Üçüncü Sektör Sosyal Ekonomi Dergisi
Third Sector Social Economic Review
61(1) 2026, 735-747
doi: 10.63556/tisej.2026.1617

Araştırma Makalesi

Sağlık Personelinin Bilgi Güvenliği Konusunda Bilinç Düzeyinin Ölçülmesi

Measuring The Knowledge Level of Healthcare Personnel on Information Security

Aykut EKİYOR	**Ferhat BAŞ**
Prof. Dr., Ankara Hacı Bayram Veli Üniversitesi İktisadi İdari Bilimler Fakültesi aykut.ekiyor@hbv.edu.tr https://orcid.org/0000-0002-7718-9329	Dr., Etlik Şehir Hastanesi sidmaa@gmail.com https://orcid.org/0000-0002-1595-16560

Makale Geliş Tarihi	**Makale Kabul Tarihi**
28.07.2025	**25.02.2026**

Öz

Bilgi güvenliği, dünya genelinde öncelikli ve kapsamlı bir konu haline gelmiştir. Hasta güvenliği için kritik öneme sahip olmasına rağmen, yeterince dikkate alınmamaktadır. Bilgi güvenliğinin teminine yönelik mevzuat ve düzenleyici çerçevede kaydedilen gelişmelere rağmen, etkin ve bütüncül bir güvenlik ekosisteminin oluşturulabilmesi; insan faktörü, teknolojik sistemler ve örgütsel süreçlerde çok boyutlu yapısal değişimleri zorunlu kılmaktadır. Sağlık kuruluşları, zengin ve değerli veri kaynakları olmaları nedeniyle siber suçlar açısından cazip hedeflerdir. Sağlık sektöründe görülen siber güvenlik ihlalleri, hasta bilgilerinin çalınması ve sağlık kurumlarını hedef alan fidye yazılımı saldırıları gibi hem veri gizliliğini hem de hizmet sürekliliğini tehdit eden unsurları kapsamaktadır. Bu ihlaller, hasta güvenini zedeleyebilir, sağlık sistemlerinin işleyişini aksatabilir ve insan hayatını tehdit edebilir. Bu araştırmanın temel amacı, sağlık personelinin bilgi güvenliği konusundaki algı ve değerlendirmeleri doğrultusunda, bilgi yönetim sistemlerinin kullanımına ilişkin yapısal ve uygulamaya dönük eksiklikleri ortaya koymaktır. Araştırmada kolayda örnekleme yöntemi kullanılmış ve veriler anket yoluyla toplanmıştır. Sağlık personeli, çalıştıkları bölüme göre idari ve tıbbi birim olarak ayrılmış ve bu birimler arasındaki görüş farklılıkları incelenmiştir. Çalışma sonuçları, katılımcıların %25'inin bilgi güvenliği konusunda yeterli duyarlılık ve özen düzeyine sahip olmadığını göstermekte; buna ek olarak bilgi yönetim sistemi eğitimlerinin kapsam ve süre bakımından yetersiz kaldığı anlaşılmaktadır. Sağlık kurumlarında üretilen ve saklanan verilerin güvenliğinin sağlanması ile olası veri kayıplarının önlenebilmesi, özellikle tıbbi birim çalışanlarının yeterli süre ve içerikte yapılandırılmış eğitim programlarına tabi tutulmasını zorunlu kılmaktadır.

Anahtar Kelimeler: *Bilgi güvenliği, hastane bilgi yönetim sistemi, sağlık personeli*

Abstract

Information security has become a global priority and an increasingly comprehensive field of concern. Despite its critical importance for patient safety, it is not accorded sufficient attention in practice. Although significant progress has been made in establishing legal and regulatory frameworks to ensure information security, the development of an effective and holistic security ecosystem necessitates multidimensional structural transformations encompassing human factors, technological systems, and organizational processes. Healthcare institutions constitute attractive targets for cybercrime due to the richness and value of the data they generate and store. Cybersecurity breaches in the healthcare sector include unauthorized access to patient information and

Önerilen Atıf /Suggested Citation

Ekiyor, A. & Baş, F., 2026, Sağlık Personelinin Bilgi Güvenliği Konusunda Bilinç Düzeyinin Ölçülmesi, *Üçüncü Sektör Sosyal Ekonomi Dergisi*, 61(1), 735-747.

ransomware attacks targeting healthcare organizations, thereby threatening both data confidentiality and service continuity. Such breaches may undermine patient trust, disrupt the functioning of healthcare systems, and ultimately pose risks to human life. The primary aim of this study is to identify structural and practice-based deficiencies in the use of information management systems based on healthcare personnel's perceptions and evaluations regarding information security. A convenience sampling method was employed, and data were collected through a questionnaire. Healthcare personnel were categorized into administrative and clinical units according to their departments, and differences in perceptions between these groups were examined. The findings indicate that 25% of participants do not demonstrate an adequate level of awareness and diligence regarding information security. Furthermore, training programs related to information management systems were found to be insufficient in terms of both duration and content. Ensuring the security of data generated and stored within healthcare institutions, as well as preventing potential data loss, requires particularly clinical staff to undergo structured training programs of adequate duration and scope.

Keywords: *Information security, hospital information management system, healthcare personnel*

1. Giriş

Son yıllarda elektronik sağlık teknolojilerinin dünya genelindeki kullanımı hızlı bir şekilde artış göstermiş ve bu sistemlerin kapsama alanı oldukça genişlemiştir (Koçel, 2010). Bu teknolojiler arasında yer alan elektronik sağlık kayıtları (ESK), bireylerin yaşam kalitesini artırma potansiyeliyle öne çıkmaktadır (Dimiter, 2016). ESK sistemleri sayesinde sağlık uzmanları hasta geçmişine kolayca erişebilmekte, ilaç ve alerji gibi kritik bilgilere ulaşabilmekte ve bu da tıbbi hataların önlenmesine katkı sağlayarak hasta bakımının kalitesini yükseltmektedir (Shenoy ve Appel, 2017). Ancak tüm bu teknolojik ilerlemelere rağmen, bilgi güvenliği sağlık alanında hâlâ çözülmesi gereken önemli bir sorun olarak varlığını sürdürmektedir.

Sağlık çalışanları, bireylerin doğumdan ölüme kadar en mahrem sağlık verilerine erişebilen birincil meslek grubudur. Bu verilerin gizliliği, bütünlüğü ve erişilebilirliği yalnızca hasta hakları açısından değil, aynı zamanda ulusal güvenlik ve bireysel mahremiyet açısından da kritik öneme sahiptir (Sağlık Bakanlığı, 2019). Literatürde, güvenlik teknolojileri ne kadar gelişmiş olursa olsun, insan faktörünün "en zayıf halka" olduğu ve sağlık çalışanlarının bilinçli veya bilinçsiz hatalarının büyük güvenlik ihlallerine yol açabildiği vurgulanmaktadır (Özlük ve Çakır, 2024; Sari, vd., 2023).

