J 5N1 Quality, 2023, 1(1): 19-28

Araştırma Makalesi/ Research Article

Bilgi güvenliği kapsamında yer alan rol gruplarının değerlendirilmesi*

Evalution of role groups in the scope of ınformation security

Zeynep Yıldız[1], Hediye Yurttaş[2], Bülent Ozan[3]

[1]Gölcük Necati Çelik Devlet Hastanesi, zynp.lptkn@hotmail.com, 0009-0007-2198-3236

[2]Gölcük Necati Çelik Devlet Hastanesi, hediyeyurttas@hotmail.com, 0009-0000-7327-3163

[3]Gölcük Necati Çelik Devlet Hastanesi, bulentozan@saglik.gov.tr, 0009-0005-9512-6021

*Bu çalışma, 14-17 Aralık 2022 tarihlerinde VIII. Uluslararası Sağlıkta Performans ve Kalite Kongresinde sözel bildiri olarak sunulmuştur.

ÖZ

Bu çalışmada; kurumumuzda tüm çalışanların bilgi güvenliği çalışmaları doğrultusunda; rol gruplarının belirlenmesi, sistem erişim yetkilerinin verilmesi ile yetki değişikliklerinin yönetiminde yapılan faaliyetlerin Sağlıkta Kalite Standartları Bilgi Yönetim Sistemi ve Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu doğrultusunda yapılmasının önemini vurgulamak amaçlanarak kurumun bilgi güvenliği kapsamında yapılan tüm çalışmaların değerlendirilmesi planlanmıştır. Tanımlayıcı nitelikte bir araştırmadır. Araştırmada; Gölcük Necati Çelik Devlet Hastanesi'nde Sağlıkta Kalite Standartları Bilgi Yönetim Sistemi doğrultusunda kurumda çalışanların rolleri ve verilen yetkilerle, yaptığı iş ve işlemlerin bilgi güvenliğine uygunluğu ile rol grupları ve yetki değişikliklerinin yönetimi incelenmiş, vaka çalışması yapılmıştır. Aktif 860 çalışanın görev yaptığı hastanemizde toplamda 37 rol grubu belirlenmiş olup bu rol gruplarına hizmet aldığımız Sağlık Bilgi Yönetim Sistemi üzerinde bulunan 30 modül üzerinden yetki dağılımı yapılmıştır. arşiv sorumlusuna modül üzerinde 6 işlem yetkisi verilirken arşiv birim çalışanı 3 işlem ile sınırlandırılmıştır. Kullanıcılara yetki verilirken yetki düzeylerinin eklendiği rol grubundaki çalışanlarla aynı olmasına dikkat edilir. Kurumlarda bilgi güvenliğinin sağlanmanın yolu; yöneticilerin tam desteğini alan bir süreç başlatarak kurumsal bilgi güvenliği politikalarını oluşturmak, politikalar doğrultusunda ilgili prosedür süreçlerini dokümante etmek ve yasal mevzuatlar doğrultusunda izleme, iyileştirme, güncelleme ve denetleme çalışmalarını aynı kararlılıkla devam ettirmekten geçmektedir. Tüm kurum çalışanlarına bilgi güvenliği yönetiminin bilgi yönetim sistemi birimi kapsamında teknik bir iş olmadığı, kurumun tüm birimlerinin ve çalışanlarının sorumluluk yüklenmesi gerektiği etkili bir şekilde ve yerinde anlatılmalıdır.

Anahtar Kelimeler:

Bilgi Güvenliği, Bilgi Yönetim Sistemi, Rol Grupları, Yetki

ABSTRACT

In this study; in line with the information security activities of all employees in our institution; It is planned to evaluate all the activities carried out within the scope of information security of the institution with the aim of emphasizing the importance of determining the role groups, granting system access authorizations and the activities carried out in the management of authorization changes in line with the Health Quality Standards Information Management System and the Ministry of Health Information Security Policies Guide. It is descriptive research. In the research; In Gölcük Necati Çelik State Hospital, in line with the Health Quality Standards Information Management System in line with the Health Quality Standards Information Management System, the roles of the employees in the institution and the authorities given, the compliance of the work and transactions with information security and the management of role groups and authorization changes were examined and a case study was conducted. In our hospital, where 860 active employees work, a total of 37 role groups have been determined and these role groups have been authorized over 30 modules on the Health Information Management System from which we receive service. While the archive officer is authorized for 6 transactions on the module, the archive unit employee is limited to 3 transactions. When authorizing users, it is ensured that the authorization levels are the same as the employees in the role group to which they are added. The way to ensure information security in organizations is to establish corporate information security policies by initiating a process with the full support of managers, to document the relevant procedural processes in line with the policies, and to continue monitoring, improvement, updating and auditing activities in line with legal regulations with the same determination. It should be effectively and appropriately explained to all employees of the organization that information security management is not a technical task within the scope of the information management system unit, and that all units and employees of the organization should assume responsibility.

Key Words:

Information Security, Information Management System, Role Groups, Authority

Corresponding Author/Sorumlu Yazar

Gölcük Necati Çelik Devlet Hastanesi, zynp.lptkn@hotmail.com, 0009-0007-2198-3236

DOI:

10.5281/zenodo.7761218

Received Date/Gönderme Tarihi:

09.03.2023

Accepted Date/Kabul Tarihi:

21.03.2023

Published Online/Yayımlanma Tarihi

23.03.2023

Reference | Atıf : Yıldız, Z., Yurttaş, H. & Ozan, B. (2023). Bilgi güvenliği kapsamında yer alan rol gruplarının değerlendirilmesi. Journal of 5N1Quality, 1(1), 19-28.

