Vizyoner dergisi

Süleyman Demirel Üniversitesi Vizyoner Dergisi, Yıl: 2019, Cilt: 10, Sayı: 23, ss.108-125.
Suleyman Demirel University Visionary Journal, Year: 2019, Volume: 10, Number: 23, pp.108-125.

ARAŞTIRMA MAKALESİ / RESEARCH ARTICLE

HASTANELERDE BİLGİ GÜVENLİĞİ YÖNETİMİ: NİTEL BİR ARAŞTIRMA

INFORMATION SECURITY MANAGEMENT IN HOSPITALS: A QUALITATIVE STUDY

Selma BARAN[1]

Dr. Öğr. Üyesi Emine ŞENER[2]

ÖZ

Bilgi güvenliği son yıllarda sağlık kurumlarında daha da önem kazanmaya başlamıştır. Özellikle teknolojik gelişmeler ile birlikte gerekli önlemler alınmadığı takdirde bilgi sızıntılarının artacağı düşünülmektedir. Hastane bilgi güvenliğine ilişkin çalışanların görüş, öneri ve değerlendirmelerini tespit etmek amacıyla nitel araştırma yönetmelerinden derinlemesine görüşmenin kullanıldığı bu çalışmada farklı birimlerde çalışan 12 hastane çalışanına ulaşılmıştır. Görüşmelerden elde edilen veriler ATLAS.ti nitel veri programında analiz edilerek yorumlanmıştır. Bu doğrultuda uygulamada ortaya çıkan sorunlar ve çözüm önerileri bu görüşler doğrultusunda oluşturulmuştur. Araştırma sonucunda, katılımcıların yaygın olarak bilgi güvenliğinin önemini vurguladıkları ve bilgi güvenliği olgusunun "hasta mahremiyeti" olgusuyla birlikte algılandığı tespit edilmiştir. Bunun yanı sıra fiziksel koşulların, gizlilik, bütünlük ve erişilebilirlik açısından bilgi güvenliği için gerekli olduğu görülmüştür. Bilgi güvenliği yönetim sisteminin etkili işlemesi amacıyla, yöneticiler ve çalışanların işbirliği içinde olması araştırma sonuçlarına ilişkin geliştirilen önerilerden biridir.

Anahtar Kelimeler: Bilgi Güvenliği, Bilgi Güvenliği Yönetimi, Hastane, Sağlık Bakım Bilgi Sistemleri, Durum Çalışması.

JEL Sınıflandırma Kodları: M12, M15.

ABSTRACT

Information security has become more important in health care institutions in recent years. Especially, if necessary precautions are not taken in line with the development of technology, it is expected that information leaks would increase. In the study in which in-depth interviews with qualitative research directives are used in order to determine the opinions, suggestions and evaluations of employees about hospital information security, 12 hospital employees working in different units are reached. The data obtained from the interviews are analysed and interpreted in ATLAS.ti qualitative data program. In this respect, the problems that arise in practice and the solution proposal are established in line with these opinions. As a result of the research, it is determined that participants emphasize the importance of information security widely and that information security is perceived together as "patient privacy". In turn, is it also seen that physical infrastructure is necessary for information security in terms of privacy, integrity and accessibility. It is one of the proposals of the research that managers and employees should cooperate for an effective information security management system.

[1] Kırşehir Ahi Evran Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, İşletme Bölümü, selma_baran137@hotmail.com, https://orcid.org/0000-0001-8285-789X.

[2] Kırşehir Ahi Evran Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, İşletme Bölümü, esener@ahievran.edu.tr, https://orcid.org/0000-0002-8903-1684.

Makale Geliş Tarihi / Received : 17.07.2018
Makale Kabul Tarihi / Accepted: 09.12.2018

DOI: 10.21076/vizyoner.444451

Keywords: Information Security, Information Security Management, Hospital, Healthcare Information Systems, Case Study.

JEL Classification Codes: M12, M15.

1. GİRİŞ

Güvenlik konuları günlük yaşamın ayrılmaz bir parçası olup kuruluşların da yeterince önem vermek zorunda oldukları bir konudur. Yasalar ile güvence altına alınan bilgi güvenliği, kurumsal yönetişimi güçlendirmek ve olabilecek risklerden korunmak bakımından önemlidir. Kurum ve kuruluşlarda verimliliğin artırılması, bilgiye erişilebilirliğin kolaylaşması, bilgi güvenliğinin sağlanması amacıyla bilgi güvenliği sistemi kullanımı gittikçe yaygınlaşmaktadır. Son yıllarda bilgi gizliliğine gereken önemin verilmesine ilişkin gereklilik gözden kaçmamaktadır. Gerek kamu gerekse özel sektörde bir zorunluluk haline gelen bu sürecin yönetimi ele alınması ve üzerinde durulması gereken bir konudur.

Bilgi güvenliği çok geniş bir alanı kapsamaktadır. Teknolojinin gelişmesi ile birlikte çok fazla veri kullanılmaktadır. Teknoloji bir bakıma işlerin kolaylaşmasını sağlarken diğer taraftan sistemden kaynaklı oluşabilecek hataların giderilebilmesi için alanında uzman personele ihtiyaç artmaktadır. Sağlık personeline kendi alanlarında eğitim ve seminerler vermek sistemin uygulanma düzeyini artırmaktadır. Bu bakımdan eğitimin yanı sıra bilgi gizliliğinin etik kurallar çerçevesinde uygulanması da sağlanmalıdır. Her türlü riske karşı veri sorumluları gerekli tedbirleri almak zorundadır aynı zamanda kişisel verileri kanun hükümlerine aykırı olarak bir başkasına açıklayamaz ve kullanamaz (Sağlık Bakanlığı, 2018:147). Tüm bu ifadeler mevzuat hükümlerince belirlenmiş olsa da konuya gereken önemin verilmesi ile bilginin gizliliği ve güvenliği ile sağlanabilir.

Hastaneler kişisel ve klinik bilgileri toplar, kullanır ve saklar. Sağlık kurumları ciddi bir organizasyon yapısı olduklarından, bilgi sızıntısı, bilgi ihlali, gizlilik ve güvenlik ayarlarına daha fazla dikkat etmelidirler. Kurallara, yönetmeliklere, güvenlik konularına ve tıbbi yasalara uyulması gerekir (Mehraeen vd., 2016:49). Bu çalışmada hastanede oluşturulan, bilgi güvenliği yönetimi politikaları hakkında bilgi verilmekte, karşılaşılan teknik ve yönetsel zorluklar ve bu zorlukların nasıl üstesinden gelinebileceği, uygulanan yöntemler, kurumsal bilgi güvenliği kültürü bu bilinci oluşturma aşamaları ile hastanenin bilgi güvenliği seviyesinin durumu, katılımcıların görüşlerine bağlı olarak aktarılmaktadır. Bu çalışmanın genel amacı, hastanelerde bilgi güvenliği yönetim sisteminin uygulamasında ortaya çıkan sorunları tespit edip çözüm önerisi geliştirmektir. Bu genel amaç çerçevesinde hastane çalışanlarının görüşlerin belirlenmeye çalışılmıştır. Araştırma kapsamında Bilgi Güvenliği Yönetim Sistemi (BGYS) uygulamasının, varsa aksayan yönlerine yönelik çözüm önerisi geliştirmenin sağlık hizmetlerinde bilgi güvenliği yönetim sürecine katkı sağlayacağı düşünülmektedir.

2. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Bilgi, yaşadığımız dönem ve geçmiş dönemin anahtarı, geleceğin şekillenmesinde anahtar rollere sahip bir varlıktır. Bilginin doğru amaçla kullanılmasını sağlayan, bilgiyi kesintiye uğratan, çalınmasına neden olan risk faktörlerinin önlenmesi olarak tanımlanan bilgi güvenliği (Aksu, 2014:13; Başdinkçi, 2017:1) günümüzde kurumsal ve kişisel düzeyde değişen ve gelişen bir öneme sahiptir. Elektronik uygulamaların artmasıyla birlikte bilginin, paylaşılması, erişilmesi ve bilgi kaybının olması, bilgi güvenliliğinin öneminin artmasını sağlayan etkenlerdir. Bilişim teknolojilerinin her alanda kullanılıyor olması, bilgi güvenliğinin sağlanmasını zorunlu hale getirmiştir. Gelişen bilişim teknolojisi, bilginin çoğaltılmasını sağlayıp ve her yerden erişimi mümkün kılmaktadır. Bilginin kaybolması veya kötü amaçlı kullanılması durumlarında bilgi güvenliğinin sağlanması büyük önem taşımaktadır. Kurumlarda bilgi güvenliğinin sağlanabilmesi için sorumlu olan kişilerin görevlerini tam olarak yerine getirmeleri gerekmektedir. Kurallara uyulmaması sonucu sistemde meydana gelebilecek olan açıkların engellenmesi için kişilerin eğitilmeleri gerekmektedir (Başdinkçi, 2017:1).

Bilgi güvenliği, yaşadığımız çağda çokça kullanılan elektronik ortamda, bilgilerin saklanması, korunması ve taşınması sırasında bilgilerin bütünlüğünün bozulmadan güvenli bir şekilde oluşturma çabalarıdır. Bu aşamaların sağlanması için, kurumlar kendilerine uygun güvenlik politikası belirlemelidir. Bu politikalar sayesinde kullanılacak faaliyetlerin sorgulanması, sınırlılıkların bilinmesi, yöntemlerin belirlenmesiyle birlikte uygulamaya konulur (Canbek ve Sağıroğlu, 2006:168). Bilgi güvenliği, verilerin, saklanması taşınması ve izinsiz kullanılmasını engellemek amacıyla gerçekleştirilen koruma işlemidir. Gizlilik, bütünlük ve erişilebilirlik olmak

üzere üç unsuru olan kavramın bileşenlerinden birinin zarar görmesi durumunda bilgi açığı meydana gelmektedir. Temel amacı ise şu şekilde sıralanabilir (Aksu, 2014:34):

- Veri bütünlüğünün korunması,
- Yetkisiz erişimin engellenmesi,
- Mahremiyet ve gizliliğin korunması,
- Sistemin devamlılığının sağlanmasıdır.

Bilgi güvenliğinin *gizlilik* unsuru; bilginin, yetkisiz kişilerin erişimine kapalı olması ve yetkisiz kişilerin engellenmesi olarak tanımlanabilir (Yılmaz, 2014:47). Uluslararası Standartlar Örgütü (ISO) gizliliği, "bilginin sadece yetkilendirilmiş kişilerce erişilmesinin sağlanması" olarak tanımlar. Gizlilik düzeyi, kanunlara, yapılan sözleşmelere ve kurumların yapmış olduğu risk analizlerine göre belirlenir. Bu bağlamda belli prosedürlerin uygulanması gerekmektedir (Başdinkçi, 2017:8). *Bütünlük* unsuru ise, bilginin, doğru ve tam olarak işlenmesi, yetkisiz kişiler tarafından değiştirilmesinin engellenmesini ifade etmektedir (Aksu, 2014:35). Bilginin, bütünlüğünün bozulmadan, göndericiden çıktı halinde alıcıya ulaşmasıyla, doğruluk ve tamlığının korunmuş olmasıyla bütünlük sağlanır. Bilgi göndericiye ulaşırken, yeni veriler eklenmemiş veya çıkarılmamış, sırası ve izlediği yollar değiştirilmemiş olarak alıcıya ulaşması gerekir (Gerçeker, 2012:38). Bilgi güvenliğinin bir diğer unsuru olan *erişilebilirlik* bilginin, gerekli olduğu durumlarda, yetkili kişiler veya kurumlar tarafından kullanılabilmesidir. Bilgiye ihtiyaç duyulduğunda yetkili kişiler tarafından kullanılabilir olması, bilginin güvenliğinin de bir göstergesi olarak kabul edilir. Erişime yetkilendirme, kurumlar tarafından güvenli ve doğru bir şekilde yapılmalıdır (Aslandağ, 2010: 20).