Sağlık kurumlarının, bilgi güvenliğini her düzeyde sağlaması beklenmektedir. Bu kapsamda hem fiziksel hem de teknik önlemler alınmalıdır. Fiziksel güvenlik önlemleri arasında iş istasyonlarının korunması, cihazların denetimi ve erişim kontrolleri bulunurken; teknik önlemler kapsamında kullanıcı kimliklerinin özelleştirilmesi, acil durum erişim kuralları, oturumların otomatik kapanması, veri şifreleme ve şifre çözme gibi uygulamalar yer almaktadır (Coventry ve Branley, 2018; Williams ve Woodward, 2015). Buna rağmen siber saldırganlar, sistemlerdeki açıkları istismar ederek kötü amaçlı yazılımlar, kimlik avı girişimleri ya da içeriden gelen tehditler aracılığıyla verilere erişebilmektedir (Coventry ve Branley, 2018; Williams ve Woodward, 2015). Sağlık sektörünün dijital sistemlere hızla geçiş yapmasına rağmen, siber güvenlik yatırımlarının yetersiz kalması ve çalışanların alternatif yollar üretmesi, sektörü tehditlere karşı savunmasız bırakmaktadır (Kruse vd., 2017). Bu durum, doğrudan hasta güvenliğini tehlikeye atmakta ve dolayısıyla bilgi güvenliğinin sağlık hizmetlerinde temel bir unsur olarak ele alınmasını zorunlu kılmaktadır (Coventry ve Branley, 2018).Yılmaz (2024) tarafından yapılan çalışmada kişisel sağlık verileri ihlallerine neden olan en önemli faktörün siber saldırılar olduğu ortaya konulmuştur. Sağlık sektörünün siber saldırılara açık olmasının temel nedenleri arasında hasta verilerinin yüksek ekonomik değere sahip olması, tıbbi cihazların ağ bağlantılı çalışması ve sağlık kuruluşlarında eski bilgi sistemlerinin kullanılmaya devam edilmesi yer almaktadır. Bu durum sağlık kurumlarının bilgi güvenliği altyapılarının güçlendirilmesini zorunlu kılmaktadır (Dönmez & Torun, 2022). Bilgi güvenliği yalnızca teknik altyapı ile açıklanamaz. Özellikle sağlık kurumlarında çalışanların iş yükü ve zaman baskısı, güvenlik protokollerine uyumu olumsuz etkileyebilmektedir (Ifinedo, 2012)

COVID-19 sürecinde bu saldırılar daha da artmış; sağlık hizmetlerine olan talebin yükselmesiyle birlikte sistemler üzerindeki baskı büyümüştür (CISA, 2021). Tıbbi bilgilerin yüksek maddi değer taşıması (örneğin tam bir hasta kaydının 1000 dolar ve üzeri fiyatlara satılabilmesi), bu bilgilerin suç örgütleri için cazibesini artırmaktadır (Kruse vd., 2017). COVID-19 pandemisi döneminde yapılan bir araştırma, sağlık çalışanlarının bilgi güvenliği farkındalığının iş performansını pozitif ve anlamlı bir şekilde

etkilediğini göstermiştir. Ancak, bilgi güvenliği gereksinimlerinin yarattığı baskı (bilgi güvenliği stresi), çalışanlar üzerinde bir yük oluşturabilir. Araştırmaya göre, bilgi güvenliği stresi, farkındalık ile iş performansı arasındaki ilişkide "aracı" bir rol oynamaktadır (Gün ve Çelik, 2022). Çalışanların güvenlik konusundaki farkındalığı arttıkça performansları artmakta, ancak bu süreçte yaşadıkları stres de denklemin bir parçası olmaktadır.

Sağlık kurumları, bilgi güvenliği yönetim sistemleri kurarak, yetkisiz erişimi engelleme, veri bütünlüğü sağlama ve gizliliği koruma hedefiyle çeşitli politikalar geliştirmektedir (Canbek ve Sağıroğlu, 2007; Canberk ve Sağıroğlu, 2006). Türkiye Bilişim Derneği'nin (2005) yayımladığı raporlarda, bilgi güvenliği sistemlerinin sadece kurum imajını korumadığı, aynı zamanda hizmetin sürekliliği, yasal uyum ve çalışan farkındalığı gibi kritik katkılar sağladığı vurgulanmaktadır. Ancak yeterli eğitim programlarının olmaması, açık politikalardan yoksunluk ve yetersiz risk yönetimi, bu süreci sekteye uğratan temel sorunlar arasında yer almaktadır (Farzandipour, vd., 2010; Misic ve Misic, 2007).

Sonuç olarak, sağlık kuruluşlarının yüksek miktarda hassas veri ile çalıştığı günümüzde, yalnızca teknik altyapılar değil; kurumsal kültür, sürekli eğitim ve farkındalık odaklı stratejilerle güçlendirilmiş bütüncül bir bilgi güvenliği yaklaşımı benimsenmelidir (Mehraeen, vd., 2016). Sağlık çalışanlarının bilgi güvenliği konusunda bilinçlendirilmesi ve bu bilincin kurumsal düzeyde desteklenmesi, kurumların öncelikli sorumluluğu olarak ele alınmalıdır.

2. Bilgi Güvenliği

Günümüzde olduğu gibi, dünya genelinde de bilgi teknolojilerinin kullanımı hızla yaygınlaşmakta ve bu teknolojiler kurumlar için vazgeçilmez hâle gelmektedir (Internet World Stats, 2020). Kurum ve kuruluşlar, bilgiye daha hızlı ulaşmak, karar süreçlerini desteklemek ve operasyonel verimliliği artırmak amacıyla sistemli bir şekilde veri toplamaktadır (Baran ve Şener, 2019). Ancak yalnızca verinin toplanması ve işlenmesi yeterli değildir; aynı zamanda bu bilginin güvenli bir şekilde korunması da büyük önem arz etmektedir (Kuusisto, vd., 2003).

Geleneksel yöntemlerde bilgiler çoğunlukla fiziksel dosyalar aracılığıyla saklanmakta ve bu belgeler sadece fiziksel erişimi olan personel tarafından ihlal edilebilmekteydi (Arndt, 2018; Coventry ve Branley, 2018). Oysa günümüzde verilerin dijital ortamlarda tutulması, çok daha geniş bir erişim ağı oluşturmuş ve milyonlarca kişinin verilerini risk altına sokabilecek tehditlerin ortaya çıkmasına neden olmuştur. Bu duruma rağmen, elektronik ortamda tutulan kayıtların bir avantajı olarak; kullanıcıların erişim hareketleri sistem üzerinden izlenebilir hâle gelmiş, böylece veri güvenliği açısından ek bir kontrol mekanizması oluşturulmuştur (Coventry ve Branley, 2018).

Bilgi güvenliği, yalnızca verinin saklanmasıyla sınırlı bir alan olmayıp; bilginin doğruluğunun korunması, yetkisiz erişimlerin engellenmesi ve bilgiye erişim süreçlerinin denetlenmesi gibi pek çok bileşeni içinde barındıran çok boyutlu bir yönetim sürecidir (Canberk ve Sağıroğlu, 2006). Etkili bir bilgi güvenliği yönetimi için teknik altyapının yanı sıra insan faktörü ve eğitim süreçleri de göz ardı edilmemelidir (Vural ve Sağıroğlu, 2007). Nitekim, bir kurumun sahip olduğu bilgi varlığını güvence altına almadan, çalışanların ya da hizmet alan bireylerin güvenliğini sağlamak mümkün değildir (Vural ve Sağıroğlu, 2008).