1.GİRİŞ

Bilgi, sözlü veya yazılı kaynaklar gibi hayatın her yerinde, her anında var olan ve bireyin korunması istediği en değerli varlığıdır. Bireyin ve kurumun en değerli varlığı olan bilginin bozulması, zarara uğraması, yok olması ve yetkisiz kişilerin eline geçmesinin engellenmesinin gerekliliği ile bilgi güvenliği kavramı ortaya çıkmıştır. Hizmette kalite ve verimliliği ön planda tutan kurumlarda bilgiye erişilebilirliğin kolaylaşması amacıyla bilgi güvenliği sistemlerinin kullanımı gittikçe yaygınlaşmaktadır. Günümüzde tüm kurumlar faaliyet süreçlerinin tamamında bilgi kaynaklarını ve teknolojik iletişim sistemlerini kullanmaktadırlar. Kurumlarda elektronik sistemlerin kullanılması, kâğıt üzerinden yapılan işlemlere göre erişim yetkilerinin ve olayların çok daha kolay yönetilmesini sağlamaktadır (Bartlett, 2008:66). Elektronik sistemlere geçilmesiyle birlikte kullanıcılar tam ve güvenilir bilgiye zamanında, hızlı ve kesintisiz şekilde erişebilmeyi talep etmektedirler (Şahin, 2008:158).

Bilgi güvenliği uygulamaları teknolojik uygulamaların girdiği her sektörde geniş bir şekilde kullanılmaya başlanmıştır. Özellikle insanların sağlık sorunları ile ilgili mahrem bilgilerin yer aldığı hastane bilgi sistemleri, bilgi güvenliği konularının öncelikli alanlarından biridir (Varol, 2016:156). Sağlık sistemi; birey ve toplumun sağlık düzeyini koruyup geliştirmeyi amaçlayan alt sistemler, kurumlar ve programlar bütünüdür (Marşap, 2010:32). Sağlık sisteminde yer alan elektronik sağlık kayıtları, hastalara dair geniş ölçekli bilgileri içerisinde bulunduran bir sistem olmakla birlikte taşıdığı öneme paralel olarak bu sistemin kullanımında nitelikli çalışanların varlığına ihtiyaç duyulmaktadır. İster sağlık personeli olsun isterse sistemin başındaki çalışanlar olsun, sağlık kuruluşları açısından önemli olan sürecin yetkin bireylere bırakılması ve bu bireylerin konuya dair hukuki ve etik odaklı yaklaşımlarının sorgulanması gerekmektedir (Öğütçü vd., 2011).

Teknolojinin geliştiği ve yoğun olarak kullanıldığı günümüzde, sağlık kurumlarında, hastaların sağlık durumlarına ait bilgilerin mahremiyet sınırları çerçevesinde gizliliği, ihtiyaç duyulduğu anda bir bütünlük çerçevesinde kullanılabilirliği her zaman için önemli bir ihtiyaç olmuş ve bilgi güvenliği yönetim sistemleri içerisinde değerlendirilmiştir (Eriş, 2017). Sağlık kurumları son teknolojiden yararlanarak güvenlik önlemlerini alsalar da insan kaynaklı bilgi güvenliği açıklarının hiçbir zaman önüne geçemezler. Çünkü sağlık kurumlarının bilgi güvenliği konusunun en zayıf halkası insan faktörüdür. En ufak ciddiyetsizlik ve sorumsuzluk kurumlar için maddi ve manevi telâfisi mümkün olmayan sorunlara yol açar. Bilgi güvenliği farkındalığı oluşturmaktaki amaç; kişilerin bilgi eksikliğinden kaynaklı hata ve risklerini en aza indirmek ve çalışanların bu tehditlerden haberdar olmasını sağlamaktır. (Şahinarslan vd., 2009).

Sağlık işletmelerinde güvenli bilgi teknolojileri, yeni gelişimler ışığında günümüzde çok daha fazla önem kazanmış olup etkinlikle kullanılmaktadır. Bilgiye erişim sürecinde devreye giren bilgi güvenliği yönetim sistemlerinin temel amacı, bilgi kaynaklarında gizlilik, bütünlük ve yetki bazında erişimi sağlamaktır. Bilgi güvenliği yönetimi, kurumsal bilgi kaynaklarının farkına varma, bu kaynaklara her türlü denetimsiz erişimi engelleme, risk analizleri yaparak bilginin gizliliğinin ve bütünlüğünün korunması için gerekli idari ve teknik önlemleri alma ve tüm iş süreçlerini bilgi güvenliği politikaları doğrultusunda düzenleyerek yönetme işlevidir (İleri, 2016). Bilgi Güvenliği Yönetim sistemleri, kurumu sürekli iyileştirmek adına etkin, sürekli ve 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 bilgi güvenliği yönetim sistemleri geliştirilmelidir (Yılmaz, 2014).

Sağlıkta Kalite Standartları'yla hastalara ve tüm sağlık çalışanlarına ait bilgilerin doğru olarak toplanıp kaydedilmesi, güvenliği sağlanmış ortamlarda (elektronik/arşiv) saklanması ve hastanenin bilgi güvenliğini sağlamaya yönelik düzenlemelerin yapılarak bilgi işlem ağındaki bilgilerin güvenliği, gizliliği, erişilebilirliği ve kişisel mahremiyetin korunması için standart kuralların belirlenmesi amaçlanmıştır. Hastanelerde tüm bu standartlarda ve bilgi güvenliği uygulamalarında hastane yönetimi, bilgi yönetim sistemi çalışanları ve tüm çalışanların sorumluluğu vardır. Aşağıda Şekil 1'de hastanelerde bilgi güvenliği yönetim sürecine ait sağlık hizmetinde uygulanması gereken aşamalar bulunmaktadır. Hastanelerin hazırladığı politikalarının uygulanabilmesi en üst yetkili makamlar ile sağlanmalıdır. Böylece, yönetim, teknik ekip ve kullanıcı, belirtilen politikaya uyacaktır (Baran, 2018).

Şekil 1: Bilgi Güvenliği Grupları

Araştırmada; Gölcük Necati Çelik Devlet Hastanesi'nde çalışanların rol gruplarının belirlenmesi, rol grupları kapsamında sistem erişim yetkilerinin verilmesi ile yetki değişikliklerinin yönetiminde yapılan faaliyetlerin Sağlıkta Kalite Standartları Bilgi Yönetim Sistemi ve Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu doğrultusunda yapılmasının önemini vurgulamak amaçlanmıştır.