BGYS, kurumlarda bilginin, gizliliğini, bütünlüğünü, erişilebilirliğini sağlayarak hassas bilgileri kontrol altına alan bir yaklaşımdır. Üst yönetim tarafından desteklenen bilgi güvenliği yönetim sistemi, risk faktörlerini en aza indirgeyebilmek için, faaliyete geçirilmesiyle mümkün olmaktadır. Kurum yapısında oluşturulan, bilgilerin, gizliliği, bütünlüğü, erişilebilirliğini sağlamak kurumun temel hedefidir (Gerçeker, 2012:49). Kurumlar kendi bünyesinde BGYS, oluştururken planlı ve sistemli şekilde süreci yönetmeleri gerekir. Sistemin nelerden oluşacağı, kapsamının neler olacağı konusunda ön bilgi oluşturulmalıdır. Kurum, risk faktörlerini belirleyerek, hedeflerini ortaya koyarak, yönetime yön veren durumlardan hangi BGYS'ni kapsamına alacağını karar vererek, kendine göre bir politika belirlemelidir (Akay, 2014:75-77).

BGYS'nin kurulumu aşamasında, hedefler, amaçlar ve süreç belirlenerek geliştirilmeye başlanır. Uygulama aşamasında belirlenen bu politikalar işlenir. Gerekli aşamalar yapıldıktan sonra istenilen güvenliğin sağlanıp sağlanmadığı kontrol edilir. Bir döngü içerisinde devam eden BGYS, gözden geçirme sonucunda hedefine uygun çalışmayan sistemler için önlem alınır (Marttin ve Pehliven, 2010:50). BGYS, kurumu sürekli iyileştirmek için etkin bir şekilde devamlı uygulanması gerekir. Bir defada kullanılabilecek bir faaliyet değildir. Kuruma faydalı olabilmesi için kuruluşun bir parçası olarak görülmelidir. Kurumların, teknik önlemlerinin yanı sıra teknik olmayan faktörlerin de denetimleri yapılarak, iş süreçleri ve bilgi güvenliği standartlarına uygun olarak korunmaları ve güvenliğin sağlanabilmesi için BGYS geliştirilmelidir (Aslandağ, 2010:17; Yılmaz, 2014:51).

2.1. Bilgi Güvenliği Yönetim Sistemi Standardı

Yönetim bilgi sistemleri, yöneticileri doğru bilgiye doğru zamanda yönlendiren, yönetim fonksiyonlarını kolaylaştırmak amacıyla oluşturulan bir sistemdir. Bilgi sistemleri, kurumların yapılarına göre farklılık göstermektedir. Bilgiye çok fazla gereksinim duyan sağlık kurumlarında bunun önemi artmaya başlamıştır. Sağlık kurumlarında bilgilerin yeterli ve güvenilir olabilmesi için bilginin etkin yönetimi önemlidir. Sağlık sektöründe hayati öneme sahip olan bilgi yönetiminin bu açıdan hatasız olması gerekmektedir (Yılmaz ve Demirkan, 2012:9).

BGYS, bilgilerin yönetilebilmesi amacıyla kullanılan bir yaklaşımdır (Marttin ve Pehliven, 2010:50). BGYS, uluslararası düzeyde kabul edilmiş bir standart olarak görülür. Bu bilgi sistemi, kurumlarda bir takım denetimlerin sağlanması ve önlemlerin alınması konusunda uygun bir yapı sunmaktadır. BGYS, kurumların ihtiyacına yönelik önemli bir yere sahiptir (Aslandağ, 2010:16). Sağlık sektörünün oluşturacağı ISO 27001 Bilgi Güvenliği Yönetim Sistemi standardı, kendi bünyesinde kendini yenileyen düzenleyici özelliği ile sistemli bir şekilde gereksinimleri ve özellikleri kuruluşlara fayda sağlar (Uğuz, 2018:3). Hassas bilgilerin korunması ve yönetilebilmesi amacıyla oluşturulan BGYS, ilk defa 1998 yılında yayınlanan BSI (British Standards Institute) tarafından BS 7799-2 olarak kullanılmıştır. Uluslararası Standartlar Kurumu'nun kabul etmiş olduğu bu standart ISO/IEC 27001, 2005 yılında

BGYS'nin en temel standardı olarak yayımlanmıştır. ISO/IEC 27001 standardı kurumlarda yapılması gereken çalışmaların belirlenmesi için kılavuz niteliği taşımaktadır (Yılmaz, 2014:52).

Ülkemizde bilgi güvenliği yönetimini ilgilendiren 27730 sayılı "Elektronik Haberleşme Güvenliği Kapsamında TS ISO/IEC 27001 Standardı Uygulamasına İlişkin Tebliğ" ile hizmet türüne göre bazı kurumlara bilgi güvenliği standardına uygunluk sağlama veya uygunluk belgesi alma yükümlülüğü bazı kurumlara ise uygunluk belgesi almadan standarda uygunluk sağlama yükümlülüğü getirilmiştir (Resmi Gazete, 2010).

ISO 27001 standardı, kendini yenileyen, tehdit ve saldırılara karşı tepki gösteren bir sistemdir. Süreç olarak ele alınması gereken ISO 27001 bilgi güvenliği, planla, uygula, kontrol et ve önlem al aşamalarından oluşur. Bu model, sistemde olması gereken öğeleri tanımlayarak, bir döngü şeklinde çalışmasına yardımcı olur (Evrin ve Demirer, 2011:27). ISO 27001 standardı, sertifikalandırma kurumu tarafından uygulanır. Denetimi gerçekleştirmek için, kurumun dokümanlarını, risk faktörlerini, güvenliğini, uygunluğunu içeren prosedürler uygulayarak, denetim işlemi gerçekleştirilir. Kurumun faaliyet yapısına göre değerlendirmede bulunulur, prosedürlere uyulup uyulmadığı gözden geçirilir. Gerekli tetkikler yapıldıktan sonra, başarılı denetim sağlandığında ISO 27001 standardı belgesi alınır (Marttin ve Pehliven, 2010:55). ISO 27001'de BGYS'nin kurumların gereksinimleri olan belgelendirilme için yapılacaklar anlatılırken, ISO 27002' de BGYS uygulama kodu niteliğinde, pratik uygulamaları ve kontroller anlatılmaktadır (Başdinkçi, 2017:17). Kurumlar isterlerse kendi bünyelerinde uygulayabilirler. ISO 27002 uygulamasından seçilen önlemleri ISO 27001 standardında bulunan döngülerle, bilgi güvenliği gerçekleştirilmeye çalışılmaktadır. Esas olan ISO 27001 standardıdır, ISO 27002 sisteminde belirlenen önlemler için birlikte çalıştırılması sağlanmaktadır (Aslandağ, 2010:52-53).

Uluslararası düzenlemelerde ISO 27799:2008 sağlıkta bilgi güvenliği yönetim sistemi oldukça önemli bir standarttır. Bu standart, ISO 27001 kontrol maddelerin sağlanmasını ve ISO 27002 kurullarına uyumunu esas alan bir kılavuzdur. Kurumlar açısından zorunluluk gerektirmez. Sağlık sisteminde oluşabilecek sorunları tanımlamak amacı ile kullanılır (Akay, 2014:45). Kurumlar, ISO sertifikasını almak istediklerinde, gereklilikleri yerine getirerek uygulamak durumundadırlar. Kuruma uygulama kararı yönetim tarafından alınır. Bu standardın uygulanabilmesi için zorunlu olan prosedürler yerine getirilerek, sorumlu atanmalıdır. Bir defa uygulanacak bir sistem değildir, devamlı kendini yenileyen, değişim ve dönüşüm içinde olan bir sistemdir (Aslandağ, 2010:39).

2.2. Sağlık Hizmetlerinde Bilgi Güvenliği Yönetim Sistemi

Sağlık hizmetlerinin amacı, yapılan hizmetin, etkinliğini, kapsayıcılığını, toplumun sağlık düzeyini yükselterek ve devamlılığını sağlayarak kaliteli hizmet sunmaktır. Günümüzde, teknolojideki gelişmeler, birçok tıbbı prosedürlerin uygulanmasını sağlamıştır. Sağlıkta bilgi güvenliği gereksinimi büyük ölçüde artırmıştır. Sağlık bilgi teknolojilerinin kullanılmasıyla birlikte, bilgiye erişim süreci de hız kazanmıştır (Gerçeker, 2012:69).

Sağlık hizmetlerinde bilgi teknolojilerinin kullanılması, bilginin depolanması, erişilebilirliği, güvenirliği, hizmet kalitesini artıran bir özelliğe sahiptir. Bilginin gizliliği bakımından da bilgi güvenliğinin korunması gerekmektedir. Sistemsel ve fiziksel önlemlerin yanında, sağlık kurumunda çalışanların bilgi güvenlik politikalarını bilmeleri gerekmektedir. Olabilecek riskleri en düşük seviyeye indirgeyebilmek için çalışanların donanım ve yazılım standartlarını bilmeleri önemlidir (Aksu, 2014:14-15). Bu bakımdan problemlerin çözümü için gerekli olan sistematik bilgi yaklaşımları planlanarak uygulanmalıdır. Problemlerin, yönetilmesi, önlenmesi, uygulanması, düzeltilmesi yönünden çalışmaların yürütülmesi önemli bir konudur (Altındiş, 2010:346). Hastanelerde tüm birimlerin ve personelin görev tanımlarının yapılması, yetki ve sorumluluklarının farkında olunması amacıyla bilgi güvenliği modülü oluşturulup hastane çalışanına bu modüle erişimleri sağlanarak gerektiği durumlarda prosedürlere ve görev tanımlarına ulaşma imkanı verilmesi gerekir (İleri, 2016:62).

Sağlık kurumlarında bilgi güvenliğinin sağlanması, öncelikle örgütlerin kurumsal anlamda bilgi güvenliğini sağlamaları ve vatandaşlarımızın bu konuda bilinçlendirilmesiyle mümkündür. Yöneticilere bu noktada büyük görev ve sorumluluklar düşmektedir. Yöneticiler, kurumlarının finansal yapılarına, rekabet güçlerine ve üretim kapasitelerine verdikleri önemi, bilgi güvenliği konusunda da vermeleri gerekmektedir. Bu bakımdan yöneticilerin liderliğinde, yöneticilerin tam desteğiyle kurumlarda bilgi güvenliği sistemi konusunda bilinçlenme ve bilinçlendirme atılımı yapılarak çalışmalara ivme kazandırılması gerekmektedir (İleri, 2016:70).