Günümüzde pek çok kurum, bu doğrultuda bilgi güvenliğine ilişkin politikalar oluşturmakta ve kurumsal düzeyde bilgi güvenliği yönetim sistemlerini hayata geçirmektedir (Canbek ve Sağıroğlu, 2007). Bilgi güvenliğinin etkin biçimde sağlanabilmesi için; kullanıcı erişimlerinin denetlenmesi, sistem içi işlemlerin kayıt altına alınması, kritik verilerin yetkisiz şekilde silinmesinin engellenmesi ve tüm faaliyetlerin izlenebilir olması gibi politikaların açık biçimde belirlenmesi ve uygulanması gereklidir (Canberk ve Sağıroğlu, 2006).

Türkiye Bilişim Derneği (2005), etkili bir bilgi güvenliği yönetiminin sağladığı katkıları şu şekilde özetlemektedir:

Kurumsal itibarı korur ve güven temelli ilişki geliştirir.

Faaliyetlerin kesintisiz devamını güvence altına alır.

Bilgi kaynaklarına erişimi denetim altında tutar.

Verilerin doğruluğunu ve güvenilirliğini garanti eder.

Tüm çalışan ve paydaşların bilgi güvenliği farkındalığını artırır.

Bilgilerin kötüye kullanımını önler.

Gerekli durumlarda, bilgiler üçüncü taraflara güvenli biçimde aktarılabilir.

Yazılım, donanım ve personel kaynaklı aksaklıklara veya kötü niyetli girişimlere karşı koruma sağlar.

2.1 Bilgi Güvenliğinde İnsan Faktörünün Rolü

Bilginin gizliliği, bütünlüğü ve erişilebilirliği, çağdaş bilgi güvenliği anlayışının temel bileşenlerini oluşturmaktadır (Whitman & Mattord, 2018; ISO/IEC, 2013). Bu temel unsurların sürdürülebilir biçimde korunması yalnızca teknolojik önlemlerle sınırlı kalmamalı; aynı zamanda bireylerin potansiyel tehditler, riskler ve kurumsal güvenlik politikaları konusunda farkındalıklarının artırılmasıyla desteklenmelidir (von Solms & von Solms, 2004; Parsons ve ark., 2017). Çalışanların, bilgi güvenliği uygulamalarının neden gerekli olduğu, olası risklerin nasıl azaltılabileceği ve kurumsal prosedürlere nasıl uyulması gerektiği konularında bilinç ve farkındalık sahibi olmaları kritik önem taşımaktadır.

Bilgi güvenliğinde en zayıf halkanın sıklıkla insan unsuru olduğu yönündeki görüş literatürde yaygın kabul görmektedir. Gelişmiş güvenlik sistemleri ve karmaşık şifreleme teknikleri, kullanıcı hataları ve dikkatsiz davranışlar karşısında tek başına yeterli koruma sağlayamaya bilmektedir. Bu nedenle yalnızca teknik altyapıya odaklanan değil, aynı zamanda kullanıcı davranışlarını analiz eden ve yönlendiren bütünleşik güvenlik yaklaşımlarına ihtiyaç duyulmaktadır. Güvenlik duvarları, yama yönetim sistemleri, dosya bütünlüğü izleme araçları ve saldırı tespit sistemleri gibi önlemler, özellikle iş istasyonları ve kritik erişim noktalarının korunmasına yönelik geliştirilmektedir. Ancak kullanıcı faktörü bu sistemlerle entegre biçimde ele alınmadığında, en güçlü teknolojik önlemler dahi kurumsal bilgi güvenliği mimarisinin etkinliğini sınırlayabilmektedir (Arce, 2003).

Literatürde yapılan araştırmalar, kurumsal bilgi güvenliğinde teknik olmayan faktörlerin, en az teknik önlemler kadar belirleyici olduğunu göstermektedir. Dolayısıyla bilgi güvenliğinde insana odaklanan yaklaşımlar, teknik çözümlerle birlikte ele alınmalıdır (Gebrasilase ve Lessa, 2011). Bu noktada, çalışanlara yönelik düzenli ve sistematik eğitimlerin önemi ortaya çıkmaktadır. Kullanıcı eğitimi, bilgi güvenliğinin sürdürülebilirliği için vazgeçilmezdir. Özellikle internet ve e-posta gibi kanallar üzerinden yürütülen etkileşimler, kurumsal ağlara yönelik potansiyel güvenlik açıkları yaratabilmektedir. Dolayısıyla kullanıcı kaynaklı tehditlerin azaltılmasında yalnızca pasif savunma önlemleri yeterli değildir; davranışsal riskleri azaltacak eğitim ve politika desteği de zorunludur (Dodge vd., 2007).

Bilgi güvenliği yönetiminde kurumların yalnızca teknik altyapılar oluşturması yeterli olmamakta; çalışan davranışlarını yönlendiren açık, uygulanabilir politikaların geliştirilmesi ve kurumsallaşmış eğitim programlarının yapılandırılması gerekmektedir. Bu bağlamda Türkiye'de, bireylerin özel hayatının gizliliği başta olmak üzere temel hak ve özgürlüklerini koruma amacıyla 6698 sayılı Kişisel Verilerin Korunması Kanunu yürürlüğe girmiştir. Söz konusu düzenleme, kişisel verilerin işlenmesi sürecinde uyulması gereken ilke ve kuralları belirlemekte; bu süreçte sorumluluğu bulunan gerçek ve tüzel kişilerin yükümlülüklerini kapsamlı biçimde tanımlamaktadır.

2.2 Sağlık Kuruluşlarında Bilgi Güvenliği

Günümüz sağlık kurumları yalnızca hizmet sunmakla yetinmemekte, aynı zamanda kalite ve verimlilik temelinde rekabet etmek durumunda kalmaktadır. Bu bağlamda, sağlık hizmetlerinin sürdürülebilirliğini sağlamak ve geri ödeme sistemlerine raporlama yapabilmek amacıyla hem klinik hem de kişisel veriler sistematik biçimde toplanmakta, işlenmekte ve saklanmaktadır. Bu süreçte dijital bilgi sistemlerinin kullanımı yaygınlaştıkça, sağlık bilgilerinin güvenliğine ilişkin kaygılar da artmaktadır. Özellikle verilerin gizliliğinin korunması ve yalnızca yetkili kişilerin erişimine izin verilmesi gibi konular; veri girişi, depolama, kullanım ve transfer aşamalarında titizlikle ele alınması gereken temel risk alanlarıdır (Deshmukh ve Croasdell, 2009; Cavalli, vd., 2004).

Sağlık kurumlarının sahip olduğu hassas verilerin büyük veri altyapılarına aktarılması, bu bilgilere erişen kişi ve cihaz sayısının artmasına yol açmakta ve dolayısıyla hasta bilgilerinin korunmasını daha karmaşık hale getirmektedir (Rowe, 2016). Hastaneler; bilgi üretimi, işlenmesi, analizi ve saklanmasına

dair yüksek hacimli operasyonlar yürüten veri yoğun yapılardır (Rindfleisch, 1997; Kruse, vd., 2017). Bu çerçevede hastane bilgi sistemleri, hem hasta bakımı hem de yönetsel işlemler açısından birçok avantaj sunar. Günlük görevlerin yürütülmesini kolaylaştıran, farklı bölümler arasında koordinasyonu sağlayan bu sistemler, aynı zamanda laboratuvar ve görüntüleme verilerine hızlı erişimi, finansal kayıtların takibini ve sağlık hizmetinin kalitesini artırmayı da mümkün kılar (Blazona ve Koncar, 2007; Deshmukh ve Croasdell, 2009).