2. KAPSAM VE YÖNTEM

Araştırmada; Gölcük Necati Çelik Devlet Hastanesi'nde Sağlıkta Kalite Standartları Bilgi Yönetim Sistemi doğrultusunda kurumda çalışanların rolleri ve verilen yetkilerle, yaptığı iş ve işlemlerin bilgi güvenliğine uygunluğu ile rol grupları ve yetki değişikliklerinin yönetimi incelenmiştir. Kurumda Bilgi Yönetimi doğrultusunda hazırlanan mevcut tüm prosedürler, politikalar, yetki matrisi ve formların Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu'na uygun olarak hazırlanma durumları değerlendirilmiştir. Kurumun tüm yazılı düzenlemeleri, oluşturulan erişim kontrol matrisi, erişim izinlerinin verilmesi, parola ve şifre güvenliği, ağ kontrolü, yapılan bilgi güvenliği denetimleri, bilgi güvenliği kapsamında yapılan toplantılar ve bilgi güvenliği eğitimleri değerlendirilerek vaka çalışması yapılmıştır.

Araştırma kapsamında kurumda Sağlık Bakanlığı politikaları esas alınarak yapılan faaliyetlerin sağlık hizmetleri bilgi güvenliği yönetim sürecine katkı sağlayacağı düşünülmektedir.

3. BULGULAR

Hastanemizde bilgi güvenliği doğrultusunda hazırlanan yazılı düzenlemeler, erişim kontrol matrisinin oluşturulması, erişim izinlerinin verilmesi, bilgi güvenliği denetimleri, parola ve şifre güvenliği, ağ kontrolü ve bilgi güvenliği eğitimleri ele alınmıştır.

3.1. Yazılı Düzenlemeler

Hastanemizde; SKS 6 Hastane Bilgi Yönetim Sistemi, Bilgi Güvenliği Politikaları Kılavuzu ve Kişisel Verileri Koruma Kanunu (KVKK) doğrultusunda bilgi güvenliği faaliyetleri yürütülmektedir. Bu faaliyetlerde sorumluluklarımızı yerine getirmek üzere başta hastane yönetiminin katılımının sağlandığı, bilgi yönetim sistemi birim çalışanları ve kalite direktörünün de dâhil olduğu Bilgi Güvenliği Yönetim Ekibi kurulmuştur. Kurumda bilgi güvenliği ile ilgili yapılan çalışmalar ve çalışmaların takibi bu ekibin sorumluluğundadır. Ekip düzenli olarak toplanarak bilgi güvenliği ile ilgili dokümanları hazırlamak ve bunları gözden geçirmek, son dönem verilen yetkiler ve yetki değişikliklerinin takibini yapmak, ayrılış ve katılışlar ile verilen veya iptal edilen yetkileri değerlendirmek ve bilgi yönetim sistemi ile ilgili tüm verileri yürütmekle sorumludur. Kurum Bilgi Güvenliği Politikası, Bilgi Yönetim Sistemi Prosedürü, Erişim Kontrol Politikası, Erişim Kontrol ve Yetki Matrisi, Listesi gibi bilgi yönetim sistemi ile ilgili dokümanlar Bilgi Güvenliği Yönetim Ekibi takibinde hazırlanmış olup tüm kullanıcıların erişimine sunulmuştur. Belirlenen politikalar kapsamında; kurumumuzda öncelikle hastalara ait kişisel ve idareye ait kurumsal bilgilerin tutulduğu ana sunucu ve uç bilgisayarlardaki verilere kimin hangi seviyede erişeceğine ilişkin yetkilendirmeler sisteme ait modüller bazında yapılmıştır. Yapılan bu temel yetkilendirmeler de kendi içinde seviyelendirilerek kuruma ve hastaya ait bilgilerde mahremiyet ve gizlilik ilkelerine uygun olacak şekilde uygulama modülleri içerisinde yetki dâhilinde yapılacak eylemler belirlenmiştir.