Sağlık sektörü, bilgiyi işleyen, toplayan, kullanan ve depolayan bir sistemdir. Kaliteli bir hizmet sunabilmesi ve etkin yönetimi için, bilginin kapsamlı şekilde yönetilmesi zorunludur. Sağlık sisteminde uygulayabilmek için bilgi, yönetim sistemi ile birlikte gerçekleşir. Sağlık hizmetleri, iyi planlanmış ve kapsamlı sürece bağlı olarak bilginin elde edilmesi ile etkin yönetimini sağlar. Bilginin diğer kurumlara göre, daha fazla duyarlı olduğu bir alandır

(Aksu, 2014:46-48). Son yıllarda, sağlık planlamasının ve değerlemesinin teknolojik sistemi yaygın olarak kullanılmaktadır. Ağ tabanlı teknolojiye sahip kurumlar, bilgi ve veri tabanı oluşturarak, bireylerin bilgilerine erişimini sağlamak ve bilgilerin korunması amacıyla geliştirilmektedir (Ömürbek ve Altın, 2009: 214). Ülkemizde bilgi güvenliği esaslarını belirleyen, günümüzde mevcut düzenlemeyi yapan, 28363 sayılı "Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik" in amacı, elektronik haberleşme sektöründe, kişisel verilerin işlenmesi, gizliliğin korunması için kurumların uyacakları usul ve esasları belirlemektir. Buna göre kurumlar, sakladıkları verilerin, yetki dışı kullanımı, tahribi değişimi karşısında gerekli önlemi almakla sorumludurlar. Teknik önlemlerinde alınması ile birlikte işlenen ve saklanan verilerin saklama süresinin bitiminden itibaren en geç bir ay içinde imha edilmesi ve anonim hale getirilerek bu işlemlerin tutanaklarla veya sistemsel olarak kayıt altına alınması gerekir (Resmi Gazete, 2012).

Kişisel verilerin korunması mevzuatına göre, Anayasa'nın 20. Maddesi, 6698 Sayılı Kanun ve Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelik, "*kişisel verilerin korunmasına ilişkin hükümlerine azami düzeyde hassasiyet gösterilir*." ifadesi ile verilerin güvence altına alınması amaçlanmıştır (Sağlık Bakanlığı, 2018:147). Ayrıca 1982 Anayasası'nın 20. Maddesinde "*Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz*." ifadesi yer almaktadır. 5237 sayılı Türk Ceza Kanununa göre çeşitli yaptırımlara bağlanarak özel hayatın gizliliği, güvence altına alınmıştır. İnsan Hakları Evrensel Bildirgesi (İHEB) 12. Maddesine göre aynı şekilde, *"Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir."* ifadesine yer verilmektedir. İstisnai durumlar dışında üçüncü kişiler ile bilginin paylaşılması yasaktır, kanunla düzenlenir ve cezai sorumluluk gerektirir (Arslan ve Demir, 2017:193). Teknoloji gelişmeden önce, hasta ile hekim ilişkisi, Dünya Hekimler Birliği'nin sunduğu Sağlık Veri Tabanları ile İlgili Etik Düşünceler Bildirgesi'nde, hastanın mahremiyet bilgilerinin hekim kontrolünde olmasını kolaylaştırmaktaydı. Teknolojinin gelişmesi, hastanın kişisel bilgilerine daha hızlı ulaşımını sağlamıştır ve özerkliğinin korunmasını gerekli hale getirmiştir. (İzgi, 2014:32). Hastanın bilgilerine erişiminin güvenli olması yanında bilginin gizliliğini sağlamak, hukuka aykırı işlenmesini ve erişilmesini önlemek, her türlü idari ve teknik tedbirleri almak veri sorumlusunun (idare) yükümlülüğündedir. Dolayısı ile veri sorumlusu, kendi kurumunda, kanun hükümlerinin uyumluluğun sağlanıp sağlanmadığı konusunda gerekli denetimlerini yapmak veya yaptırmak zorundadır (Sağlık Bakanlığı, 2018:147).

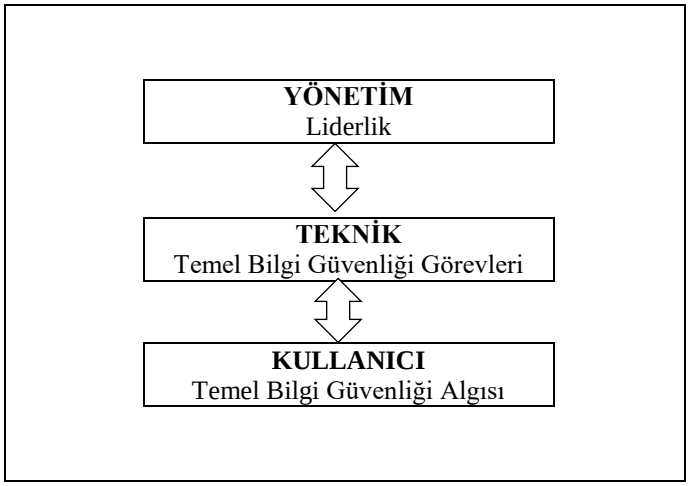
Hastaya ait mahremiyet bilgilerinin saklanması ve korunması en temel alanlardır. Bilgi ve belge güvenliğini sağlamak, maksimum hizmet çabası içerisinde olmak, Sağlıkta Kalite Standartlarının yerine getirilmiş olması kurumlar için önemli rekabet avantajı sağlamaktadır (Varol vd., 2016:155). Siegler'e göre tıpta mahremiyet '*hastanın kişisellik ve gizlilik düşüncesine saygının gelişmesine' ve 'tıbbın temel bir amacı olan hastanın sağlık bakımının geliştirilmesine'* bağlı olarak iki amaca hizmet eder. Hastanın, psikolojik ve fiziksel mahremiyetini korumak, gizlilik ve kişisellik düşüncesine bağlı kalınmasını gerektirir. Saygının bir sonucu olarak mahremiyet konusu, hasta ile hekim arasındaki bilgilerin, bir başkasına anlatılamayacağına, gizli tutulacağına olanak sağlar. Doktor ile hasta arasında sağlanan güven bağı ile hastayı dürüst ve açık konuşmaya teşvik etmesi, tedavi sürecinde önem taşır. Mahremiyet kavramı, geçmişte ve günümüzde önemli ve gereklidir (İzgi, 2014:33). Mahremiyet konusunda hastalara gerekli özenin gösterilmesi, memnuniyeti ve sunulan hizmetin kalitesini artıran bir etmen olarak görülür. Çalışanların göstermiş olduğu titizlik, sağlık kurumlarındaki mahremiyetin değerlendirilmesinde büyük bir öneme sahiptir (Özata ve Özer, 2016:12).

Bilgi teknolojilerinin yaygınlaşmasıyla birlikte, dokümanların bulunduğu yazılı kaynaklar yerini, bilgilerin işlenebildiği elektronik kaynaklara bırakmıştır. Gelişen teknoloji, bilgiye erişim olanaklarının artmasını sağlamıştır. Bu durum avantajın yanında dezavantaja da neden olmaktadır. Günümüzde bilişim teknolojisinde yaşanan gelişmelerle birlikte, bilgi hırsızlığı, bilgi sızdırma, elektronik saldırılar ve kurumun çalışanları tarafından da iç saldırılar olabilmektedir. Sağlık kuruluşlarında da bu saldırılar büyük bir tehdit oluşturmaktadır. Önlemlerin alınmasıyla bu unsurlar azaltılabilir (Varol vd., 2016:156). Bilgi teknolojilerinde yapılan hatalar, erişilebilirlik, güvenlik sorunlarının artmasına neden olur. Büyük bir güvenlik açığının olması, dikkatsiz yapılanmalar, bilginin yetkisiz kişiler tarafından erişimine yol açması olasıdır. Bu şekilde bilginin, değiştirilmesi, yok edilmesi ve görülmesinin engellenmesi gerekir. Bilgi güvenliği, sağlık sektörünün ihtiyaç duyduğu alanlardandır (Aksu, 2014:62).

Tablo 1'de hastanelerde bilgi güvenliği yönetim sürecine ait tablo yer almaktadır. Herhangi bir sağlık hizmetinde uygulanması gereken aşamalar bulunmaktadır. Hastanenin uyguladığı bu yönetim politikalarının uygulanabilmesi

en üst yetkili makamlar ile sağlanmalıdır. Böylece, yönetim, teknik ekip ve kullanıcı belirtilen politikaya uyacaktır (Ismail vd., 2013:51).

Tablo 1. Bilgi Güvenliği Grupları



Kaynak: (Ismail vd., 2013:51)

Sağlıkta bilgi güvenliği yönetim sistemi olarak adlandırılan ISO 27799, 2008 yılında yayımlanmıştır. Bu standart hassas olan sağlık bilgilerinin korunmasını, kişisel bilgilerin yetkisiz kişilerin erişimine geçmesini engelleyerek, bilginin korunması için hareket planı oluşturur. Tedbirlerin alınmasını sağlayarak bilgilerin, güvenlik altına alınmasını sağlar. Uluslararası standartlarda bulunan standartları kullanarak, ilgili duruma göre gerekli güvenlik şartlarını uygular. Bilgi güvenliğinden sorumlu olan yetkilileri ve çalışanları ilgilendiren bu standart sağlık sektörüne uygulanabilmektedir. ISO 27799 sağlık kurumları için yardımcı kaynak oluşturmayı amaçlar. ISO 27001 BGYS'ne ek olarak bu standart, sağlık sektörüne nasıl yorumlanarak uygulanması gerektiğini açıklar (Akay, 2014:46; Aksu, 2014:62-63).

ISO 27001'in uluslararası standardı, bilgi güvenliğinin, kurulması, uygulanması, işletilmesi için şartları gözden geçirme, sürdürme ve iyileştirme işlemleri tamamlandıktan sonra belgelenir. Yeterli düzeyi sağlamak ve tasarlanmış bilgi varlıklarını korumak için gerekli güvenlik kontrolleri yapılmaktadır. Bu standart genellikle tüm organizasyon türlerinde, özel veya kamu kuruluşları uygulanabilir (Susanto vd., 2011:24).

Sağlık sistemi ile ilgili olan ISO 27799 standardı, ISO 27002 kullanılarak, sağlık sistemine nasıl entegre edeceğini düzenlemektedir. ISO 27002 bilginin korunması için fiziksel güvenlik önlemleri alınarak yetkisiz girişten erişim, hırsızlık ve hasar oluşumunun engellenmesi sağlanır. Standart prosedürlerinin işleyişi kılavuzda belgelendirilir. Aynı şekilde süreçler, istisnai durumlar, gecikmeler, kesintiler, arızalar belirlenir ve belgelendirilir. Teknik veya organizasyonel değişiklikler kontrol edilir. Bilgi teknoloji sistemlerinin operasyonları üzerindeki potansiyel etkiler uygulanmadan önce güvenlik olayları analiz edilir, değerlendirilir ve güvenlik sistemi için önemli gelişmeler belirlenir. Son olarak, yerine getirmek için uygun önlemler alınarak veri güvenliği gereksinimleri veri koruma standardında belirtilmiş olarak doğrulanmış bir şekilde düzenlenir ve bilgiler güvence altına alınmış olur (Disterer, 2013:98).

Sürekli değişen ve kendini yenileyen bilgi sistemleri, kurumlarda eğitim ihtiyacını doğurmaktadır. Sağlık kurumları, hastaların ve hasta yakınlarının sağlık güvenliğinden sorumludurlar. Bilgi güvenliğini sağlayacak olan yöneticiler ve çalışanlar için eğitime istekli olmaları gerekmektedir. Sağlık hizmetleri, süreklilik, devamlılık, iletişim, kalite, değerlendirme ve uzmanlık gerektiren bir süreçtir. Teknolojinin yeni olanaklarını kendine entegre eden dinamik bir sistemdir. Riski en aza indirmek için bilgi güvenliği eğitim programı, kullanılan standartları ile birlikte uygulanmalıdır (Marşap vd., 2010:34). ISO 27001 standardı alınması uygulama aşamasına geçilmeden önce yöneticiler veya sorumlu kişilerce BGYS uygulama eğitimi verilmelidir. Kurum içerisinde bilgi güvenliği eğitimini almış bir kişinin olması uygulama aşamasında hazırlığı kolaylaştırır. Kâğıt üzerinde yazılı olan bir belge kurum çalışanları tarafından uygulamaya geçilmediği müddetçe başarılı olunamaz. Çalışanlar, yöneticiler, teknik olan veya teknik olmayan personele ve bilgi güvenliğinin ilgi alanına giren kişilere eğitim verilerek farkındalık oluşturulur (Gülmüş, 2010:66-68). Hastanelerde eğitim planlaması, Sağlık Bakanlığı Genel Müdürlüğü tarafından, bağlı kuruluşlarda gerçekleştirilir. Kurum içerisinde bulunan her personelin bilgi düzeyini artırmayı amaçlar. Bilgi

güvenliği alanında çalışan personel için ileri seviyede BGYS eğitimi planlaması yapılır. Kurumlarda, konferans, seminer, sempozyum şeklinde yıllık planlar yapılır, eğitimler web tabanlı sunulur (Sağlık Bakanlığı, 2014:10).