Sağlık kuruluşlarının ürettiği veriler, yalnızca hizmetin etkinliğini artırmakla kalmaz; aynı zamanda iyi bir bilgi yönetimi stratejisi olmadan ciddi etik ve hukuki riskler de barındırır. Son yıllarda artan tıbbi veri ihlalleri, sağlık kuruluşlarının hem itibarını zedelemekte hem de çeşitli yasal yaptırımlara neden olabilmektedir (Civelek, 2009; Mahreen, Batool ve Hussain 2016). Bu nedenle, bilgi güvenliği açıklarının önlenmesi adına daha kapsamlı ve proaktif bir yaklaşım benimsenmelidir.

Sağlık bilgilerinin güvenliği, doğası gereği oldukça hassas ve çok boyutlu bir yapıya sahiptir. Bir yandan kişisel sağlık verilerinin mahremiyeti korunmalı; öte yandan farklı sağlık birimlerinin bu verilere erişimi sağlanmalıdır (Fernando, 2004; Ray ve Newell, 2010). Bu bağlamda yalnızca teknik güvenlik önlemleri yeterli olmayıp, bu önlemlerin kurumsal kültür, politika ve çalışan eğitimi ile entegre edilmesi gerekmektedir (Mehraeen vd., 2016). Ayrıca, sağlık bilgi güvenliği yalnızca kurumsal düzeyde değil, ulusal düzenlemeler ve standartlar çerçevesinde ele alınmalıdır (Misic ve Misic, 2007; Farzandipour vd., 2010).

Başarılı bir sağlık bilgi güvenliği sistemi, yalnızca sunulan hizmetin niteliğine değil; aynı zamanda finansman mekanizmalarına ve ülkenin sağlık sistemine uyum sağlama kapasitesine de bağlıdır (Maşrap vd., 2010). Bu nedenle çalışanların bilgi güvenliği ve kişisel verilerin korunmasına dair yasal çerçeveye ilişkin bilinç düzeyinin artırılması, sistemin etkinliği açısından kritik öneme sahiptir. Eğitimin yetersiz olması, açık prosedürlerin eksikliği veya güvenlik politikalarının kurumsallaşmaması; hem çalışanlar hem de kurum açısından önemli güvenlik risklerine neden olabilmektedir (Farzandipour vd., 2010; Misic ve Misic, 2007).

3. Yöntem

Bu çalışmada sağlık personelinin bilgi güvenliği farkındalığını çok boyutlu olarak değerlendirmek amacıyla güvenlik politikası, örgütsel güvenlik, güvenlik uygulamaları, erişim ve yetkilendirme ile hizmet sunumu boyutlarını içeren bir ölçek kullanılmıştır. Bu boyutlar, bilgi güvenliği farkındalığının yalnızca teknik güvenlik önlemleriyle sınırlı olmadığını; çalışan davranışları, kurumsal güvenlik kültürü ve sağlık hizmeti sunum süreçleriyle bütünleşik bir yapı gösterdiğini ortaya koymaktadır. Ölçeğin çok boyutlu yapısı, bilgi güvenliği farkındalığının teknik, davranışsal ve kurumsal boyutlarını birlikte değerlendirmeye olanak sağlamaktadır. Çalışma, Sağlık Bakanlığı'na bağlı bir eğitim ve araştırma hastanesinde görev yapan sağlık personelinin bilgi güvenliğine ilişkin algı ve tutumlarını değerlendirmek amacıyla yürütülmüştür. Çalışmanın yürütülebilmesi için ilgili hastane yönetiminden gerekli izinler alınmıştır. Araştırmanın hedef kitlesi, hastane bilgi yönetim sistemi (HBYS) kullanan tıbbi ve idari birimlerde çalışan tüm personeldir. HBYS'yi aktif olarak kullanmayan personel araştırma kapsamı dışında tutulmuştur.

Veri toplama süreci 10 Nisan ile 27 Mayıs 2022 tarihleri arasında gerçekleştirilmiştir. Toplamda HBYS'yi düzenli kullandığı belirlenen 784 personele çevrim içi anket formu gönderilmiş ve 102 kişiden geçerli yanıt elde edilmiştir.

Araştırmada kullanılan anket formu yapılandırılmış biçimde hazırlanmış olup, hem çalışanların demografik özelliklerine hem de bilgi güvenliği konusundaki görüşlerine ilişkin sorular içermektedir. Bilgi güvenliği farkındalığını ölçmek amacıyla, Upfold ve Sewry (2005) tarafından geliştirilen ve Aksu (2014) tarafından Türkçeye uyarlanarak geçerlilik ve güvenilirliği test edilmiş bir ölçek kullanılmıştır. Ölçekte, katılımcıların her bir ifadeye 5 dereceli Likert tipi (1 = Kesinlikle katılmıyorum, 5 = Kesinlikle katılıyorum) üzerinden yanıt vermesi istenmiştir. Anket iki ana bölümden oluşmaktadır. İlk bölümde (1–11. sorular), katılımcıların yaş, cinsiyet, eğitim durumu gibi kişisel ve mesleki özelliklerine dair sorular yer almakta; ikinci bölümde ise (12–51. sorular), bilgi güvenliği uygulamaları ve kurumsal politikalarla ilgili algı ve tutumları ölçen ifadeler bulunmaktadır.

Veri toplama sürecinde kolayda örnekleme yöntemi kullanılmıştır. Bu yöntem veri erişimini

kolaylaştırmakla birlikte, örneklemin evreni temsil etme gücünü sınırlayabilmekte ve bulguların genellenebilirliğini etkileyebilmektedir. Katılımcıların belirli kurumdan ve gönüllülük esasına dayalı olarak seçilmiş olması, farklı sağlık kurumlarında görev yapan personelin bilgi güvenliği farkındalık düzeylerinin tam olarak yansıtılamamasına neden olabilir. Bu nedenle gelecekte yapılacak çalışmalarda olasılıklı örnekleme yöntemlerinin kullanılması, bulguların genellenebilirliğini artırabilir.

4. Bulgular

Çalışmada anketi 102 personel yanıtlamıştır. Çalışmaya katılanların yaş ortalaması 42 (24-55 yaş aralığında), %73,5'i kadın, %83,7'si evlidir. %82,7'si hastane bilgi yönetim sistemini kullanma eğitimi aldığını ve eğitim alanların %80,5'i bu eğitimin en fazla bir hafta sürdüğünü ifade etmişlerdir ancak eğitime katılanların yaklaşık yarısı (%48,9) verilen eğitimin yeterli olmadığını düşünmektedir. Katılımcıların %69,8'i, bilgisayar kullanımı konusundaki becerilerini yeterli bulduğunu ifade etmiştir. HBYS kullanımına dair kendi yeterliliklerini 100 puan üzerinden değerlendirmeleri istendiğinde, katılımcıların %41,2'si bu becerilerini 61–80 aralığında puanlamıştır. Bununla birlikte, %80,2 oranındaki katılımcı, hasta verilerine HBYS üzerinden rahatlıkla erişebildiğini bildirmiştir. Bu veriler dışında en sık ulaşılan bilgi türleri arasında kurum prosedürleri ve personel bilgileri yer almıştır.