3.2. Erişim Kontrol Matrisinin Oluşturulması

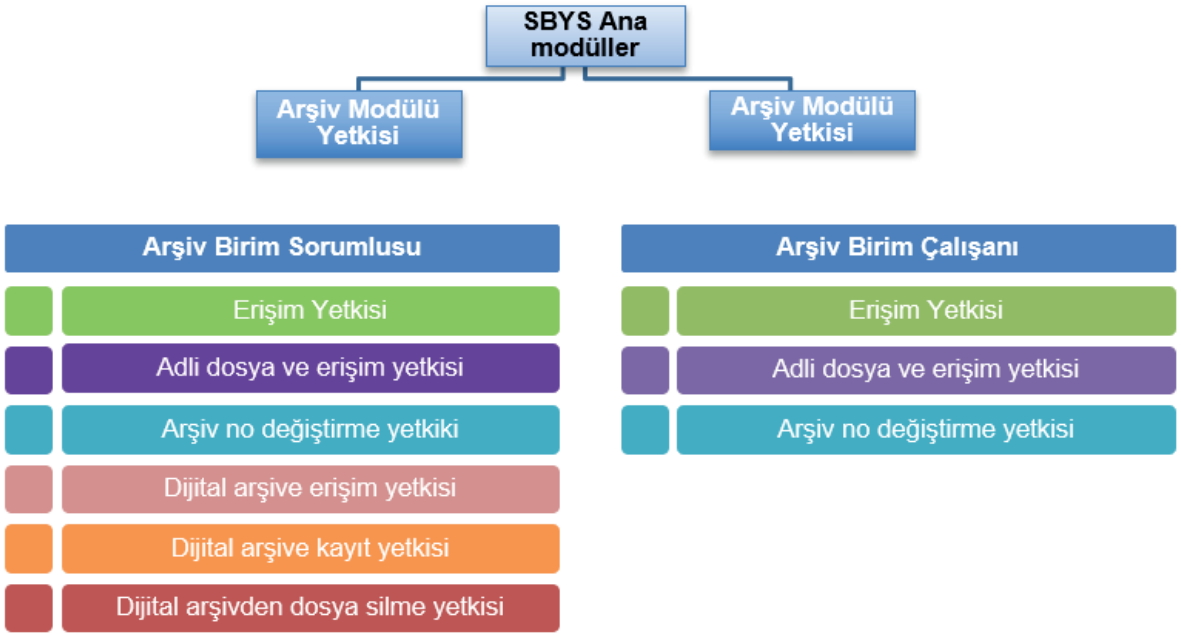
Hastane içerisindeki tüm personel ve birimlerin yetki ve sorumlukları ile bilgi kaynaklarını ilgilendiren süreçlerde uyulması gereken kuralların yer aldığı görev tanımları çalışan tüm personel tarafından çok iyi bilinmesi ve özümsenmesi amacıyla, hastane otomasyon sisteminde oluşturulan Kalite Yönetim Sistemi modülüne yüklenmiştir. Hastane personeline sorumlulukları çerçevesinde modüle erişim yetkisi verilerek gerektiği anda görev tanımlarına ulaşım imkânı sağlanmıştır. Kurumumuzda yönetim kadro ve bilgi güvenliği yönetim ekibi ile birlikte, organizasyon şemasında yer alan birimlerimiz ve görevler bazında rol grupları belirlenmiştir. Rol grupları belirlenirken bir birimde aynı veya farklı görevleri icra edenler, görev tanımı dışında farklı birimlerde çalışan personeller de göz önünde bulundurulmuştur. Aktif 860 çalışanın görev yaptığı hastanemizde toplamda 37 rol grubu belirlenmiş olup bu rol gruplarına hizmet aldığımız Sağlık Bilgi Yönetim Sistemi üzerinde bulunan 30 modül üzerinden yetki dağılımı yapılmıştır. Tablo 2'de Erişim Kontrol ve Yetki Matrisinin bir bölümü alınarak roller doğrultusunda verilen yetkiler görülmektedir.

Tablo 2: Erişim Kontrol ve Yetki Matrisi Listesi

	YETKİ MATRİSİ						
Roller/Yetkiler	**Yönetici**	**Hekim**	**Hemşire**	**Birim Sorumluları**	**Servis Sorumluları**	**Ayniyat Birimi**	**Psikologlar**
HBYS	X	X	X	X	X	X	X
KYS	X	X	X	X	X	X	X
İKYS	X	X		X	X		
PDKS	X			X	X		
İOBS	X	X	X	X	X	X	X

Bir role modül yetkisi verilirken o modülde her işlem yetkisi yerine görevi ve yapacağı işlemler kapsamında yetkiler tanımlanmıştır. Örneğin arşiv biriminde çalışanların öncelikle rol grupları, arşiv birim sorumlusu ve arşiv birim çalışanı olarak belirlenmiştir. Belirlenen bu rollerden sonra her iki role de arşiv

modül yetkisi verilmiş fakat arşiv modülünde işlem yapabilme sayısı her iki rolün yaptığı iş ve işlemlere göre sınırlandırılmıştır. Şekil 2'de görüldüğü gibi arşiv sorumlusuna modül üzerinde 6 işlem yetkisi verilirken arşiv birim çalışanı 3 işlem ile sınırlandırılmıştır. Kullanıcılara yetki verilirken yetki düzeylerinin eklendiği rol grubundaki çalışanlarla aynı olmasına dikkat edilir.

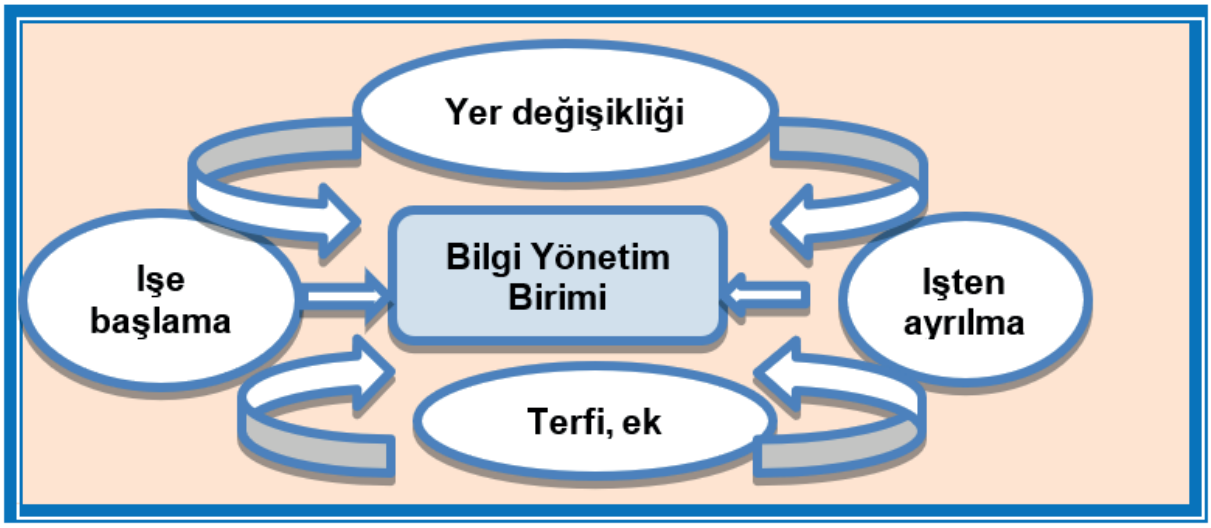


Şekil 2: Yetki Matrisi Arşiv Örneği

3.3. Erişim İzinlerin Verilmesi

Erişim kısıtlaması getirilmeyen; özel bir erişim kontrol tedbiri alınmasına gerek olmayan, herhangi bir gizliliği bulunmayan, herkesin erişimine açık olan bilgiler (hasta ve çalışan bilgilendirme ilanları, tetkik sonuç verme süreleri, sağlık bakanlığı bilgilendirme afişleri vb.) hasta ve hasta yakınlarını bilgilendirmek amacıyla kurumumuz internet sayfasında ve mevcut yerleşkemizde bulunan duyuru panoları vb. ortamlarda yayınlanmaktadır. (Bilgi Güvenliği Politikaları Kılavuzu s;63). Yetkilendirmeler hazırlanan Erişim Kontrol ve Yetki Matrisi Listesinde belirlenen rol grupları doğrultusunda Hastane Bilgi Yönetim Sistemi (HBYS) modülü üzerinden yapılmaktadır.