3. GEREÇ VE YÖNTEM

3.1. Araştırmanın Deseni

Bu araştırma, hastane çalışanlarının bilgi güvenliği yönetim sisteminin uygulama sürecine ilişkin görüşlerinin belirlenmesi amacıyla nitel yöntemde planlanmış bir içsel durum çalışmadır. Burada temel amaç, teori üretmek ya da bulgulara geniş bir evrene genellemek değildir (Yılmaz, 2014:270). Araştırmacının gerçek yaşam, güncel sınırlı bir sistem/durum ya da belli bir zaman içerisindeki çoklu sınırlandırılmış durumlar hakkında çoklu bilgi kaynakları (gözlem, mülakat, dokuman inceleme ve raporlar) aracılığıyla detaylı ve derinlemesine bilgi topladığı, bir durum betimlemesi ya da durum temaları ortaya koyduğu nitel bir yaklaşımdır (Creswell, 2013:99). Bu doğrultuda, bir kurumda cereyan eden bilgi güvenliği yönetim sistemi sürecine odaklanılmış ve sürece ilişkin detaylı bilgiler elde edilmiştir. Farklı birimlerde görev yapan sağlık personelinin, bilgi güvenliği konusunda görüşleri alınarak, birimlerde farklılık olup olmadığını saptanmıştır.

3.2. Araştırma Evreni ve Örneklemi

Araştırmanın evrenini, bir kamu hastanesinde görev yapan sağlık personeli oluşturmaktadır. Katılımcıların gözlem ve görüşlerine dayalı yapılan veri toplama amaçlı bir içsel durum çalışması olan bu çalışmada, evreni temsil niteliği olan ve bilgi güvenliği yönetim sürecinde rol alan, farklı birimlerde çalışan toplam 12 kişiye ulaşılmıştır. Birimler, Sağlık Bakım Hizmetleri Müdürlüğü, İdari Mali İşler Müdürlüğü, Arşiv Birimi, Satın Alma Birimi, Kalite Verimlilik Birimi, Hasta ve Çalışan Hakları, Personel İşleri Birimi, Teşhisle İlişkili Gruplar (TİG), Adli Rapor Hizmetleri, Sağlık Kurulu, Bilgi Sistemleri Birimi şeklindedir. Bu kapsamda çalışmaya, 4 Hemşire, 2 Veri Hazırlama Kontrol İşletmeni, 1 Memur, 1 Avukat (Uzman), 1 Tıbbi Teknolog, 1 Sağlık Teknikeri, 1 Sağlık Memuru ve 1 Bilgi İşlem Birimi Çalışanı, katılmıştır.

3.3. Verileri Toplama Süreci

Araştırmada veri toplama süreci, gizlilik ve gönüllülük esasına göre katılımcıların sözel onamları alınarak görüşme yapmak suretiyle gerçekleştirilmiştir. Araştırmanın amacı doğrultusunda görüşme yapılacak birimler belirlenerek bilgi alınmıştır. Araştırma kapsamında katılımcılara aşağıdaki sorular sorulmuştur;

- *Sizce hastanelerde bilgi güvenliği yönetimi neden önemlidir?*
- *Sizce bilgi güvenliği uygulaması yeterli midir? Yeterliyse neden yeterli? Yetersizse neden yetersiz?*
- *Sizce uygulanan BGY'nin aksayan yönleri var mıdır? Varsa nedenleri ve çözüm önerileri nelerdir?*
- *Sizce kurumunuzda etkin BGYS oluşturmak için hangi koşullar nasıl sağlanmalıdır?*

Nitel araştırmada veri doyumu açısından birden çok kişi ile görüşme sağlanmıştır. Nitel araştırmanın amacına uygun olarak verilerin toplanması ve çalışılan alanın derinlemesine inceleme ile çalışılacak alanın tanınması önemli bir konudur. Bu doğrultuda yetkili kişilerce görüşme yapılmıştır. Görüşme sorularının hazırlanmasında, araştırmanın amacına ve konusuna uygun sorulara yer verilmesine dikkat edilmiştir. Nitel veri analiziyle, görüşlerin gruplandırılmaları ve kavramsal kodlamaları yapılmıştır. Araştırmanın tematik analizi yapılarak kavramlar arasındaki ilişkilere ulaşılarak yorumlanmıştır. Bu çalışmanın veri analizi aşamasında, toplanan verilerin kodlanması, düzenlenmesi, kavramsallaştırılması sağlanarak bilgisayar destekli Atlas.ti programının "free trial" versiyonu kullanılmıştır (https://atlasti.com/free-trial-version/).

3.4. Verilerin Değerlendirilmesi

Nitel araştırma yöntemi sayesinde, sağlık personelinin bilgi güvenliğinin önemini, uygulamanın yeterli olup olmadığını, aksayan yönlerini ve çözüm önerilerine yönelik görüşleri alınmıştır. Yorumlayıcı bir yaklaşımla, esneklik sağlaması bakımından bu araştırmada nitel araştırma tercih edilmiştir. Niteliksel yöntemler metin ve veri görüntüsüne dayanır. Niteliksel araştırmanın amacı, spesifik tasarımlardan bahsetmek ve elde edilen verileri dikkatlice yansıtmaktır (Creswell, 2014:184). Nitel araştırma yöntemi olarak Atlas.ti programının "free trial" versiyonu kullanılarak veriler aktarılmıştır. Nitel araştırma sürecini, bir araştırma projesi olarak kabul eden Atlas.ti, programı, farklı ve büyük veri setlerinden (belgeler, notlar, işitsel ve görsel dosyalar, alıntılar vb.) elde

edilen kodlara erişimi sağlayan sistemli bir çalışma alanı sunar (Çayır ve Sarıtaş, 2017:526). Çalışmada veriler tematik analiz ile değerlendirilmiştir. İlk olarak kodlama yapılmış olup yapılan kodlamalar veride anlatılmak isteneni kapsayacak şekilde oluşturulmuştur Oluşturulan kodların gruplandırılması yapılmıştır. Daha sonra ağ örüntüsü oluşturarak, nitel araştırma veri analizi yapılmıştır ve katılımcıların görüşleri yorumlanarak değerlendirilmiştir.

4. BULGULAR

4.1. Araştırma Grubuna Ait Bulgular

Bu bölümde araştırma kapsamında görüşme yapılan katılımcıların temel özellikleri verilmiştir. Sonraki bölümlerde görüşmeler sonucu nitel araştırma veri analizi tekniği kullanılarak elde edilen veriler öznel bakış açısıyla değerlendirilmiştir.

Araştırma kapsamında, katılımcıların mesleği, çalıştığı birim, öğrenim durumu ve çalışma süresi aşağıdaki tabloda verilmiştir.

Tablo 2. Katılımcıların Özelliklerine İlişkin Dağılım

Sıra	Cinsiyet	Meslek	Çalışılan Birim	Öğrenim Durumu	Çalışma Süresi (Yıl)
BG1	Kadın	VHKİ*	İdari Mali İşler Müdür Yardımcısı	Lisans	24
BG2	Kadın	Hemşire	Sağlık Bakım Hizmetleri Müdürü	Lisans	10
BG3	Erkek	Memur	Arşiv Birimi	Lise	27
BG4	Erkek	Hemşire	Satın Alma Birimi	Lisans	15
BG5	Kadın	Hemşire	Kalite Verimlilik Birimi	Lisansüstü	11
BG6	Kadın	Hemşire	Hasta Ve Çalışan Hakları	Lisans	2
BG7	Erkek	Avukat (Uzman)	Personel İşleri Birimi	Lisans	8
BG8	Kadın	Tıbbi Teknolog	TİG (Teşhisle İlişkili Gruplar)	Lisans	30
BG9	Kadın	Sağlık Teknikeri	Adli Rapor Hizmetleri	Lisans	12
BG10	Erkek	VHKİ*	Personel İşleri Birimi	Lisans	24
BG11	Erkek	Sağlık Memuru	Sağlık Kurulu	Lisansüstü	16
BG12	Erkek	Bilgi İşlemci	Bilgi Sistemleri Birimi	Lisans	7

* Veri Hazırlama Kontrol İşletmeni

Araştırma kapsamında yapılan görüşmelerde katılımcılara yöneltilen sorulardan elde edilen bulgular aşağıda ayrıntılı olarak sunulmuştur.

4.2. Katılımcıların Bilgi Güvenliği Algısına İlişkin Görüşleri

Bilgi güvenliğinin algısı açısından bütün katılımcıların en çok üzerinde durdukları ortak nokta, bilgilerin yetkisiz kişiler tarafından görülmemesini sağlamak ve mahremiyet konusudur. Konuya ilişkin olarak katılımcıların, kişisel bilgilerin güvenliği, hasta hakları konusunda uygulanan prosedürleri, bilgilerin doğru teşhisi için önemliliğini vurgulayan farklı görüşler bulunmaktadır.

Şekil 1. Katılımcıların Bilgi Güvenliği Algısı

Şekil 1.'de katılımcıların bilgi güvenliğinin hangi açılardan önemli olduğuna ilişkin görüşlerine ait sınıflandırma yer almaktadır. Ayrıca katılımcıları bu konuya ait görüşlerine aşağıda doğrudan da yer verilmiştir.

Kişilere ait bilgilerin üçüncü kişiler tarafından görülmemesini ya da bilgi edinilmemesini sağlamak. Sistemde hastanın, TC kimlik numarası, doğum tarihi ve tüm bilgileri mevcuttur. Bu bilgileri kesinlikle kimsenin görmemesi gerekir." ***(BG 1).***

"Hastaların kişisel mahremiyeti açısından önemlidir. Bu bilgilerin, tıbbi sekreterler ve hekim arasında kalması gereklidir. Yasalar çerçevesinde bilgi güvenliğinin sağlanması açısından kalite standardına uyulması zorunludur. Etiğe aykırı davranışlarda bulunulmaması gerekir. Hemşirelerin bilgi güvenliğinin sağlanmasına dair bilgi yemini vardır." ***(BG2)****.*

"Doğru bilgiye çabuk ulaşabilmek için önemlidir. Arşive indirilen belgelere kolay ulaşmayı sağlar. Çalışanlar ve yetkili kişiler ulaşabilir bu bilgilere. İnsanlara daha iyi kaliteli hizmet sunabilmek amaçtır. Hasta ile ilgili veriler doğru teşhis açısından kaydedilmektedir." ***(BG3).***

"*Hasta mahremiyeti açısından önemlidir. Gizlilik ve mahremiyet konusunda dikkat edilmesi gerekir."* ***(BG4).***

"Çünkü hasta mahremiyeti bizim için önemlidir. Her hastanın kendine özel tedavi yönleri ve süreci var. Hasta mahremiyeti hasta ve çalışan güvenliği açısından bilgi güvenliği olması zorunludur. Hiç kimse kendi kişisel bilgisinin kullanılmasını rızası olmadan kabul etmez." ***(BG5).***

"Mahremiyet açısından önemlidir. Aynı zamanda çalışanlar ve hasta mahremiyeti açısından da önemlidir. Bilgiler kişiye özeldir." ***(BG6).***