Katılımcıların %77,2'si, hasta bilgilerinin HBYS sistemi içerisinde güvenli şekilde korunduğuna inandığını belirtmiştir. Ancak sistem üzerinden hasta bilgilerine kimin ya da kimlerin erişim denetimi yaptığına dair soruya verilen yanıtlar heterojen dağılım göstermiş ve 20'nin üzerinde farklı kişi ya da birim belirtilmiştir.

Sisteme erişimde kullanılan kimlik doğrulama yöntemleri arasında en yaygın olanı kullanıcı adı ve şifre kombinasyonudur (%90). Şifre oluşturma alışkanlıklarına bakıldığında, %70,3 oranında kullanıcıların hem harf hem de rakam içeren kombinasyonlar tercih ettiği, buna karşılık %25,3'ünün şifrelerinde kişisel isimleri kullandığı görülmüştür. Ayrıca, %13,2 oranındaki katılımcının kullanıcı adı ve şifresinin aynı olduğunu belirtmesi; ayrıca %5,5'inin "1234" ve %4,4'ünün "8765" gibi kolay tahmin edilebilen ardışık sayı dizilerini tercih etmesidir.

Katılımcıların %82,4'ü hasta kimlik bilgilerine ulaşabildiğini; %82,8'i ise hastalara ait klinik verileri görüntüleyebildiğini ifade etmiştir. Bununla birlikte, %65,9'luk bir kesim bu bilgileri üçüncü kişilerle paylaşmadan önce hasta onamı aldığını bildirmiştir.

Yaklaşık olarak her 10 katılımcıdan 7'si, hasta bilgilerinin korunmasında yazılım ve donanım güncellemelerinin yanı sıra şifrelerin başkalarıyla paylaşılmamasının da önemli bir güvenlik önlemi olduğunu düşünmektedir. Katılımcıların %84,8'i hastanede yazılı bilgi güvenliği politikalarının mevcut olduğunu, %80,8'i bu politikalardan çalışanların haberdar olduğunu ve %73,8'i tüm personele yeterli düzeyde bilgi güvenliği eğitimi verildiğini belirtmiştir.

Bilgi sistemlerine yönelik farkındalık düzeyine bakıldığında; katılımcıların %76,6'sı çalışanların yetkili ve yetkisiz işlemler hakkında bilgi sahibi olduğunu, %81,9'u personelin bilgi güvenliği konusunda yeterli özeni gösterdiğini ve %82,9'u ise hastane yöneticilerinin bu alanda yeterli hassasiyete sahip olduğunu ifade etmiştir. Ayrıca %87,3'lük bir kesim, yöneticilerin bilgi güvenliği uygulamaları konusunda sorumluluk bilinci taşıdığını dile getirmiştir.

Bununla birlikte, %64,6 oranında katılımcı hastanede bir bilgi güvenliği uzmanının görev yaptığını belirtmiş, %48,9'u ise böyle bir uzmanın bulunmadığı durumlarda dış kaynaktan danışmanlık hizmeti alındığını ifade etmiştir.

Katılımcıların %75,9'u, bilgi güvenliği ihlallerinin yönetime bildirilmesi gerektiğini bildiklerini ifade etmiştir. %75,5'i, çalışanların görev alanlarından ayrıldıklarında bilgisayarlarını güvenli şekilde bırakmaları konusunda eğitildiğini belirtmiştir. Kurumsal politikalara ilişkin olarak ise %69,9'u, güvenlik politikalarının ihlali durumunda disiplin cezalarının uygulandığını düşünmektedir.

Ayrıca, %93,5 oranında katılımcı, sistem arızası, çökme ya da hırsızlık gibi olağanüstü durumlarda veri yedeklerinin hizmet sürekliliğini koruyacak şekilde hazırlandığını belirtmiştir. HBYS'nin, herhangi bir sorun ortaya çıkmadan önce planlı biçimde güncellendiği görüşünü paylaşanların oranı %84'tür. %79,6'lık bir kesim, bir güvenlik ihlali durumunda kime başvurulması gerektiğini bildiğini ifade etmiştir. Antivirüs sistemlerinin güncel olduğunu ve sistemin potansiyel virüs saldırılarına karşı yeterli

düzeyde koruma sağladığını düşünenlerin oranı ise %80,7'dir.

Katılımcıların bilgisayar kullanımına ilişkin öz değerlendirmeleri incelendiğinde; idari birim çalışanlarının yalnızca %6,7'si bu alanda kendini yetersiz olarak ifade ederken, bu oran tıbbi birim çalışanlarında %22,4'e yükselmektedir. Bu bulgu, tıbbi birimlerde bilgisayar okuryazarlığının desteklenmesi gerektiğini işaret etmektedir.

Tablo 1: Araştırmaya Katılan Tıbbi ve İdari Birim Çalışanlarının Çalışma Durumları ve HBYS Kullanımları

Sorular		İdari birimler		Tıbbi birimler		p
		n	%	n	%	
Kurumda çalışma süresi	0-5 yıl	7	14,6	14	25,9	0,443
	11-15 yıl	25	52,1	21	38,9	
	15-20 yıl	3	6,3	3	5,6	
	21 yıl ve >	4	8,3	8	14,8	
	6-10 yıl	9	18,8	8	14,8	
HBYS kullanımı deneyim süresi	0-1 yıl	6	12,5	5	9,3	0,903
	11 yıl >	21	43,8	23	42,6	
	2-5 yıl	8	16,7	7	13,0	
	6-10 yıl	13	27,1	19	35,2	
HBYS kullanmak için eğitim aldı mı?	Evet	38	79,2	46	85,2	0,426
	Hayır	10	20,8	8	14,8	
HBYS kullanmak için alınan eğitim süresi	0-1 Hafta	26	54,2	47	87,0	0,001*
	2 Haftadan fazla, 1 aydan az	15	31,3	2	3,7	
HBYS eğitimi yeterliliği	Yeterli	28	58,3	20	37,00	
	Yetersiz	9	18,8	10	18,5	0,117
	Kararsızım	8	16,7	18	33,3	
	Yanıt yok	3	6,3	6	11,1	

*p<0,05

Tablo 1'e göre tıbbi ve idari birimlerde görev yapan katılımcılar arasında; kurumdaki hizmet süresi, HBYS kullanım deneyimi ve bu sistemi kullanmak üzere eğitim alıp almama durumları açısından istatistiksel olarak anlamlı bir fark saptanmamıştır (p>0,05). Buna karşılık, HBYS eğitimlerinin süresi bakımından iki grup arasında farklılık gözlemlenmiş ve bu farklılık istatistiksel olarak anlamlı bulunmuştur (p=0,001).

Çalışmaya katılan sağlık personelinin değerlendirmelerine göre, idari birimlerde görev yapan çalışanlar, bilgi güvenliği alanında yeterli ve uygun eğitim verilmesi gerektiği yönündeki görüşü, tıbbi birim çalışanlarına kıyasla istatistiksel olarak anlamlı düzeyde daha fazla desteklemiştir (p=0,049). Buna karşılık, güvenlik politikasıyla ilişkili diğer maddelere yönelik verilen yanıtlar karşılaştırıldığında, iki grup arasında anlamlı bir fark olmadığı belirlenmiştir (p>0,05).