Çalışanlar işe başlarken "Personel İşe Başlama Formu" ile Bilgi Yönetim Sistemi (BYS) birimine başvurur. Atandığı göreve ve çalışacağı birime göre gereken yetki bilgi yönetim birimi çalışanı tarafından verilir, form işlem yapan çalışan tarafından imzalanır. Yetkilendirme kullanıcı erişim hakları iş akışı şekil 3'te belirtildiği şekilde işe başlama/ayrılma, terfi, sorumlulukların değiştirilmesi, ek görev veya görev yeri değişiklikleri sonrasında gözden geçirilir. Bu değişikliklerde İnsan Kaynakları Birimi tarafından Elektronik Belge Yönetim Sisteminden yazılan ve Bilgi Yönetim Sistemi birimine gelen görevlendirme yazısına istinaden birim çalışanı gerekli güncel yetkilendirmeleri yapar.



Şekil 3: Yetkilendirme Akışı

Çalışanların icra edecekleri görevin tanımına ve çalıştığı yere göre hangi bilgilere erişebileceği Erişim Kontrol ve Yetki Matrisi'nde belirlenmiştir. Rol grubu doğrultusunda yetki verilen çalışanlar yalnızca kendilerine verilen yetki kadar işlem yapabilir. Erişim kontrolünde bilgi ve bilgi işlemede yapılacak olan erişimlerin kısıtlanmasında, sadece yetki verilen kişilerin kontrollü ve kayıt altına alınarak bilgiye erişmesi amaçlanmıştır. Çalışanlar icra ettiği işe/role göre verilen yetkiler kapsamında kullanıcı olarak tanımlanmaktadır.

Çalışan, görev yaptığı kurum tarafından kendisine teslim edilmiş veya erişim yetkisi verilmiş olan bilgileri, sadece görevi ile ilgili işler için kullanır. Bu bilgileri kendi gizli bilgisi gibi korur ve bilmesi gereken yetkili kişiler haricinde hiçbir kimse ile paylaşmaz. Çalışan, bilgi paylaşabileceği kişiler konusunda şüpheye düşerse, bilgi yönetim sistemi birimi ile irtibata geçerek veriyi kimlerle paylaşabileceğini teyit edebilmektedir.

Bilgiye kimin ve hangi yetki ile erişeceğinin kararı, belirlenen yetki matrisi ve bireysel yetki taleplerine göre Bilgi Güvenliği Yönetim Ekibi kontrolünde verilir. Başta kişisel sağlık verilerinin işlendiği bilgi sistemleri olmak üzere erişim kontrolüne tabi tutulacak tüm sistem ve hizmetler için hazırlanan Erişim Kontrol Politikası'nda belirlenen esaslar, kullanıcılar başta olmak üzere ilgili tüm çalışanlara resmen duyurulmuştur.

Erişim izinleri verilirken, "görevlerin ayrılığı" ve "bilmesi gereken" prensiplerine göre hareket edilir. "Görevlerin ayrılığı" prensibi uyarınca; kritik iş süreçlerinin gerçekleştirilmesi için birden fazla kullanıcı görevlendirilir. Bilgiye erişim için aşamalı yetkilendirme yapılarak bir kişinin kendi başına tüm bilgi varlıklarına erişimi engellenir. Etki alanı yöneticisi, veri tabanı yöneticisi gibi teknik nedenlerle görev ayrımı yapılamayan süreçlerin kontrolü için ilave tedbirler alınır.

"Bilmesi gereken" prensibi uyarınca; sistemde bulunan süreçler ve kullanıcılara, sistem kaynaklarına erişirken, kendilerine atanmış görevlerini gerçekleştirmelerine yetecek kadar yetki verilir. Hizmet veya sistemlerin sahiplerince erişim hakları periyodik olarak incelenir. Bilmesi gereken prensibi uyarınca gereksiz olarak verilmiş yetkilerin kaldırılması sağlanır. İncelemeler tüm kullanıcılar için düzenli aralıklarla ve rutin olarak en az 6 (altı) aylık aralıklarla yapılır.

3.4. Bilgi Güvenliği Denetimleri

Kurumumuzda bilgi güvenliği doğrultusunda idari kontrol mekanizması oluşturmak amacıyla; bilgi güvenliği yönetim ekibi tarafından özellikle parola/şifre güvenliği ile yetki mekanizmalarını içeren "Bilgi Güvenliği Denetim Formu" hazırlanmış olup düzenli olarak saha denetimi yapılmakta ve tespit edilen uygunsuzluklara yönelik iyileştirmeler başlatılmaktadır. 31 maddelik soru listesinden oluşan denetim formları ile birlikte temiz masa temiz ekran uygulamaları, çalışma alanları ve birimlerde kullanılan bilgi teknolojileri araçlarının kontrolü yapılır. Temiz masa temiz ekran uygulamaları ile tüm çalışanlar kendi masalarının temizliği ve düzeninden sorumludur. Gizli ve üzeri bilgi sınıfındaki evraklar, parolalar, taşınabilir depolama ortamları, bilgi ve belgeler masa üzerinde, yazıcı veya faks gibi cihazlarda ya da kolayca ulaşılabilir yerlerde bırakılmaz. Kullanımı biten basılı evraklar kırpma makinesi ile kırpılarak imha edilir. Terk edilmiş masaların üzerinde not kâğıtları, kişisel ajandalar ve işle ilgili dokümanlar bırakılmamaktadır. Bilgisayar ekranlarında kuruma ait çalışma dosyaları, klasörler, herhangi bir formatta bilgi içeren dosyalar ve bunlara ait kısa yollar bulundurulmamaktadır. Çalışanların kullandığı masaüstü veya dizüstü bilgisayarların iş sonunda ya da masa terk edilecekse ekran kilitlenerek çalışma ortamlarında veri güvenliği şartlarını kontrol etmek personel sorumluluğundadır. Şifre, parola gibi kimseye söylenmemesi gereken gizli bilgiler hiçbir suretle masa üzerindeki bir dosyaya yazılmamakta, ekranın üzerine not şeklinde yapıştırılmamaktadır. Temiz masa temiz ekran uygulamaları ile ilgili olarak kurumda bulunan tüm masaüstü bilgisayarlarına farkındalık oluşturmak amacıyla ekran bilgilendirme mesajları gönderilmektedir.