"Her kurumda olduğu gibi sağlık kurumunda da hasta ve çalışan mahremiyeti önemlidir. Hastaların ve çalışanlarını bilgisini yetkisiz kişilerle paylaşılması bazı aksaklıklara ve istenmeyen problemlere neden olabilir. Örneğin günümüzde dolandırıcılık faaliyetinin artması bilgi güvenliğini gerekli kılar." ***(BG7).***

"Başkasının bilgisine ulaşılmasını engellemek için önemlidir. Hastanın özel durumuyla ilgili olarak, çünkü analiz alınıyor, alınan analizlerde hastanın özel kullandığı, bağımlılık yapan ilaçlarından tutunda kendisiyle ilgili durumlar özel dosyaya not alınıyor. Kimse özel durumlarının başkaları tarafından görülmesini ve ulaşılmasını istemez." ***(BG8).***

"Gizlilik açısından, hasta mahremiyeti açısından önemlidir. Bilgi güvenliği prosedürleri bulunmaktadır." ***(BG9).***

"Hastaların mahremiyeti için önemlidir. Onların bilgilerini gizlemek zorundayız. Amaç, hastanın kişisel ve sağlık bilgilerinin yetkisiz kişilerce görülmemesini sağlamaktır." ***(BG10).***

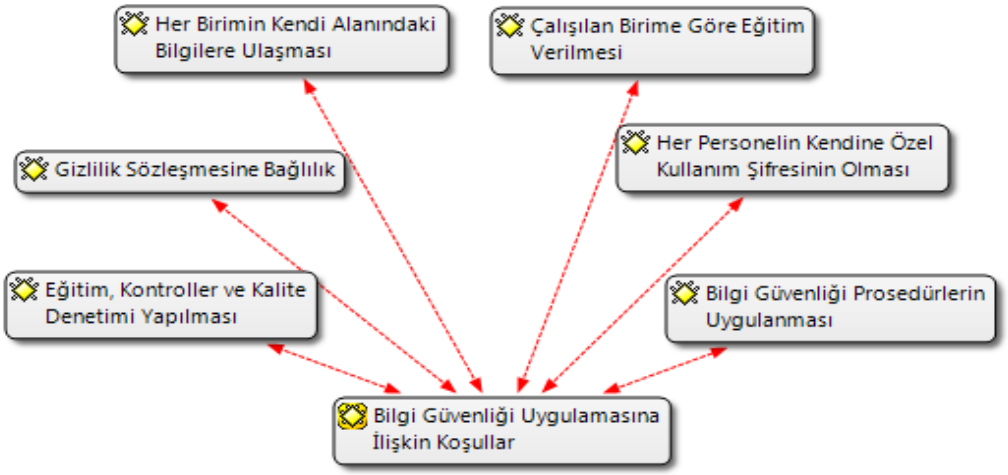
"Kişilerin özel bilgileri var bu bilgiler bankacılık ve her yerde kullanılabilir. Bu sebepten bilgi gizliliği önemlidir. Kişinin sosyal yaşantısını etkileyecek bilgiler olabilir, mahrem konuları olabilir." ***(BG11).***

"Hasta bilgilerinin yetkisiz kişilerce paylaşılmaması gerekir. Hasta bilgilerinin gizliliği bakımından önemlidir." ***(BG12)****.*

4.3. Hastanede Bilgi Güvenliği Yönetiminin Yeterli Olup Olmadığına İlişkin Görüşler

Katılımcıların büyük çoğunluğu (8 kişi) kurumlarında bilgi güvenliği uygulamasını yeterli olarak görmektedir. Yeterli olarak görenler içinde BG1, BG3 ve BG11 kısmen yeterli olduğunu düşünmektedir. Uygulamanın daha çok geliştirilebileceği ve bazı eksiklikler olduğu görüşündedirler. Kurumda yeterlilik düzeyinin eğitimler verilerek, denetim yapılarak ve yasal prosedürlere uyularak sağlandığını belirtmektedirler. En çok üzerinde durulan konu her personelin kendine özel kullanım şifresi olması ve yetkisiz kişilerin bu bilgileri görmesinin engellendiğini vurgulamaktadırlar.

Şekil 2. Bilgi Güvenliği Uygulamasına İlişkin Koşullar



Şekil 2.'de katılımcıların bilgi güvenliğinin yeterliliğine ilişkin görüşlerine ait sınıflandırma yer almaktadır. Ayrıca katılımcıları bu konuya ait görüşlerine aşağıda doğrudan da yer verilmiştir.

*"Şu anda yeterli gibi görünüyor ama daha da bilgi güvenirliliğinin olabilmesi için tüm personelin bilgi güvenliği eğitimi verilmesi gerekir. Gizlilik ilkesinin tüm personele bildirilmesini sağlanmalıdır." (**BG1);***

*"Yeterlidir fakat eğitimler verilerek, kontrolleri sıklaştırarak daha fazla geliştirilmesi sağlanabilir. Bilgilerin sadece hastanın kendisine verilmesi sağlanabilir. Hastanede bütün yönetici ve personelin bunun bilincinde olması gerekir." **(BG2);***

*"Tam anlamıyla yeterli değildir. Yer sıkıntısının olması arşivlerin saklanmasını zorlaştırabiliyor. Bilgisayar doğru ve tam kullanılarak bilgilere erişim sağlanıyor." **(BG3);***

*"Yeterlidir. Çünkü herkesin bilgisayarında kendilerine ait kullanım şifresi bulunmaktadır. Bu bilgiler yetkili olmayan kişilerle paylaşılmamaktadır." **(BG4);***

*"Şuan bizim hastanemiz için yeterlidir. Bilgi güvenliği uygulamasında herkese gizlilik sözleşmesi imzalatıyoruz. Herkesin kendi yetki sınırı var. Bir tıbbi sekreter, bir doktor veya bir personel kendi modülünden sınırlı alanda yetkilendirilmiş alanı vardır. Her servis bilmesi gerektiği alanı bilir, yetkisi dışında olan hiçbir şeyi göremez. Herkes kendine sınırlandırılmış ve yetkilendirilmiş alanı görür. Böyle olduğu içinde bilgi sızdırma gibi bir olay olamaz." **(BG5)**;*

*"Şuan yeterli görüyorum. Dosyalar hastane personeli dışında kimse taşımıyor, dosyalar ortada durmuyor, elden dosya teslim edilmiyor kendi birimim adına böyle olduğunu düşünüyorum." **(BG8);***

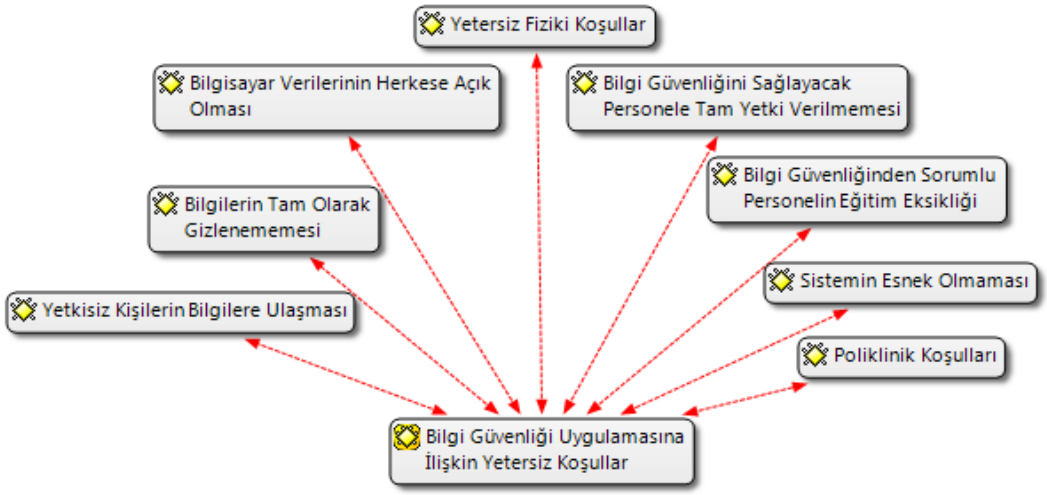
*"Kısmen yeterli, tam anlamıyla yeterli değil. Kişi hastaneye girdiğinde, parmak izi, retina taraması veya resmi çekilerek muayeneye başlarsa muayeneye sırasında ne bilgiler elde edilmiş öğrenilebilir ve başkasının görmesi engellenebilir. Bu şekilde başkasının yerine muayene olma durumunun da önüne geçilmiş olur. Hasta bilgilerinin personel tarafından kötüye kullanılması engellenmelidir." **(BG11);***

*"Alınan önlemlerle yeterli olduğunu düşünüyorum. Hasta hakları konusunda hassasiyet gösterilmesi önemlidir. Gizlilik sözleşmesine bağlı olarak her birim kendi yetki alanında bulunan bilgilere ulaşabiliyor." **(BG12).***

4.4. Katılımcıların Bilgi Güvenliği Uygulamasında Yetersiz Koşullara İlişkin Görüşleri

Katılımcılar kurumlarında bulunan yetersizlikleri ağırlıklı olarak şu şekilde gruplandırmaktadırlar. Yetersiz fiziki koşullar, bilgi güvenliğinden sorumlu personelin eğitim eksikliği ve bilgilerin tam olarak gizlenemediğini yetkisiz kişilerin ulaşabildikleri görüşündedirler. Ayrıca, hastaların bazı durumlarda başka biri yerine muayene olma durumu olduğunu belirtmektedirler. Bu bağlamda bilgi güvenliğinin tam olarak uygulanamadığı söylenebilir.

Şekil 3. Bilgi Güvenliği Uygulamasına İlişkin Yetersiz Koşullar



Şekil 3.'de katılımcıların bilgi güvenliği uygulamasına yetersiz koşullara ilişkin görüşlerine ait sınıflandırma yer almaktadır. Ayrıca katılımcıları bu konuya ait görüşlerine aşağıda doğrudan da yer verilmiştir.

"Yeterli değildir. Çünkü bilgisayar uygulamalarında yeterli donanım yoktur. Gizliliği olan birimlerin tek odalarda çalışmaları gerekir. Her birimin kendine özel odaları olmalıdır." ***(BG6);***

"Yetersizdir. Bilgisayar kurumumuzda görevli personelin veya hasta ve çalışan bilgilerine ulaşan personelin, gizlilik ve mahremiyet konusunda eğitimlerinin eksikliği bulunmaktadır." ***(BG7);***

"Yeterli değil. Çünkü bizim hastanede bu programları kullanan herkes, istediği hastanın bilgisine ulaşabiliyor. Hastanede kullanılan bir Karmek programı var bu programı kullanmayı bilen herkes istediği bilgiye ulaşabiliyor. Bir sınırlama yok." ***(BG9);***

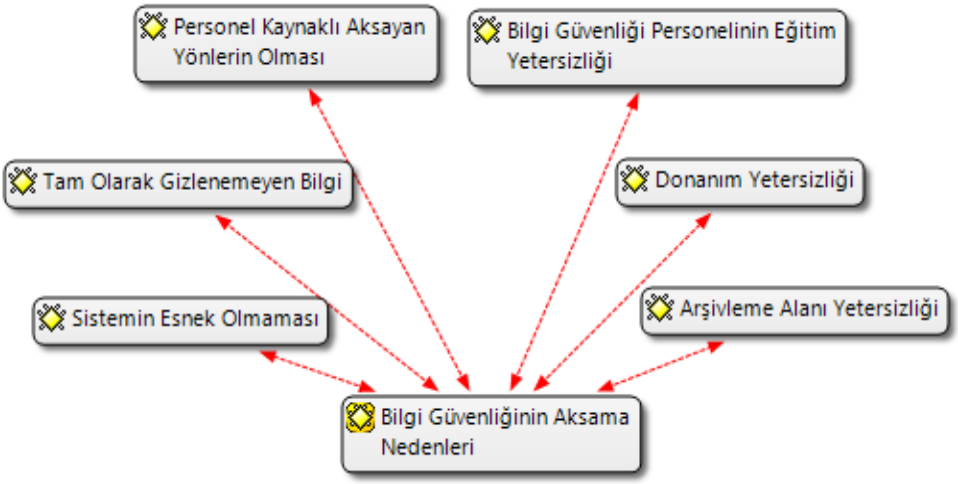
"Yeterli değildir. Sistemin tam olarak oturmaması esneklik olmasından dolayı yeterli değildir. Çünkü hasta servise gittiğinde bilgilerini paylaşmak durumunda kalıyoruz. Bilgiler tam olarak gizlenemiyor." ***(BG10)***, yeterli olarak görmemektedirler.