Araştırma bulgularına göre, örgütsel güvenlik politikalarına ilişkin değerlendirmelerde, tıbbi ve idari birim çalışanları arasında istatistiksel olarak anlamlı bir fark saptanmamıştır (p>0,05). Benzer şekilde, örgütsel güvenlik boyutuna dair diğer alt ifadelerde de iki grup arasında anlamlı bir farklılık olmadığı gözlemlenmiştir (p>0,05). Güvenlik uygulamaları boyutu açısından yapılan analizlerde de, tıbbi ve idari personelin değerlendirmeleri arasında önemli bir istatistiksel fark bulunmamıştır (p>0,05). Aynı şekilde, erişim ve yetkilendirme uygulamalarına ilişkin görüşler karşılaştırıldığında da, her iki grubun yanıtları arasında anlamlı bir ayrım olmadığı belirlenmiştir (p>0,05).

Ancak hizmet sunumu boyutunda, belirli iki ifade grubuna dair anlamlı farklar tespit edilmiştir. "Yoğun iş yükünün bilgi güvenliği konusuna yeterli önemin verilmesini engellemediği" görüşü, tıbbi birim çalışanları tarafından idari personele kıyasla anlamlı derecede daha yüksek oranda benimsenmiştir (p=0,015). Benzer biçimde, "iş akışındaki değişimlerin bilgi güvenliği hassasiyetini azaltmadığı" yönündeki ifadeye verilen yanıtlar da tıbbi birimlerde anlamlı düzeyde daha yüksek puanlarla değerlendirilmiştir (p=0,004). Bununla birlikte, "bilgi güvenliği süreçlerinin hizmet kalitesi üzerinde olumsuz bir etkisi olmadığı" ve "bilgi güvenliğinin günlük iş akışı içinde öncelikli bir konu olduğu"

ifadelerinde, tıbbi ve idari birim çalışanları arasında istatistiksel olarak anlamlı bir fark görülmemiştir ($p>0,05$).

5. Sonuç ve Öneriler

Bu araştırmada elde edilen bulgular, sağlık çalışanlarının yaklaşık %17,3'ünün görev ve sorumlulukların net tanımlanmadığını düşündüğünü ortaya koymuştur. Ayrıca, HBYS kullanan personelin %20'si bu alanda herhangi bir eğitim almadığını belirtmiş, eğitim alanların ise yaklaşık yarısı aldıkları eğitimi yetersiz bulmuştur. Her ne kadar yalnızca birkaç kişi bu eksikliği açıkça belirtmiş olsa da, genel olarak eğitimlerin kapsam ve süresi yönünden güçlendirilmesi gerektiği anlaşılmaktadır.

Çalışmanın genel bulguları, araştırmanın yapıldığı hastanede yazılım ve donanım altyapısının bilgi güvenliği açısından yeterli olduğunu göstermektedir. Ancak personelin dörtte biri, bilgi güvenliğine yeterince önem verilmediği ve gerekli hassasiyetin gösterilmediği kanaatindedir. Bulgular, çalışanların bilgi güvenliği süreçlerine yönelik farkındalıklarının artırılması gerektiğini göstermektedir.

Tıbbi personelin klinik iş yükü ve hasta bakımına öncelik verme zorunluluğu, bilgi güvenliği prosedürlerine uyumu sınırlayabilmektedir. Tıbbi birimlerde görev yapan katılımcılar, yoğun iş temposu ve iş süreçlerindeki değişimlere rağmen bilgi güvenliğine yönelik duyarlılıklarını koruduklarını ifade etmişlerdir. Öte yandan, idari birim çalışanlarının daha uzun süreli eğitim almış olmalarına rağmen, bu eğitimlerin yeterliliği konusunda daha eleştirel oldukları gözlemlenmiştir.

Bu farklılıklar, mesleki rol ve sorumlulukların bilgi güvenliği davranışları üzerinde belirleyici olduğunu göstermektedir. Sağlık kurumlarında bilgi güvenliği farkındalığının artırılabilmesi için eğitim programlarının meslek gruplarının iş süreçleri ve risk profilleri dikkate alınarak yapılandırılması önem taşımaktadır. Özellikle klinik personel için hasta bakım süreçleriyle entegre edilebilen pratik ve uygulama temelli eğitim yaklaşımlarının geliştirilmesi, güvenlik farkındalığının artırılmasına katkı sağlayabilir.

Bu çalışmada elde edilen bulgular, sağlık çalışanlarının bilgi güvenliği farkındalık düzeylerinin mesleki rol, kurumsal yapı ve bilgi sistemleri kullanım yoğunluğu gibi faktörlerden etkilendiğini göstermektedir. Elde edilen sonuçlar, bilgi güvenliği farkındalığının çalışan davranışları ve örgütsel güvenlik kültürü ile ilişkili olduğunu ortaya koyan önceki çalışmalarla paralellik göstermektedir (Parsons ve ark., 2017; Ifinedo, 2012). Özellikle güvenlik uygulamaları ve erişim kontrolü boyutlarında gözlenen farklılıklar, literatürde sağlık çalışanlarının yoğun iş yükü ve zaman baskısı nedeniyle güvenlik prosedürlerini ihmal edebildiğini gösteren bulgularla örtüşmektedir (Stanton ve ark., 2005). Bununla birlikte bazı alt boyutlarda elde edilen farkların önceki çalışmalardan daha belirgin olması, sağlık kurumlarında dijitalleşme düzeyinin artması, elektronik sağlık kayıtlarının yaygınlaşması ve veri güvenliği risklerinin çeşitlenmesi ile açıklanabilir.

Öte yandan çalışmada belirlenen bulgular, bilgi güvenliği farkındalığının yalnızca bireysel bilgi düzeyi ile açıklanamayacağını, kurumsal güvenlik politikaları ve yönetsel destek mekanizmalarının da belirleyici olduğunu ortaya koymaktadır. Bu durum, güçlü örgütsel güvenlik kültürüne sahip kurumlarda çalışanların güvenlik kurallarına uyumunun arttığını ortaya koyan çalışmalarla uyumludur (Von Solms & Von Solms, 2004). Ancak bazı bulgular, eğitim programlarının yaygın olmasına rağmen çalışan davranışlarının istenilen düzeye ulaşamadığını gösteren literatürle de örtüşmektedir. Bu durum, bilgi güvenliği eğitimlerinin teorik içerikten ziyade uygulama temelli ve davranış değişimini hedefleyen yaklaşımlarla yapılandırılması gerektiğini düşündürmektedir.

Bu çalışmada şifre kullanımı, kullanıcı davranışları ve eğitim yetersizliği alanlarında elde edilen bulgular, bilgi güvenliği literatüründe insan faktörünün kritik rolünü vurgulayan çalışmalarla paralellik göstermektedir. Bilgi güvenliği ihlallerinin önemli bir bölümünün teknik zafiyetlerden ziyade kullanıcı hatalarından kaynaklandığı bilinmektedir. Zayıf parola kullanımı, parolaların paylaşılması veya düzenli güncellenmemesi gibi davranışlar, sağlık kurumlarında kişisel sağlık verilerinin gizliliğini doğrudan tehdit etmektedir. Von Solms ve Von Solms (2004), bilgi güvenliğinde teknik altyapının tek başına yeterli olmadığını, kullanıcı davranışlarının güvenlik yönetiminin temel bileşeni olduğunu belirtmektedir. Benzer şekilde, Parsons ve ark. (2017) kullanıcı farkındalığı ve güvenlik eğitimlerinin, veri ihlallerini azaltmada kritik öneme sahip olduğunu ortaya koymuştur.