3.5. Parola / Şifre Güvenliği

Kullanıcıların kimliklerinin doğrulanması için asgari teknik önlem olarak, parola kullanımı zorunlu tutulur. Hastanemiz çalışanı tarafından kullanılmakta olan parolalar işletim sistemi parolalarıdır. Domain sisteminde her çalışan için ayrı "adı. soyadı" formatında küçük harflerle kullanıcı tanımlanır. Şifrelerin en az sekiz (8) karakter olması, en az bir büyük harf, bir sayı veya karmaşık karakter içermesi, kullanıcı adıyla aynı olmaması sağlanır. Sistem tarafından yapılan ayarla, domaindeki kullanıcı şifrelerinin her doksan günde bir değiştirilmesi zorunlu kılınmıştır. On beş gün önceden kullanıcılar bilgisayarlarına giriş yaparken, gerekli ikaz, sistem tarafından otomatik olarak ekranlarında görünmektedir. Kullanıcı ilk verilen geçici şifreyle sisteme giriş yaptığında, yeni bir şifre belirlenmesi sistem tarafından otomatik olarak istenmektedir. Sistemin ilk girişte belirlenmesini istediği yeni şifrenin tanımlanması, uygunluğu ve korunması ilgili personelin sorumluluğundadır. Belirli bir şifre ile yapılan tüm işlemlerin idari ve yasal sorumluluğu söz konusu şifrenin tanımlanmış kullanıcısına ait olduğundan, kullanıcıya ayrılmış şifre hangi şartla olursa olsun başkalarına verilemez. Bilgi Güvenliği kurum denetimlerinde bu konulara dikkat edilir. Çalışanların yer değiştirmesi veya işten ayrılması durumunda şifrenin kapatılma işlemleri yapılır. Bilgi güvenliği açısından ilişiği kesilen çalışanın şifresinin bir an önce iptali esastır. Çalışanların yer değiştirme, işten ayrılma durumunda yeni görevlendirme yazıları kurum içinde İnsan Kaynakları birimi tarafından Bilgi Yönetim Sistemi birimine iletilir. İlişiği kesilen çalışanın tüm şifreleri ve kullanıcı yetkileri kullanıma kapatılır. Şifrenin 24 saat içerisinde iptali Bilgi Yönetim Biriminin sorumluluğundadır.

3.6. Ağ Kontrolü

Bilgi varlıklarına yapılan erişimler için iz kayıtları oluşturulmakta olup erişim ile ilgili hangi kullanıcı hareketlerinin izleneceği hususu varlık sahipleri tarafından belirlenmektedir. Kurumumuz SBYS iz kayıtları hizmet aldığımız SBYS yazılım firması tarafından takip edilmekte ve yasal sürede saklanmaktadır. Sağlık Bilişim Ağı (SBA) dışındaki ağlar güvensiz ağ olarak kabul edilir. Yetkisiz erişimler de dâhil olmak üzere iç ağı dış tehditlerden korumak için sınır güvenlik sistemleri (güvenlik duvarı vb.) tesis edilir.

Kullanıcı ve sunucuların bulunduğu ağlar, güvenlik duvarları ve/veya ağ cihazları erişim kontrol listeleri vasıtasıyla ayrılır. Veri Tabanı Yönetim Sistemi sunucularının bulunduğu ağ kesimlerinde VLAN topolojisi ile sunucular ve son kullanıcıların iletişimi belirlenmiş olup normal kullanıcıların erişimleri engellenmiştir.

Bilgi varlıklarına fiziksel olarak yapılacak erişimler için Kılavuz'un 8. maddesindeki Fiziksel ve Çevresel Güvenlik maddesinde belirtilen önlemler alınır (SB, 2019). Güvenlik sınırları belirlenirken kişilerin kontrolsüz olarak giriş çıkış yapabilecekleri herhangi bir boşluk bulunmamasına dikkat edilir. Bu tür boşlukların kapatılması/korunması için ilave tedbirler alınır. Sunucu odası ve Bilgi Yönetim Sistemi birimi sadece yetkili personele erişim izni vermektedir. Özel nitelikli kişisel verilere (kişisel sağlık verileri) erişim için KVKK'nin 2018/10 sayılı kararında belirtilen teknik ve idari tedbirler alınmaktadır. 90 gün veya daha fazla süre ile kullanılmayan hesaplar devre dışı bırakılır ve erişim izinleri askıya alınır. Bu süre kurumların bilgi güvenliği alt komisyonları tarafından değiştirilebilir. Her bir sistem için belirlenecek süreler, kurumların erişim kontrol politikası içinde yazılı olarak kayıt altına alınır.

