyor musunuz? (Birden fazla seçenek işaretleyebilirsiniz)
- 1) 1234.....
2) 8765.....
3) Kullanıcı adı ve şifrenin aynı olması
4) Şifrede kişisel isim kullanımı
5) Şifrede bölüm adı kullanımı
6) Şifrede hastane adı kullanımı
7) Sayı ve harfin bir arada kullanımı
8) Diğer
18. Hastaya ait olan bilgilerin paylaşımı için hastalardan onam formu alıyor musunuz?
- 1)Evet 2)Hayır
19. Hastane bilgi yönetimi sisteminde hastaya ait bilgiler için aşağıdaki işlemlerden hangisini/hangilerini yapabiliyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)
- 1)Okuma 2)Yazma 3)Silme 4)Gönderme 5)Değiştirme 6)Kopyalama 7)Ekleme
8) Diğer.....
20. Hastaya ait hangi bilgilere erişebiliyorsunuz? (Birden fazla seçenek işaretleyebilirsiniz)
- 1)Kimlik bilgileri 2)İletişim bilgileri 3)Hastalık bilgileri 4)Tıbbi raporlar 5)Tetkik sonuçları
6) Önceden aldığı tıbbi hizmetlere ait bilgiler 7)Ödeme bilgileri 8) Sigorta bilgileri 9)Diğer.....

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

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

22. Sizce bilgi güvenliği ile ilgili sorunların nedeni nedir?

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

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

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

- 1) Evet
- 2) Hayır

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

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

26. Hastanedeki bilgi güvenliği için kaç puan verirsiniz?

(Çok kötü) 0 ————— 100 (Çok iyi)

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

Kesinlikle katılmıyorum

1	2	3	4	5
---	---	---	---	---

Kesinlikle katılıyorum

Orta derecede
katılıyorum

28. Hastanede, bilgi güvenliğine ilişkin yazılı politikalar vardır.

Kesinlikle katılmıyorum

1	2	3	4	5
---	---	---	---	---

Kesinlikle katılıyorum

Orta derecede
katılıyorum

29. Çalışanlar bilgi güvenliği politikalarından haberdardır.

Kesinlikle katılmıyorum

1	2	3	4	5
---	---	---	---	---

Kesinlikle katılıyorum

Orta derecede
katılıyorum

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

Kesinlikle katılmıyorum

1	2	3	4	5
---	---	---	---	---

Kesinlikle katılıyorum

Orta derecede
katılıyorum

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

Kesinlikle katılmıyorum

1	2	3	4	5
---	---	---	---	---

Kesinlikle katılıyorum

Orta derecede
katılıyorum

32. Bilgi güvenliğinin sağlanması için çalışanlar gerekli özeni gösterir.

Kesinlikle katılmıyorum

1	2	3	4	5
---	---	---	---	---

Kesinlikle katılıyorum

Orta
derecede katılıyorum

33. Hastanedeki yöneticiler bilgi güvenliğine gereken özeni gösterir.

Kesinlikle katılmıyorum

1	2	3	4	5
---	---	---	---	---

Kesinlikle katılıyorum

Orta derecede
katılıyorum

34. Yöneticiler bilgi güvenliğinin uygulaması konusunda sorumluluk sahibidirler.

Kesinlikle katılmıyorum

1	2	3	4	5
---	---	---	---	---

Kesinlikle katılıyorum

Orta derecede
katılıyorum

35. Hastane içinde bilgi güvenliği konusunda bir uzman bulunmaktadır.

Kesinlikle katılmıyorum

1	2	3	4	5
---	---	---	---	---

Kesinlikle katılıyorum

Orta derecede
katılıyorum

36. Bilgi güvenliği uzmanı bulunmadığında dışarıdan danışmanlık hizmeti alınmaktadır.

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum
Orta derecede katılıyorum						

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

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum
Orta derecede katılıyorum						

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

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum
Orta derecede katılıyorum						

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

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum
Orta derecede katılıyorum						

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

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum
Orta derecede katılıyorum						

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

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum
Orta derecede katılıyorum						

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

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum
Orta derecede katılıyorum						

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

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum
-------------------------	---	---	---	---	---	------------------------

Orta derecede katılıyorum

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

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum
-------------------------	---	---	---	---	---	------------------------

Orta derecede katılıyorum

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

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum
-------------------------	---	---	---	---	---	------------------------

Orta derecede katılıyorum

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

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum
-------------------------	---	---	---	---	---	------------------------

Orta derecede katılıyorum

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

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum
-------------------------	---	---	---	---	---	------------------------

Orta derecede katılıyorum

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

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum
-------------------------	---	---	---	---	---	------------------------

Orta derecede katılıyorum

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

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum
-------------------------	---	---	---	---	---	------------------------

Orta derecede katılıyorum

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

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum
Orta derecede katılıyorum						

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

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum
Orta derecede katılıyorum						

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

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum
Orta derecede katılıyorum						

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

Kesinlikle katılmıyorum	1	2	3	4	5	Kesinlikle katılıyorum
Orta derecede katılıyorum						

ÖZGEÇMİŞ

Adı	PINAR	Soyadı	KILIÇ AKSU
Doğum Yeri	ERZURUM	Doğum Tarihi	07.03.1975
Uyruğu	T.C.	Tel	536 370 05 05
E-mail	pinarkilicaksu@yahoo.com		

Eğitim Düzeyi

	Mezun Olduğu Kurumun Adı	Mezuniyet Yılı
Doktora/Uzmanlık		
Yüksek Lisans	İstanbul Üniversitesi Sosyal Bilimler Enstitüsü	2002
Lisans	İstanbul Üniversitesi Dişhekimliği Fakültesi	1998
Lise	Bilge Kağan Lisesi	1992

İş Deneyimi

	Görevi	Kurum	Süre (Yıl - Yıl)
	Hastane Müdürü	Yeditepe Üniversitesi Hastanesi	2005-2011
	Genel Müdür Yardımcısı	Medicalpark Hastanesi	2011-2013
	Hastane Müdürü	Dünyagöz Hastanesi	2013-2014

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

Yabancı Dil Sınav Notu #

YDS	ÜDS	IELTS	TOEFL IBT	TOEFL PBT	TOEFL CBT	FCE	CAE	CPE
	62.500							

	Sayısal	Eşit Ağırlık	Sözel
ALES Puanı	52.784	54.706	56.627
(Diğer) Puanı			

Bilgisayar Bilgisi

Program	Kullanma becerisi
Office	İyi

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