Etik açıdan değerlendirildiğinde, sağlık çalışanlarının hasta verilerinin gizliliğini koruma sorumluluğu mesleki etik ilkeler ve hasta hakları kapsamında ele alınmaktadır. Kişisel sağlık verilerinin ihlali, yalnızca bireysel mahremiyetin zedelenmesine değil, aynı zamanda sağlık sistemine duyulan güvenin azalmasına da yol açabilmektedir. Hukuki açıdan ise Türkiye'de 6698 sayılı Kişisel Verilerin Korunması Kanunu ve ilgili sağlık mevzuatı, sağlık verilerinin korunmasına yönelik ciddi sorumluluklar yüklemektedir. Bu kapsamda çalışanların bilgi güvenliği farkındalık düzeylerinin yetersiz olması, kurumlar açısından idari yaptırımlar ve hukuki sorumluluk risklerini artırmaktadır.

Yönetsel açıdan değerlendirildiğinde, bilgi güvenliğinin sürdürülebilir şekilde sağlanabilmesi için yalnızca teknik önlemlerin değil, kurumsal güvenlik kültürünün geliştirilmesine yönelik eğitim programlarının, düzenli denetimlerin ve davranış odaklı güvenlik politikalarının uygulanması gerekmektedir. Kurumlarda sürekli eğitim programlarının uygulanması, güçlü parola politikalarının oluşturulması ve kullanıcı davranışlarının izlenmesine yönelik sistemlerin geliştirilmesi, veri güvenliği risklerinin azaltılmasına önemli katkı sağlayacaktır.

Bu çalışma, sağlık personelinin bilgi güvenliği farkındalığını çok boyutlu olarak değerlendirmiş ve özellikle eğitim süreçleri, kullanıcı davranışları ve kurumsal uygulamalara ilişkin önemli bulgular ortaya koymuştur. Araştırma sonuçlarına göre sağlık çalışanlarının önemli bir kısmı bilgi güvenliğine ilişkin temel farkındalığa sahip olmakla birlikte, eğitim içeriklerinin yetersizliği, şifre güvenliği uygulamalarındaki eksiklikler ve erişim denetim mekanizmalarına ilişkin belirsizlikler bilgi güvenliği açısından potansiyel risk alanları olarak belirlenmiştir. Ayrıca tıbbi birim çalışanlarının bilgisayar kullanım yeterliliklerinin görece düşük olması, bilgi güvenliği uygulamalarının etkinliğini sınırlandırabilecek önemli bir bulgudur.

Araştırma bulguları doğrultusunda yöneticilere, uygulayıcılara ve politika yapıcılara yönelik aşağıdaki öneriler geliştirilebilir:

Yöneticilere Yönelik Öneriler

- Sağlık kurumlarında bilgi güvenliği eğitimleri yalnızca oryantasyon sürecinde değil, düzenli aralıklarla ve uygulamaya dayalı şekilde planlanmalıdır.
- HBYS kullanım eğitimleri personelin görev alanına ve mesleki rolüne göre modüler biçimde tasarlanmalıdır.
- Kurumlarda bilgi güvenliği sorumluluğunu üstlenen birim veya uzman personelin istihdam edilmesi sağlanmalıdır.
- Bilgi güvenliği ihlallerine yönelik raporlama mekanizmaları açık, erişilebilir ve cezalandırma odaklı değil öğrenme odaklı olacak şekilde yapılandırılmalıdır.
- Şifre güvenliği, veri erişim yetkilendirmesi ve kullanıcı davranışlarının düzenli olarak denetlenmesini sağlayan iç kontrol mekanizmaları oluşturulmalıdır.

Uygulayıcılara (Sağlık Personeline) Yönelik Öneriler

- Kullanıcı adı ve şifre güvenliği konusunda farkındalık artırılmalı; kişisel bilgi kullanımından kaçınılmalı ve güçlü parola oluşturma alışkanlığı kazandırılmalıdır.
- Hasta verilerinin paylaşımında etik ve hukuki sorumluluklar konusunda çalışanlara uygulamalı eğitimler verilmelidir.
- Bilgi güvenliği ihlali durumunda bildirim kültürü teşvik edilmeli ve çalışanların bu süreçte desteklenmesi sağlanmalıdır.
- Tıbbi birim çalışanlarının dijital okuryazarlık ve bilgi sistemi kullanım becerilerini artırmaya yönelik eğitim programları geliştirilmelidir.

Politika Yapıcılara Yönelik Öneriler

- Sağlık bilgi sistemlerinde kullanıcı yetkilendirme ve erişim denetim süreçlerinin standardizasyonu sağlanmalıdır.

- Sağlık kurumlarında bilgi güvenliği uzmanı bulundurulmasına yönelik mevzuat düzenlemeleri geliştirilmelidir.
- Bilgi güvenliği performans göstergeleri sağlık kurumlarının kalite değerlendirme süreçlerine entegre edilmelidir.
- Kişisel sağlık verilerinin korunmasına yönelik mevzuatın uygulanabilirliğini artıracak rehber dokümanlar ve denetim mekanizmaları güçlendirilmelidir.

Sonuç olarak, sağlık kurumlarında bilgi güvenliğinin sağlanması yalnızca teknik altyapı yatırımlarıyla mümkün değildir. Kurumsal kültür, çalışan davranışları, eğitim süreçleri ve politika düzeyindeki düzenlemelerin bütüncül biçimde ele alınması gerekmektedir. Bu kapsamda geliştirilecek sürdürülebilir eğitim ve denetim mekanizmaları, sağlık hizmetlerinde veri güvenliğinin artırılmasına ve hasta güvenliğinin korunmasına önemli katkı sağlayacaktır.

Kaynakça

Aksu, H. (2014). Kamu çalışanlarının bilgi güvenliğine yönelik algı düzeylerinin belirlenmesi: Milli Savunma Bakanlığı örneği [Yüksek lisans tezi, Gazi Üniversitesi]. YÖK Ulusal Tez Merkezi.

Arce, I. (2003). What is cybercrime? IEEE Security & Privacy, 1(2), 76–77.

Arndt, T. (2018). Electronic health records: Reliable, private, and secure? Health Information Science and Systems, 6(1), 1–7.

Baran, B., & Şener, H. (2019). Bilgi güvenliği farkındalığı: Türkiye'de kamu çalışanlarına yönelik bir durum analizi. Bilgi Güvenliği Dergisi, 11(2), 45–59.

Barrentt, J. (2003). Information security: Managing the legal risks. Computers & Security, 22(6), 476–480.

Blazona, B., & Koncar, M. (2007). HL7 and DICOM based integration of radiology information systems and PACS. Computer Methods and Programs in Biomedicine, 87(2), 131–140.

CISA. (2021). Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov

Canbek, G., & Sağıroğlu, Ş. (2007). Bilgi güvenliği ve yönetimi. Akademik Bilişim Konferansı Bildirileri, 1, 101–107.

Canberk, G., & Sağıroğlu, Ş. (2006). Bilgi güvenliği yönetimi. Kamu-BİB'06 Türkiye Bilişim Derneği Kamu Bilişim Platformu, 1–6.

Cavalli, A., Rognoni, G., & Spina, G. (2004). Security issues in health care information systems. In Proceedings of the IEEE International Workshop on Factory Communication Systems (pp. 211–214).