3.7. Bilgi Yönetim Eğitimleri

Kuruma yeni başlayan tüm çalışana bilgi yönetim sistemi birimi çalışanı tarafından; Bilgi Güvenliği Farkındalık Bildirgesi okutulup kişiye tebliğ edilir. Farkındalık bildirgesi ile birlikte çalışana yürüteceği işlerde kullanacağı bilgisayarların tahsis edilmesi ve kurumsal ve hasta bilgilerinin çalışan tarafından kullanımına izin verilmesi ile bu konuda üstlenmiş olduğu sorumlulukları anlatılmaktadır. Hastanemiz hizmet alımı kapsamında merkezi yerleşke veya hastane dışında çalışan tüm firma/kullanıcı kuruluş ve ilgili kullanıcılarına, hastanemize ait bilgi teknolojileri sistemlerinin, bilgi işlem ağının kullanımına ve kişisel sağlık kayıtlarının güvenliğine ilişkin usul ve esaslarını içeren Bilgi Güvenliği Sözleşmesi okutularak tebliğ edilmektedir. Bu alanda imzalatılan sözleşmeler ile çalışanlara bilgi güvenliği alanındaki yasal mevzuatlara, donanım, yazılım ve iş alanına ait verileri düzenlemelere uygun kullanması gerektiği sorumluluğunu hatırlatılmak amaçlanmıştır.

Kurumumuzda, Eğitim Birimi tarafından her sene düzenli olarak hazırlanan Eğitim Planı doğrultusunda düzenli olarak kurum içi tüm çalışanları kapsayan bilgi güvenliği eğitimleri verilmekte ve kayıt altına alınmaktadır. Eğitimler bilgi güvenliği sorumlusu tarafından verilmekte olup bilgiyi yönetmek adına gerekli tüm konuları içermektedir. Eğitimler hastanede bilgi güvenliği sürecinin sadece bilgi yönetim sistemi teknik birim/personelinin işi olmadığı, bilgi sistemlerini kullanan tüm hastane çalışanlarının, yeterli bilgi, yetenek veya eğitime sahip olmaları ve bilgi güvenliği sistemine gereken önemi vermelerini amaçlamalıdır.

4. SONUÇ

Teknolojik uygulamaların girdiği her sektörde olduğu gibi sağlık kurum ve kuruluşlarında da geniş bir şekilde kullanılmaya başlanan hastane bilgi sistemlerinde özellikle insanların sağlık sorunları ile ilgili mahrem bilgileri yer almaktadır. Hastane bilgi sistemleri hasta bilgileri başta olmak üzere her türlü verinin farklı kullanıcılar tarafından, birbiriyle bağlantılı olduğu modüller aracılığı ile, ana bir veri tabanına girilmesi ve gerekli olan tüm çıktıların bu veri tabanından güvenilir bir şekilde geri alınmasını sağlayan sistemeler bütünüdür. Hastane bilgisi sistemlerinin kurulum amaçları olan gizlilik bütünlük ve erişilebilirliğin sağlanması amacıyla kurumlar bilgi güvenliği ile ilgili yasal mevzuatlar doğrultusunda iş ve işlemlerini yürütürler. Bilgi güvenliği kapsamında kurumlarda yapılan ve yapılması gereken teknik ve

idari tüm işlemler yönetimsel ve zaman alıcı süreçler gibi görünseler de ortaya çıkan bir bilgi güvenliği zafiyeti durumunda iş ve süreçlerinin etkilenmeden devam etmesini sağlamak çok daha fazla emek ve zaman gerektirmektedir. Planlı ve sürekli olarak çalışanlara verilecek olan bilgi güvenliği eğitimleri ile teknik, idari, yönetimsel, fiziksel ve bireysel tedbirler, bilgi güvenliği zafiyetlerinin önüne geçmek ve konunun kurumsal kültür boyutunu oluşturmak için amaçlanmış olacaktır.

Çalışmada kurumlarda bilgi güvenliği yönetim ekibinin rolü ve önemi, bilgi güvenliği ile ilgili yazılı düzenlemeler ve bu konuda farkındalık yaratılması ve erişimlerin kontrollü ve denetim mekanizmaları dâhilinde verilmesi konularına değinilmiştir. Hastane içi rol gruplarının, personel kurumda çalıştığı süre boyunca çalıştığı birim ve aldığı rol kapsamında belirlenip belirlenen rol gruplarının düzenli olarak güncellenmesi, yazlı talep olmaksızın yetki verilmemesi, yazlı taleplerin bilgi güvenliği yönetim ekibi tarafından değerlendirildikten sonra uygun görülmesi durumunda verilmesi ve tüm bu eylemlerin izlenebilir olması ile kurum içi rol çatışmalarının önüne geçtiği düşünülmektedir.

Kurumlara ve hastaya ait bilgilerin gizlilik ve mahremiyetinin önemli olduğu ve hasta güvenliğinin kurum kalite politikalarının üst sırasında yer aldığı kabul edilerek hizmet sunumunun her aşamasında bilgi güvenliğinin kontrol altına alınması doğrultusunda uygulamaların yürütülmesi amaçlanmalıdır. Bilgi Güvenliği kontrol adımlarında öncelikli olarak Sağlık Bakanlığının konu ile ilgili yayınlamış olduğu kılavuzlar, politikalar ve rehberler doğrultusunda iş ve işlemlerimizi yürütmek ve takip etmenin önemi yönetim ve tüm çalışanlar tarafından benimsenmelidir. Bu doğrultuda güncel yayınların takip edilmesi ve değişiklik durumlarında çalışanlar ile yapılan toplantılarda bilgilendirme ve bilinçlendirme çalışmaları yapılmalıdır. Başarılı ve etkin işleyen bir bilgi güvenliği bilinçlendirme süreci oluşturulabilmesi için bu alandaki görev ve sorumlulukların bilgi güvenliği yönetim ekipleri tarafından açık ve net bir biçimde belirlenmesi gerekir. Olgunlaşmış bir bilinçlendirme süreci, bu görev ve sorumlulukların sahipleri tarafından doğru anlaşılması, bilinmesi ve uygulanması ile mümkündür. Hastane yöneticilerinin hasta ve çalışan güvenliği ile ilgili değerlendirmeler yaparken bilgi güvenliği konuları ile birlikte düşünülmesi ve bu doğrultuda çalışmalar yapılması kurumda bütünleşik bir güven kültürünün oluşmasını sağlayacaktır.