4.5. Katılımcıların Bilgi Güvenliğinin Aksama Nedenlerine Ait Görüşleri

Katılımcılardan BG1, BG2, BG3 ve BG11 aksayan bir yönün olmadığını belirtmektedirler. BG1, BG2 ve BG11 hasta hakları prosedürlerinin uygulandığını, Bilgi Güvenliği uygulamasının düzenli aralıklarla kontrol edildiğine ve uygulamada daha dikkatli olunduğu görüşündedirler. BG4, bazı durumlarda aksaklık olabildiğini, bilginin dışarıya sızdırılması ile olabileceğini vurgulamaktadır.

Katılımcılardan 7 kişi, BG5, BG6, BG7, BG8, BG9, BG10, BG12, kurumda bulunan aksayan yönü şu şekilde açıklamışlardır. Daha çok, yeterli donanımın olmaması ve bilgilerin her personele açık olması vs. aksayan yönleri üzerinde durmuşlardır. Doktor ve hasta arasındaki bilgilerin diğer kişiler tarafından bilinmesi, fiziki koşulların yetersizliği yönünden, personelin BG konusunda eğitim eksikliği, geçmiş tarihte bulunan dosyalara ulaşmada sıkıntı çıkması, tanıdık vasıtasıyla bilgilere ulaşma ve personel kaynaklı aksayan yönün olduğunu vurgulayan farklı görüşler bulunmaktadır.

Şekil 4. Bilgi Güvenliğinin Aksama Nedenleri



Şekil 4.'de katılımcıların bilgi güvenliğinin aksama nedenlerine ilişkin görüşlerine ait sınıflandırma yer almaktadır. Ayrıca katılımcıları bu konuya ait görüşlerine aşağıda doğrudan da yer verilmiştir.

"Şu anda bilgi güvenliği ile ilgili aksayan bir yönümüz yok. Ama ne kadar da dikkat edersek o kadar iyi olur. Bütün personelin dikkatli olması gerekiyor. Hizmetlisinden doktoruna tüm alandaki personelin bilgi güvenliğini uygulaması gerekiyor." ***(BG1).***

"Kurumumuzda aksaklık yoktur. Bilgi güvenliği komitesi bulunuyor. Düzenli aralıklarla toplantı yapılıyor. Bilgi işlem sorumlusu bulunmaktadır. Şuan için bir aksaklık bulunmamaktadır." ***(BG2).***

"Bazı durumlarda bu aksaklıklar olabilmektedir. Satın alma biriminde, firmalar teklif sunmaktadır. Ve hiçbir firma başkasının verdiği teklifi bilmemelidir. Poliklinik bölümünde ise mahremiyet ve gizlilik açısından hastaların tek tek muayene olmaları gerekmektedir." ***(BG4).***

"Şöyle bir aksayan yönü var. Mesela, doktor hastayı muayene ederken tıbbi sekreterler görebiliyor. Tek aksayan yönü budur. Gelecekte, tıbbi sekreter ve doktorları ayırdıkları için bu olayda kalmayacak." ***(BG5).***

"Kurum olarak farklı birimde olanların aynı odada bulunması gizliliğin etik olmasını engelleyebilir. Çünkü her birimin kendine özel görebileceği bilgiler vardır. Yönetim açısından yeterli fiziki koşulların oluşturulmamasıdır." ***(BG6).***

"Vardır. Kurumun, personel eğitimleri verilerek daha da güvenli hale getirilmesini sağlar artı sistemin hacklenmesine karşı koruyucu önlemlerin alınmasını sağlar ve mevzuat konusunda personelin eğitilmesi gerekir." ***(BG7).***

"Sadece bizim birimde şu konuda aksayan yönleri oluyor. Hasta taburcu olduğunda başka hastaneye gittiğinde, bu hastanede yapılan işlemleri belgeleyen dosyalarına ulaşmak istiyor. Bu hastanede bulunan bilgilerinin birçoğu verilmiyor. Sadece tahlil sonuçları ve birkaç belge veriliyor. Hastalara taburcu olurken tüm bilgiler sadece hastanın kendisine verilmesi gerekir. Hangi tahlillerin, yapıldığı sonuçların ne olduğu ve teşhis konusunda hastaya belge şeklinde verilmelidir. Çünkü hasta geri geldiğinde dosyalar arama konusunda sıkıntı çıkmaktadır." ***(BG8).***

"Evet, aksayan yönleri var. Çünkü herkesin bu kayıtlara ulaşabilmesini engellemek için buna sınır getirilmelidir." ***(BG9).***

"Aksayan yönleri vardır. Özellikle, kişiler tanıdık vasıtasıyla dosyalara ulaşılabiliyor. Özellikle yüksek üst kurumdan tanıdıkları varsa daha kolay bilgilere dosyalara ulaşabiliyorlar. Bilgi güvenliği tam olarak yapılamamaktadır. Yazılım sisteminde bir kişinin görmesi gereken bilgiyi en az 3-5 kişi görebiliyor. Bu sebepten bilgi güvenliği zor uygulanıyor." ***(BG10).***

"Çalıştığım birimde aksayan bir yön yok. Belirli bir strateji var. Kişinin kendisi hariç bu bilgilere ulaşamaz. Hasta yakınlarının ulaşabilmesi için kişinin vasisi olması gerekir. Hasta hakları prosedürüne göre hareket edilmelidir. Hangi durumlarda bilgi verilebildiği belirlenmiştir. Çalışan eğitimi yapılmalıdır. Bilgisayar tabanlı bilgi sızdırılması engellenmelidir. Doğru yapılandırma yapılmalıdır. Bu bilgiler hasta dışında sadece veli ya da vasisi olan kişiye verilmelidir." ***(BG11).***

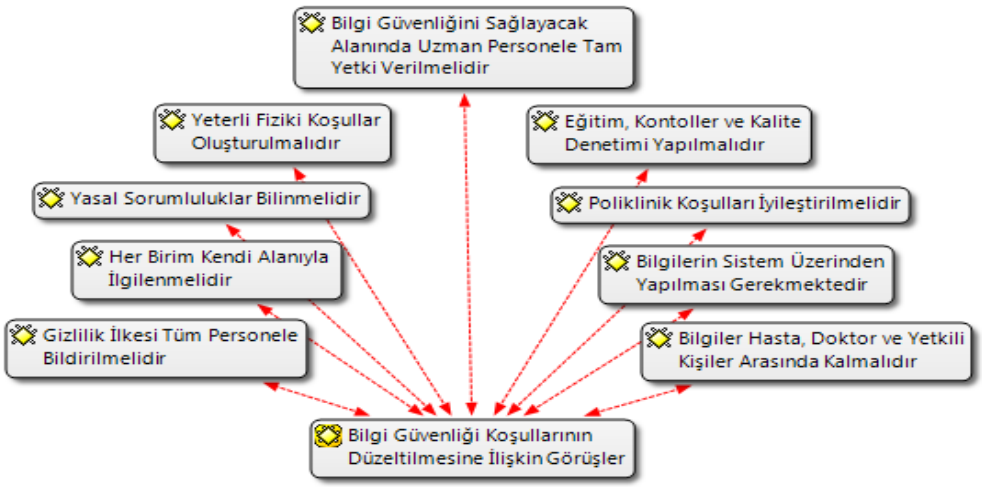
"Personel kaynaklı aksayan yönleri vardır. Bu konuda önlemlerin alınması şu şekilde olabilir. Kontroller artırılabilir, personelin gizlilik prosedürlerini dikkatli şekilde uygulaması sağlanmalıdır. Sistemsel aksayan yönleri yok fakat kullanıcı kaynaklı aksayan yönleri vardır. Aksayan yönleri tespit edildiğinde eğitim verilerek düzeltilmesi sağlanıyor." ***(BG12).***

4.6. Katılımcıların Bilgi Güvenliği Koşullarının Düzeltilmesine İlişkin Görüşleri

BG'nin sağlanmasına yönelik görüşlerde bulunan katılımcılar, bu süreçte eğitimin çok önemli olduğunu belirterek uygulamanın her birimde kendi alanına göre eğitim verilmesinin uygun olduğunu düşünmektedirler. Katılımcılardan, BG2, BG3, BG4, BG6 ve BG12 eğitimin önemine vurgu yapmışlardır. Görevli personele kendi alanında eğitim ve seminerler verilerek bilgi güvenliğini bu şekilde sağlandığını düşünmektedirler. Bazı katılımcılar, alanında uzman personel ile çalışmak gerektiğine belirtmektedirler. Yasal prosedürlere uyularak kuralların daha çok sistemleştirilmesi gerektiğini bu bağlamda yaptırım olabilme düşüncesiyle ilgili personelin daha dikkatli olabileceğine vurgu yapmaktadırlar. Hastanın muayene sırasında doktor ve sadece kendisi olması gerektiğine vurgu yapan bazı katılımcılar ileriki yıllarda tıbbi sekreterler ve doktorların aynı ortamda çalışmasının engelleneceği için bu sorunların ortadan kaldırılacağı görüşündedirler. Ayrıca hasta muayene olurken sıradaki hastalarında içeri alındığını bu nedenle herkesin birbirlerinin mahrem konularını öğrenebildiği bunun kesinlikle engellenmesi gerektiği görüşü mevcuttur.

Genel anlamda bilgilerin sadece hastanın kendisine verilmesi gerektiğini veya vasisi olan kişiye verilmesini gerektiğini savunmuşlardır. Bu bilgilerin hasta, doktor ve sadece yetkili kişiler arasında kalması gerektiğinin doğru olacağını düşünen bazı katılımcılar, bunu sağlamak için de alanında uzman personel ile çalışarak ve yasal prosedürlere uyularak olabileceği görüşündedirler.

Şekil 5. Bilgi Güvenliği Koşullarının Düzeltilmesine İlişkin Görüşler



Şekil 5.'de katılımcıların bilgi güvenliği koşullarının düzeltilmesine ilişkin görüşlerine ait sınıflandırma yer almaktadır. Ayrıca katılımcıları bu konuya ait görüşlerine aşağıda doğrudan da yer verilmiştir.