Civelek, M. E. (2009). Bilgi yönetimi ve güvenliği. İstanbul Üniversitesi Yayınları.

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas, 113*, 48–52. doi:10.1016/j.maturitas.2018.04.008

Deshmukh, A., & Croasdell, D. (2009). Health information systems: Architectures and security. Journal of Health Information Management, 23(2), 30–38.

Dimiter, V. (2016). The impact of electronic health records on healthcare quality: A literature review. Health Information Science and Systems, 4(1), 10–19.

Dodge, R., Carver, C., & Ferguson, A. J. (2007). Phishing for user security awareness. Computers & Security, 26(1), 73–80.

Farzandipour, M., Sadoughi, F., Ahmadi, M., & Karimi, I. (2010). Effective factors on implementation of security policies in Iranian hospitals. Iranian Red Crescent Medical Journal, 12(6), 660–666.

Fernando, J. I. (2004). Confidentiality and privacy in healthcare information systems. Health Management Technology, 25(4), 36–37.

Gebrasilase, D., & Lessa, L. (2011). Information security and human factors. International Journal of Advanced Computer Science and Applications, 2(6), 60–65.

IBM Security Services. (2015). 2015 Cyber Security Intelligence Index. IBM Corporation.

International Organization for Standardization. (2013). ISO/IEC 27001:2013 information technology—

Security techniques—Information security management systems—Requirements. ISO.

Internet World Stats. (2020). Usage and population statistics. https://www.internetworldstats.com/stats.htm

Koçel, T. (2010). İşletme yöneticiliği (12. baskı). Beta Yayınları.

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*, *25*(1), 1–10. doi:10.3233/THC-161263

Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. *Journal of Medical Systems, 41*(8), 127. doi:10.1007/s10916-017-0778-4

Kuusisto, R., Hintsa, J., & Pihlajamaa, M. (2003). Information security in a supply chain. In IEEE International Conference on Systems, Man and Cybernetics (Vol. 6, pp. 5487–5492).

Mahreen, M., Batool, M., & Hussain, S. (2016). Security issues and solutions in e-health. International Journal of Computer Applications, 146(1), 1–6.

Maşrap, E., Yıldız, M., & Coşkun, E. (2010). Sağlık bilgi sistemleri güvenliği. Akademik Bilişim Konferansı, Muğla, Türkiye.

Mehraeen, E., Ayatollahi, H., & Ahmadi, M. (2016). Health information security in hospitals: The application of security safeguards. Acta Informatica Medica, 24(1), 47–50.

Misic, M. M., & Misic, G. G. (2007). Security of e-health systems. In E-health systems and wireless communications: Current and future challenges (pp. 56–73). IGI Global.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165–176. https://doi.org/10.1016/j.cose.2013.12.003

Ponemon Institute. (2016). Sixth annual benchmark study on privacy & security of healthcare data. https://www.ponemon.org

Ray, P., & Newell, D. (2010). Confidentiality and privacy issues in healthcare information technology. In Healthcare Information Technology (pp. 30–45). Springer.

Rindfleisch, T. C. (1997). Privacy, information technology, and health care. Communications of the ACM, 40(8), 92–100. https://doi.org/10.1145/257874.257896.

Rowe, N. (2016). The disappearing non-academic scientist. Higher Education Quarterly, 70(3), 264–285.

Sağıroğlu, Ş. (2001). Bilgi güvenliği ve yönetimi. Bilgi Güvenliği Sempozyumu, TBD Yayınları.

Shenoy, A., & Appel, J. M. (2017). Safeguarding confidentiality in electronic health records. Cambridge Quarterly of Healthcare Ethics, 26(2), 337–341.

Upfold, C., & Sewry, D. (2005). Information security management: A South African perspective. In SAICSIT Research Symposium (pp. 1–12).

von Solms, B., & von Solms, R. (2004). The 10 deadly sins of information security management. Computers & Security, 23(5), 371–376. https://doi.org/10.1016/j.cose.2004.05.005

Vural, Y., & Sağıroğlu, Ş. (2007). Bilgi güvenliği yönetim sistemi. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 22(3), 557–566.

Vural, Y., & Sağıroğlu, Ş. (2008). Kurumsal bilgi güvenliği yönetimi. Akademik Bilişim Bildirileri, 2(1), 89–95.

Whitman, M. E., & Mattord, H. J. (2003). Principles of information security. Cengage Learning.

Williams, P. A. H., & Woodward, A. J. (2015). Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem. Medical Devices: Evidence and Research, 8, 305–316.

Research Article

Sağlık Personelinin Bilgi Güvenliği Konusunda Bilinç Düzeyinin Ölçülmesi

Measuring The Knowledge Level of Healthcare Personnel on Information Security

Aykut EKİYOR	Ferhat BAŞ
Prof. Dr., Ankara Hacı Bayram Veli Üniversitesi İktisadi İdari Bilimler Fakültesi aykut.ekiyor@hbv.edu.tr https://orcid.org/0000-0002-7718-9329	Dr., Etlik Şehir Hastanesi sidmaa@gmail.com https://orcid.org/0000-0002-1595-16560

Extended Summary

Information security has emerged as a critical issue worldwide, particularly in the healthcare sector, where sensitive personal and clinical data are collected, stored, and processed. While hospital information systems (HIS) offer numerous advantages, such as accessibility and efficiency, they also pose significant privacy and security risks. Healthcare organizations are attractive targets for cybercriminals due to the high value of medical data. Despite existing legal frameworks and technological safeguards, the human factor remains a major vulnerability. Therefore, understanding healthcare personnel's awareness and attitudes toward information security is essential to enhancing data protection in hospitals.

This study aims to evaluate the perspectives of healthcare personnel regarding information security and to identify deficiencies in the use of hospital information management systems (HIMS). It also examines differences in awareness and practices between administrative and medical staff.

The research was conducted at a training and research hospital affiliated with the Ministry of Health in Turkey. After obtaining institutional approval, a structured questionnaire was distributed to 784 employees who regularly use the HIMS; 102 completed responses were collected. The questionnaire consisted of two parts: the first gathered demographic data, and the second) measured information security awareness using the scale developed by Upfold & Sewry (2005), adapted to Turkish by Aksu (2014). Responses were scored on a 5-point Likert scale. The data were analyzed to compare responses between administrative and medical personnel.

The average age of participants was 42 years, with 73.5% being women and 83.7% married. While 82.7% reported having received HIMS training, nearly half (48.9%) found the training inadequate. Approximately 25% of respondents stated that information security was not given sufficient importance or care within the hospital. Most participants believed that patient data were protected, but more than 20 different answers were given regarding who oversees access control. Notably, 13.2% of employees used the same username and password, and about 10% used easily guessed passwords like "1234" or "8765." Both administrative and medical staff expressed that workload did not prevent them from prioritizing information security. However, administrative staff were more likely to report a need for proper and adequate training compared to medical staff (p=0.049).

The findings highlight that while healthcare employees have some awareness of information security, there are gaps in training and implementation. Many employees use weak passwords, share credentials, and are unaware of access control responsibilities. To improve information security in healthcare settings, it is crucial to provide regular and comprehensive training tailored to both administrative and

medical staff. Investments in technological, organizational, and behavioral safeguards are necessary to mitigate risks posed by cyberattacks and internal threats. Ultimately, information security must be integrated into the daily routines of healthcare personnel to ensure patient safety and institutional integrity.