Bu vaka çalışmasında da görüldüğü gibi kurumlarda bilgi güvenliğinin sağlanmanın yolu; yöneticilerin tam desteğini alan bir süreç başlatarak kurumsal bilgi güvenliği politikalarını oluşturmak, politikalar doğrultusunda ilgili prosedür süreçlerini dokümante etmek ve yasal mevzuatlar doğrultusunda izleme, iyileştirme, güncelleme ve denetleme çalışmalarını aynı kararlılıkla devam ettirmekten geçmektedir. Tüm kurum çalışanlarına bilgi güvenliği yönetiminin bilgi yönetim sistemi birimi kapsamında teknik bir iş olmadığı, kurumun tüm birimlerinin ve çalışanlarının sorumluluk yüklenmesi gerektiği etkili bir şekilde ve yerinde anlatılmalıdır. Kurumlarda düzenli olarak verilen bilgi güvenliği eğitimleri ve kurumsal bilinçlendirme ile bilgi güvenliği kültürünün oluşturulması gerçekleşecek olup bilgi kaynaklarını ilgilendiren her işlemde çalışanların bilgiyi güvenle işlemesi ve güvende tutmasını sağlanacaktır.

Bu doğrultularda yapılan çalışma kapsamında aşağıdaki öneriler geliştirilmiştir:

- Bilgi güvenliği yönetim sistemine ait sorumluluklar ve görevlerin belirlenmesi,
- Bilgi güvenliği ile ilgili yapılan çalışmalar ve çalışmaların takibinin yapılması amacı ile Bilgi Güvenliği Yönetim Ekibi'nin oluşturulması,
- Sağlıkta Kalite Standartları 6 Hastane Bilgi Yönetim Sistemi, Bilgi Güvenliği Politikaları Kılavuzu ve Kişisel Verileri Koruma Kanunu (KVKK) doğrultusunda bilgi güvenliği faaliyetlerini kapsayan kurum dokümanlarının oluşturulması,
- Bilgi güvenliği yönetim sistemi kapsamında oluşturulan yazılı düzenlemelerin tüm kurumda ulaşılabilir ve uygulanabilirliğinin sağlanması,

- Bilgi güvenliği yönetim sisteminin etkili işlemesi amacıyla, kurum yönetimi ve çalışanların iş birliği içinde olması,
- Kurumda yönetim kadro ve bilgi güvenliği yönetim ekibi ile birlikte, organizasyon şemasında yer alan birimler ve görevler bazında rol grupları belirlenmesi,
- Belirlenen rol gruplarına göre modül yetkisi ile o modüldeki işlem yetkilerinin tanımlandığı erişim kontrol matrisinin oluşturulması ve kişilere bildirilmesi,
- Bilgi güvenliği doğrultusunda idari kontrol mekanizması oluşturmak amacıyla; bilgi güvenliği yönetim ekibi tarafından saha denetimleri yapılması,
- Bilgi güvenliğini sağlayacak personele tam yetki verilmesi, yetkili kişilerin gördüğü bilgiyi başkasının gör(e)memesi, sağlamak amaçlı gerekli şartların oluşturulması,
- "Temiz masa temiz ekran" uygulamasının tüm çalışanlar tarafından benimsenmesinin sağlanması,
- Tüm personele düzenli olarak bilgi güvenliği eğitimi verilmesi.

KAYNAKLAR

Baran, S. (2019) "Hastanelerde Bilgi Güvenliği Yönetimi: Nitel Bir Araştırma", Süleyman Demirel Üniversitesi Vizyoner Dergisi, 10(23), 113.

Bartlett, M. (2008). "E-health: Enabler for Australia's Health Reform", http://www.health.gov.au/nhhrc/publishing (18.02.2022).

Eriş, H. (2017). "Kalite Sistemi ve Bilgi Güvenliği Sistemlerinin Hasta Güvenliği Üzerine Etkisi: Bir Üniversite Hastanesi Uygulaması", Sağlık Akademisyenleri Dergisi, 4(3), 207-209.

İleri, S. (2016). "Örgütlerde Bilgi Güvenliği Yönetimi, Kurumsal Entegrasyon Süreci ve Örnek Bir Uygulama", Anadolu Üniversitesi Sosyal Bilimler Dergisi, 17(4), 56.

Marşap, A. (2010). "Sağlık İşletmelerinde İnsan Kaynağının Kurumsal Bilgi Güvenliği Kültürü Gelişimi" Bilişim Teknolojileri Dergisi, 3(1), 32.

Öğütçü, G., Gürel, N. & Cula, S. (2011). "Elektronik Sağlık Kayıtlarının İçeriği, Hassasiyeti ve Erişim Kontrollerine Yönelik Farkındalık ve Beklentilerin Değerlendirilmesi". VIII. Ulusal Tıp Bilişimi Kongresi, 17-20 Kasım, Antalya.

Sağlık Bakanlığı (2019), Bilgi Güvenliği Politikaları Kılavuzu, SB,Ankara

Şahin, A. (2008). "Kamu Kurumlarında Bilgi Teknolojilerinin Kullanımında Yaşanan Sorunlar: Konya Kaymakamlıkları Örneği", Amme İdaresi Dergisi, 41(1), 158.

Şahinaslan, E., Kandemir, R. & Şahinaslan, Ö. (2009). "Bilgi Güvenliği Farkındalık Eğitimi Örneği", Akademik Bilişim Konferansı Bildirileri, 11-13 Şubat, Şanlıurfa.

Varol Ş., Orhan F., Tuncer S., & Akyüz. S. (2016). "Sağlık Kurumlarında Bilgi Güvenliği Bağlamında Biyometrik Sistemler", Sağlık Akademisyenleri Dergisi, (3)4,156.

Yılmaz, H. (2014). "TS ISO/IEC 27001 Bilgi Güvenliği Yönetimi Standardı Kapsamında Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Bilgi Güvenliği Risk Analizi", Denetişim, sayfa 51.