"Eğitimler verilmeli, kullanılan bilgisayarların veri girişlerinin herkese açık olmaması, bilgilerin saklanabilir, gizlenebilir özelliğinin olması. Bilgisayarların sürekli dışardan gelecek olan virüslere karşı sürekli olarak güncel tutulması gerekir. Tüm personelin, bilgi güvenirliği açısından hasta bilgilerini kimseyle paylaşmamalıdır. Hastanın bilgilerini kullanarak işlem yapılması çok kolaydır, bu durum açısından güvenlik önemlidir. Doğru bilgi hasta ve personel için önemlidir. Personel arşivlerin veya hasta arşivlerinin denetlenmesi ve dosyaların her

personele verilmemesi gerekir. Kimlik bilgileri veya hastalık bilgilerinin personele ya da dışardan kişilere bu bilgilerin hastaya ait kimliğinin görülmeden verilmiyor. Hasta yakınlarına hastanın kimliği varsa bilgiler veriliyor." ***(BG1).***

"Kurumumuzda, uygulama, eğitim, kontroller ve kalite denetimi yapılarak sağlanmaktadır. Yetkili personel dışında hasta bilgilerinin paylaşılmaması esastır." ***(BG2).***

"Yılın belirli sürelerinde arşivle ilgili eğitim ve seminerlerde bilgiler veriliyor. Arşiv bilgilerinde burada bulunan sadece personeller ulaşabiliyor." ***(BG3).***

"Eğitim ve seminerler verilerek sağlanmalıdır. Denetim yapılmalıdır. Yanlış bilgilerin olmaması için kontrol mekanizması oluşturulmalıdır. Ayrıca teknik aksaklıkların oluşması engellenmelidir. Hastaya ait bilgilerin sadece yetkili kişiler tarafından gizlilik politikasına uygun olarak paylaşılması gerekmektedir." ***(BG4).***

"Öncelikle iyi bir yazılım sistemi olması gerekir. Bunun için aktif iyi bir yazılım firmasıyla çalışıyor olmak gerekiyor ki hiçbir şekilde bilgi sızdırması olmasın. Bu açıdan herkes kendi kişisel şifre bilgilerini kimseye vermez. Çünkü herkesin kendi kullanıcı adı ve şifresi var. Kimseye verilmediği müddetçe hiçbir sıkıntı yok." ***(BG5).***

"Eğitimler veriliyor. Şuan eğitimler hastanede online sistem üzerinden yapılmaktadır. Öncelikle şirket personeli tarafından sunuluyor. Hastaneye yeni başlayanlar için oryantasyon eğitimi verilerek bilgi güvenliği konusunda gerekli prosedürler anlatılıyor. Hasta hakları çalışan haklarına dair oryantasyon eğitimi veriliyor. Programlar üzerinden yeterli online duyuruların yayınlanması ile kimseye ulaşılamadı durumu olmuyor. Personelin bilmesi gereken duyurular herkesin sisteminden duyuruluyor." ***(BG6).***

"İyi bir bilgi işlem personeliyle ve alanında uzman personelleri değerlendirmek gerekir." ***(BG7).***

"Her şeyin sistem üzerinden olması gerekir ve her yetkili kişinin de şifresi olacak kişiye tanımlı olmalı, onun dışında kimse ulaşamayacak. Çünkü hasta birçok birimden hastane personeli sayesinde birçok bilgisini görebilir. Bunun olmaması için bilgi güvenliği önemlidir. Sınırlamalar şuan var fakat daha detaylandırılabilir. Örneğin kendi verilerimle karşılaştırabilmem için istatistik verileri bana açıldı ben görebiliyorum başkası göremiyor. Ama bazı yerlerde veriler açık, onlarda da sınırlama olabilir. Burada en önemli şey hasta taburcu olurken hastaya yapılan işlemler hastanın yakınlarına değil hastanın kendisine bilgiler ve belgeler verilmelidir. Hasta kendi bilgilerini kendi korusun." ***(BG8).***

"Bu sisteme kısıtlama getirilebilir. Herkes sadece kendi alanında kendi bölümüyle ilgili bilgilere ulaşabilir. Bunun çalışmaları var fakat ne kadar sürede nasıl yaparlar bilemiyorum. Mesela kayıt verirken şu anda her bölüm kendi bölümüne kayıt vermeye başladı. Devamlı eğitim programları veriliyor. Ve bu kişinin çalıştığı birime göre değişiyor. Hemşireye, sağlık memuruna, kayıt memuruna, temizlikçiye vb. her birine ayrı ayrı eğitim programları veriliyor." ***(BG9).***

"En azından bilgi güvenliğini sağlayacak kişilere tam yetki verilmesi sağlanabilir. Yetkili kişilerin gördüğü bilgiyi başkası görmemesi gerekir. Bu işlerden sorumlu kişiler görevlendirilmesi gerekir." ***(BG10).***

"Uygulamayı bilen kişi bunun hangi koşullarda sağlanması gerektiğini belirler. Hasta mahremiyeti için, poliklinikte muayeneye on kişi birden giriyor. Böylece orda olan kişiler birbirlerinin bilgilerini ve mahremiyetini öğrenebiliyor. Çalışma koşulları, poliklinik koşulları, bilginin başka kişilerle paylaşılmaması önemlidir. Her birim kendi bilgilerini görebiliyor." ***(BG11).***

"Görevli personele eğitim verilerek sağlanabilir. Hastanın tanıdığı vasıtasıyla üçüncü kişilere bilgiler verilmesi engellenmelidir. Böyle durumlar çok sık olmasa da bazı birimlerde olabiliyor. Hasta mahremiyeti için poliklinikte muayene sırasında tek hasta alınmalıdır." ***(BG12).***

5. DEĞERLENDİRME

Günümüzde bilişim teknolojilerinin, kullanımının yaygınlaşması ile birlikte risk faktörlerinin belirlenmesi zorunlu hale gelmiştir. Kurumsal bilgi güvenliğine gereken önemin verilmesi ve güvenlik politikalarının belirlenmesi bu hizmeti kullananlar için büyük katkı sağlayacaktır. Genel olarak bilgi güvenliği konusunda ne kadar önlem alınsa da riskleri sıfıra indirgemek çokta mümkün olmamaktadır. Tehdit unsurlarına sürekli uyanık olmak, güvenlik politikalarını etkin bir şekilde uygulamak, süreçleri izlemek, elde edilen sonuçların ve yeni gelişmelerin güncellemeleri yapılarak risk faktörü en aza indirilebilir. Kurumların bu konuya önem vermesi, hassasiyet

gösterilmesi, önlem alınması, bilgi birikiminin artırılması ve farkındalık oluşturması gerekmektedir (Canbek ve Sağıroğlu, 2006:172). İnsan hayatı için önceliğe sahip olan sağlık hizmetlerinin hızlı ve güvenilir olması beklenir. Bu bakımdan kullanıcı görüşlerinin dikkate alınması olumlu yönde değerlendirilip hayata geçirilmesi sayesinde bilgi güvenliğinin kullanılabilirliği artacaktır. Bilgi sistemlerinin işleyişi ve nasıl kullanılacağı konusunda gerekli bilgilerin, belgelerin sağlanması ve eğitimlerin verilmesi, işlemlerin etkili, hızlı, doğru ve güvenli yapılmasına faydası olacaktır (Yılmaz ve Demirkan, 2012:27). BGYS uygulanması aşamasında üst yönetimin ve tüm çalışanların destek vermesi, işbirliği içinde bulundukları kişi veya kuruluşların da belirlenen politikalara uyma zorunluluğu getirilmesi, bilgi güvenliğinin üst seviyede gerçekleşmesine katkı sağlayacaktır (Vural ve Sağıroğlu, 2008:520).

Araştırma bulgularına göre, bu çalışmada sağlık personeli ile yapılan görüşmede aynı kurumda, farklı birimlerde çalışanların birbirleriyle çelişen cevaplar verdiği görülmüştür. Bazı çalışanlar kurumlarında bilgi güvenliğini yeterli olarak görmekteyken bazıları yetersiz görmektedir. Bunun nedeninin birimler arası iletişim eksikliği, fiziksel, elektronik ve sosyal ortamlarda paylaşılan bilginin belirlenen politikaların uygulanmasında farklılık göstermesi, bazı çalışanların bu konuda yeteri kadar duyarlı olmaması, kullanıcıların bilgi güvenliği yönetim sisteminin kullanılabilirliğinin kişilere göre değişmesi veya bu konuda bilgi sahibi olmamaları olduğu düşünülmektedir.

Araştırma yapılan hastanede, dosyalar ve belgeler dijital ortamda tam otomasyon ile yapılmamaktadır. Daha az insan ile elektronik ortamda hastane otomasyonun yapıldığını söylemek mümkündür. Kullanımı kolay, güçlü ve güvenilir tam otomasyon programı geliştirilme aşamasındadır. Bu bakımdan otomasyon programı, bilginin yönetilmesi ve kontrol edilmesi için bilgi yönetim sistemlerinde işlemlere hız kazandırması hedeflenmektedir.

6. SONUÇLAR VE ÖNERİLER

Bu çalışmada, hastanelerde bilgi güvenliği yönetimine ilişkin, sağlık personelinin görüşleri araştırılmıştır. Katılımcıların bu konuda bilgi sahibi oldukları, gerekli önlemleri aldıkları görülmüştür. Bazı aksaklıkların olduğunu fakat bunların gerekli tedbirleri alarak ve personele eğitim verilerek daha da azaltılabileceği görüşündedirler. Bilgi güvenliği konusunda katılımcıların çoğunluğu hasta mahremiyeti üzerinde durmuşlardır. Bu konuya önem verdiklerini ve daha duyarlı olduklarını belirtmişlerdir. Bilgi güvenliğinin sağlanabilmesi ve sürdürülebilmesi için yönetimin tutumuna bağlı olarak öncelikle veri sorumlusunun kanun hükümlerine göre gerekli denetimleri yapması gerektiği görülmektedir. Bilginin, gizlilik, bütünlük ve erişilebilirliğin birbirleriyle bağlantılı olduğu ve bunu sağlayan yönetim ve personel tarafından kullanılmasına imkân veren faaliyet olarak değerlendirilmektedir.

Yeterli fiziki koşullar oluşturularak, yasal sorumluluklar çerçevesinde alanında uzman kişilere yetki verilerek, bilgi güvenliğinin oluşturulması sağlanmalıdır. Ayrıca sağlık çalışanlarının bu konuda daha hassas olmaları ve bilgi paylaşımının veri sorumlusu denetiminde, hasta, doktor ve yetkili kişiler arasında kalması gerekmektedir. Bilgi paylaşımının sistem üzerinden yapılması erişilebilirlik ve güvenlik açısından önemli olarak değerlendirilir.

Sağlık kurumlarında uygulanan bilgi güvenliği yönetim sistemi, bilgi güvenliği risk yönetimi açısından büyük bir öneme sahiptir (Zarei, Sadoughi, 2016; Hou vd., 2018). Bu amaçla yaygın olarak kullanılan ISO 27001 bilgi güvenliği yönetim sisteminin hastanelerde her bir süreci ve alt süreci içerek şekilde ele alınması gerekmektedir (Tavakoli vd., 2014). Bu doğrultuda planlanan bu çalışma ile hastanelerde bilgi güvenliği yönetim sisteminin uygulamasında ortaya çıkan sorunlar tespit edilip çözüm önerileri geliştirilmiştir. Araştırmanın ana ve alt amaçları doğrultusunda, sisteminin sorunları hakkında başka araştırmalarla ile doğrulanabilecek sonuç içermektedir. Her alanda kullanılan bilgi teknolojileri sayesinde sağlık çalışanlarının işler kolaylaşmaktadır. İhtiyaç duydukları anda bilgiye kolaylıkla ulaşabilmektedirler. Burada amaç, bilginin gizliliği, bütünlüğü ve erişilebilirliğini sağlamaktır. Kurumlar iyi bir yazılım ve donanıma sahip olmalarının yanında eğitilmiş bir personel sayesinde hedeflerini gerçekleştirebilirler.

Araştırmadan elde edilen bulgular sonucunda katılımcıları görüşleri genel olarak değerlendirildiğinde;

- Bilgi güvenliği olgusunun katılımcılar tarafından en çok "hasta mahremiyeti" olgusuyla birlikte algılandığı,
- Poliklinikte muayene sırasında içeri alınan diğer hastaların hasta ve doktor arasında kalması gereken bilgilerin diğer kişiler tarafından öğrenilmesine sebep olduğu,
- Bilgi gizliliğine genel olarak önem verildiği fakat bazı birimlerde bunun çok fazla uygulanamadığı,

- Fiziki koşulların tam oluşturulamadığı, bunun sonucu olarak da farklı birimlerin aynı odada bulunmaları ile bilgi gizliliğin tam olarak sağlanamadığı,
- Hastanın özel durumuyla ilgili bilgilerinin başkaları tarafından bilinmesinin kişinin sosyal hayatını etkileyebildiği,
- Sağlık çalışanlarına bilgi güvenliği yönetim sürecinde farkındalık ve duyarlılık eğitimleri verilmesine rağmen bazı birimlerde informal olarak (bir tanıdık vasıtasıyla) hasta bilgilerine ulaşılabildiği,
- Her personelin kendine özel şifresinin olmasının bilgi güvenliği yönetim sürecine adına önemli bir adım olduğu,
- Bilgi güvenliğinden sorumlu bazı personelin eğitim ihtiyacı olduğu,
- Kontroller artırılarak, yasal mevzuat ve gizlilik prosedürlerin uygulanmasında personelin daha hassas olması gerektiği,
- Bilgi güvenliği yönetim sürecinde yaşanan aksaklıkların daha çok personel kaynaklı olduğu tespit edilmiştir.

Sonuç olarak, personelin gerekli özeni gösterdiği fakat eğitim eksikliği, donanım eksikliği, uzman personele tam yetki verilmemesi ve yeterli fiziki koşulların sağlanamaması ile bilgi güvenliği uygulamasının tam olarak yerine getirilemediği görülmüştür.

Bu doğrultuda araştırma kapsamında aşağıdaki öneriler geliştirilmiştir.

- Sağlık çalışanlarının ve hastaların bilgi güvenliği bağlamında haklarının ihlal edildiğini düşündükleri durumlarda hastanede başvurabilecekleri bir birimin bulunması,
- Yeterli donanımın oluşturularak güvenlik amacıyla biyometrik yöntemlerin yaygınlaştırılması,
- Tüm personele bilgi güvenliği eğitimi verilmesi,
- Bilgi güvenliği yönetim sistemine ait süreçler sorumluluklar ve görevlerin belirlenmesi,
- Bilgi güvenliğini sağlayacak personele tam yetki verilmesi, yetkili kişilerin gördüğü bilgiyi başkasının gör(e)memesi,
- Bilgi güvenliği yönetim sisteminin etkili işlemesi amacıyla, yöneticiler ve çalışanların işbirliği içinde olması,
- ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı kullanımının tüm hastanelerde yaygınlaştırılmasını sağlamak amaçlı gerekli şartların oluşturulması,
- Poliklinikte hastanın muayenesi sırasında mahremiyeti ihlal edecek unsurların ortadan kaldırılması, bu amaçla poliklinik koşullarının iyileştirilmesi,
- Sağlık bakanlığı tarafından uygulamaya konan, muayene sırasını bekleyen hastaların LCD ekranda istedikleri takdirde isimlerinin gizlenmesi ve uygulamanın yaygınlaştırılması,
- Profesyonel yazılım firmalarıyla çalışılması,
- Tehditler ve riskler belirlenerek acil durumlarda uygulamaya konulacak önlemlerin alınması,
- "Temiz masa temiz ekran" ilkesinin tüm çalışanalar tarafından benimsenmesinin sağlanması,
- Hasta ve hastaneye ait bilgilerin üçüncü kişilerce paylaşılmaması amacıyla informal kanalların kullanımını ortadan kaldırmak amacıyla personelin yaptırımlardan haberdar edilmesi ve gerekirse cezai işlem uygulanması önerilmektedir.

KAYNAKÇA

Akay, İ.G. (2014). "Bilgi Güvenliği Yönetim Sistemleri: Bilgi Güvenliği Uygulama Mülakatları", Yüksek Lisans Tezi, Bilecik Şeyh Edebali Üniversitesi Sosyal Bilimler Enstitüsü, Bilecik.

Aksu, P.K. (2014). "Hastane Bilgi Yönetim Sisteminin Bilgi Güvenliği Açısından Değerlendirilmesi", Doktora Tezi, Marmara Üniversitesi Sağlık Bilimleri Enstitüsü. İstanbul.

Altındiş, S. (2010). "Bilgi Yönetimi Uygulamalarının Hasta güvenliğine Katkısı: Kavramsal Bir Çerçeve", İktisadi ve İdari Bilimler Fakültesi Dergisi, 15(3), 325-352.

Arslan, E.T. ve Demir, H. (2017). "Sağlık Çalışanlarının Hasta Mahremiyetine İlişkin Tutumu: Nitel Bir Araştırma", AİBÜ Sosyal Bilimler Enstitüsü Dergisi, 17(4), 191-220.

Aslandağ, K. (2010). "Bilgi Güvenliği Kavramı ve Bilgi Güvenliği Yönetim Sistemleri İle Şirket Performansı İlişkisine Dair bir Uygulama", Yüksek Lisans Tezi, Gebze Yüksek Teknoloji Enstitüsü Sosyal Bilimler Enstitüsü. Gebze.

Atlas.ti (2018). https://atlasti.com/free-trial-version/, (Erişim Tarihi: 6 Aralık 2018).

Başdinkçi, N. (2017). "Sağlık Kurumlarında Bilgi Güvenliği Risk Değerlendirilmesi ve Kullanıcıların Bilgi Güvenliği Farkındalık Düzeyinin Ölçülmesi", Yüksek Lisans Tezi, Çukurova Üniversitesi Fen Bilimleri Enstitüsü. Adana.

Canbek, G. ve Sağıroğlu, Ş. (2006). "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", 9(3), 165-174.

Creswell, J.W. (2014). "Research Design: Qualitative, Quantitative, And Mixed Methods Approaches", Singapore, Sage Publications.

Creswell, J.W. (2013). Nitel Araştırma Yöntemleri Beş Yaklaşıma Göre Nitel Araştırma ve Araştırma Deseni, M.Bütün ve S.B.Demir (Çev.), Siyasal Kitabevi, Ankara.

Çayır, M.Y. ve Sarıtaş, M. T. (2017). "Nitel Veri Analizinde Bilgisayar Kullanımı: Bir Betimsel İçerik Analizi (2011-2016)", Necatibey Eğitim Fakültesi Elektronik Fen ve Matematik Eğitimi Dergisi, 11(2), 518-544

Disterer, G. (2013). "ISO/IEC 27000, 27001 and 27002 for Information Security Management", Journal of Information Security, (4), 92-100.

Evrin, V. ve Demirer M. (2011). Kurumsal Bilgi Güvenliği Süreç Çalışmaları: ISO/IEC-27001 Örneği, IV.Ağ Ve Bilgi Güvenliği Ulusal Sempozyumu, 25-33, Atılım Üniversitesi, Ankara.

Gerçeker, B. (2012). "Sağlık Kuruluşları Örgüt İklimi ve Bilgi Güvenliğinin İlişkisi", Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sağlık Bilimleri Enstitüsü. İzmir.

Gülmüş, M. (2010). "Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği", Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü. İstanbul.

Hou, Y., Gao, P. ve Nicholson, B. (2018). "Understanding Organisational Responses To Regulative Pressures in Information Security Management: The Case of a Chinese Hospital, Technological Forecasting and Social Change", 126, January, 64-75.

Ismail, W., Alwi, N. H., Ismail, R., Bahari, M. ve Zakaria, O. (2013). "Readiness of Information Security Management Systems (ISMS) Policy on Hospital Staff Using e-Patuh", Journal of Telecommunication, Electronic and Computer Engineering, 10(1), 47-52.

İleri, Y.Y. (2016). "Örgütlerde Bilgi Güvenliği Yönetimi, Kurumsal Entegrasyon Süreci ve Örnek Bir Uygulama", Anadolu Üniversitesi Sosyal Bilimler Dergisi, 4(17), 55-72.

İzgi, C. (2014). "Mahremiyet Kavramı Bağlamında Kişisel Sağlık Verileri", Türkiye Biyoetik Dergisi, 1(1), 25-37.

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

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

Mehraeen, E., Ayatollahi, H. ve Ahmadi, M. (2016). "Health Information Security in Hospitals: the Application of Security Safeguards", Department of Health Information Management, School of Paramedicine, Tehran University of Medical Sciences , 1(24), 47-50.

Ömürbek, N. ve Altın, F.G. (2009). "Sağlık Bilişim Sistemlerinin Uygulanmasına İlişkin Bir Araştırma: İzmir Örneği", (19), 211-232.

Özata, M. ve Özer, K. (2016). "Hastanelerde Hasta Mahremiyetine Yönelik Uygulamalarının Sağlıkta Kalite Standartları Bağlamında Değerlendirilmesi: Konya Örneği", The Journal of Academic Social Science Studies(45), 11-33.

Resmi Gazete (2010). "Elektronik Haberleşme Güvenliği Kapsamında TS ISO/IEC 27001 Standardı Uygulanmasına İlişkin Tebliğ", Sayı 27730, http://www.resmigazete.gov.tr/eskiler/2010/10/20101015-9.htm, (Erişim Tarihi: 6 Aralık 2018).

Resmi Gazete (2012). Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi ve Gizliliğinin Korunması Hakkında Yönetmelik, Sayı 28363. http://www.resmigazete.gov.tr/eskiler/2012/07/20120724.htm, (Erişim Tarihi: 6 Aralık 2018).

Sağlık Bakanlığı. (2014). Bilgi Güvenliği Politikalar Klavuzu, http://www.BilgiGüvenliğiPolitikalarıKılavuzu, (Erişim Tarihi: 19 Nisan 2018).

Sağlık Bakanlığı. (2018). Bilgi Güvenliği Politikalar Klavuzu, http://www.BilgiGüvenliğiPolitikalarıKılavuzu, (Erişim Tarihi: 9 Ağustos 2018).

Susanto, H., Almunavar, M.N. ve Tuan, Y.C., (2011). "Information Security Management System Standards: A Comparative Study of the Big Five", International Journal of Electrical & Computer Sciences, 11(5), 23-29.

Tavakoli N, Ehteshami A, Hassanzadeh A ve Amini F. (2014). Information Security Management in Isfahan University of Medical Sciences'Academic Hospitals in 2014. Int Journal Health System Disaster Management, (2),175-9.

Uğuz, S. (2018). " Kurumsal Bilgi Güvenliği Yönetim Sistemi Yazılımları: Örnek Bir Yazılım Geliştirilmesi", Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi, 2(1), 1-11.

Varol, Ş., Orhan, F., Tuncer, S. ve Akyüz, S. (2016). "Sağlık Kurumlarında Bilgi Güvenliği Bağlamında Biyometrik Sistemler", Sağlık Akademisyenleri Dergisi, 3(4), 155-162.

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

Yılmaz, G.K. (2014). Durum Çalışması. (Kuramdan Uygulamaya Eğitimde Bilimsel AraştırmaYöntemleri İçinde, Editör: Mustafa Metin) Pegem Yayınları, Ankara.

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

Yılmaz, M. ve Demirkan, A.E. (2012). "Hastane Yönetim ve Bilgi Sisteminin Kullanılabilirliğinin Değerlendirilmesi", Bilişim Teknolojileri Dergisi, 5(3), 19-28.

Zarei, J. ve Sadoughi, F. (2016). Information Security Risk Management For Computerized Health Information Systems in Hospitals: A Case Study of Iran. Risk Management Healthcare Policy. (9), 75–85.