RAED JOURNAL
RAED dergisi

Derleme / Review

RAED Dergisi 2015;7(1):16–19. © 2015 RAED
doi:10.2399/raed.15.73792

Geliş tarihi / Received: Haziran / June 10, 2015
Kabul tarihi / Accepted: Temmuz / July 14, 2015

Dijital çağda sağlık çalışanları ve bilgi güvenliği

Health professionals in the digital age and information security

Pınar Kılıç Aksu[1], Leyla Köksal[2], Gonca Mumcu[2]

[1]Yeditepe Üniversitesi Sağlık Bilimleri Fakültesi, İstanbul; [2]Marmara Üniversitesi Sağlık Bilimleri Fakültesi, Sağlık Yönetimi Bölümü, İstanbul

Özet

Günümüzde sağlık hizmetlerinde, elektronik uygulamalardaki artış, ağ sistemlerinde bilginin paylaşımı, veriye birçok noktadan erişimin olması ve veri kaybı yönündeki tehditlerin artışı, bilgi güvenliği için önemli faktörlerdir. Sağlık çalışanları da kurumlarda bilginin üretimi ve paylaşımı sürecinde etkili rol oynamaktadır. Bu derlemenin amacı, dijital çağda bilgi güvenliği çerçevesinde sağlık çalışanlarının rollerini incelemektir.

Anahtar sözcükler: Bilgi güvenliği, sağlık çalışanları, e-sağlık

Summary

Novadays, increase in electronic applications, sharing information by network systems, access to data in different points and threats of data loss in healthcare are important factors for information security. Healthcare professionals have also effective roles in the process of information production and sharing in the organisations. The aim of the review is to examine the roles of health professionals in the frame of information security in the digital age.

Keywords: Information security, health profesionals, e-health

E-sağlık Uygulamaları

Ülkemizde sağlık hizmetlerinin sunumunda verinin elektronik ortama aktarıldığı, kurumlar ve sağlık çalışanları arasında paylaşımının olduğu bir süreç yaşanmaktadır. "Türkiye Sağlıkta Dönüşüm Programı" (2003) kapsamında, sağlık hizmetlerinde sekiz ana başlık altında önemli değişimler yaşanmıştır. Bu başlıklardan biri, bilgiye hızlı ve etkili erişimi sağlayan "Sağlık Bilgi Sistemi"dir. Elektronik sağlık kayıt sisteminin bir parçası olan Aile Hekimliği Bilgi Sistemi'nin oluşturulması, Tele-Tıp projesinin uygulanması, doktor veri bankasının oluşturulması, klinik uygulamalarda uluslararası hastalık sınıflamasının kullanılması gibi bileşenlerin uyum içinde çalışabilmesi için bir sağlık bilgi sistemine ihtiyaç duyulmuştur. Bu sistem sağlık çalışanları ve kurumlar arasında veri paylaşımını sağlarken, sağlık politikalarını geliştirenler ve karar vericiler için de analiz, raporlama ve istatistik desteği sağlamaktadır.[1] Elektronik sağlık kayıtları, hekim orderlarının elektronik ortama girişi, e-reçete, elektronik karar destek sistemleri gibi klinik bilgi teknolojileri, sağlık hizmetlerinin kalitesini ve hasta güvenliğini artırmaktadır.[2] Sağlık çalışanları hizmet üretimi sürecinde; hastane bilgi yönetimi sistemlerini (HBYS) yoğun olarak kullanmaktadırlar. Bu sistemin kullanımı ile hastanın klinik bilgilerine, konsültasyonlara, laboratuvar ve tıbbi görüntüleme verilerine hızlı erişimin sağlanması,[3] finansal kayıtların tutulması, kaynakların uygun şekilde kullanılması, hizmet kalitesinin ve hasta güvenliğinin[4] artırılması hedeflenmektedir.[5,6] Ancak çalışanların iş süreçlerini de değiştiren bir özelliği olduğu da unutulmamalıdır.[7] Bu süreçte verilerin elektronik ortama taşınma-

İletişim / Correspondence:
Yard. Doç. Dr. Pınar Kılıç Aksu. Yeditepe Üniversitesi Sağlık Bilimleri Fakültesi, 26 Ağustos Yerleşimi, İnönü Mah., Kayışdağı Cad. Ataşehir, İstanbul.
e-posta: pinarkilicaksu@yahoo.com

Çıkar çakışması / Conflicts of interest: Çıkar çakışması bulunmadığı belirtilmiştir. / *No conflicts declared.*

www.raeddergisi.org
doi:10.2399/raed.15.73792
Karekod / *QR code:*

sı ve bilgi sistemlerini kullanıyor olmak, bilgi güvenliği konusunu da gündeme getirmektedir.

Günümüzde bu değişimlere paralel olarak, sağlık çalışanları, günlük iş akışları içinde bilgisayar teknolojilerini yoğun olarak kullanmaktadırlar. Böylece elektronik ortama taşınan tüm verilerin kurum içinde ve kurumlar arasında paylaşımı sağlanabilmektedir.[8] Bu sürece paralel olarak, hasta verilerinin elektronik ortamda depolanması ve iletilmesi ile birlikte, bilgi güvenliği de giderek önem kazanan bir konu olmaktadır.[9]

Bilgi Güvenliği ve Bilgi Güvenliği Sağlama Yöntemleri

Bilgi güvenliği; verilerin ya da bilgilerin, saklanması ve taşınması sırasında, bütünlüğünün bozulmadan, izinsiz erişimlerden korunması için gösterilen çabaların tümü olarak düşünülebilir. Bir başka ifade ile bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak her türlü ortamda istenmeyen kişiler tarafından erişiminin önlemesi olarak da tanımlanabilir.[10] Günümüzde bilginin, gizlilik, bütünlük ve erişilebilirlik nitelikleri bakımından sürekli olarak korunması gerekmektedir.[11]

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

Bütünlük: Bilginin yetkisiz kişiler tarafından değiştirilememesidir. Ayrıca, bilginin depolandığı yerde ve aktarılırken doğru ve tam olduğu anlamına gelir.

Erişilebilirlik: İhtiyaç duyulduğunda bilginin, yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olmasıdır.[12]

Bilgi güvenliği sağlama araçları; fiziksel güvenlik önlemleri (güvenli çevre vb), kullanıcı doğrulama yöntemleri (akıllı kart, tek kullanımlık parola), uygun şifreleme, yönetsel önlemler (kurumsal güvenlik politikaları), standartlar ve prosedürler (konfigürasyon yönetimi, yedekleme ve yedekleme ortamlarını saklama, olay müdahale, iş sürekliliği ve felaket kurtarma prosedürleri), anti-virüs sistemleri, güvenlik duvarları ve erişim denetimi olarak sıralanabilir.[13] Bu tür önlemlerin alınması tek başına yeterli değildir. Bilgi güvenliği bilgi yönetimi içinde bir süreç olarak görülmelidir. Her kurum bir güvenlik politikası oluşturmalı, bunu yazılı olarak raporlayarak çalışanlarına ve paydaşlarına aktarmalıdır. Bilgi yönetim standartları benimsenmeli ve uygulanmalıdır. Unutulmaması gereken en önemli konu, zincirin en zayıf halkasının insan kaynağı olduğudur.[14] Veri koruması ile ilgili temel alanlar; kullanıcı kimliğinin onaylanması, verilerin şifreleme yolu ile güvenlik altına alınması, elektronik verilerin bölümlere ayrılması ve internet güvenliği olarak tanımlanmaktadır.[15] Yetkili olmayan bir kişi şifrelenmiş dosyaya erişim sağlamak için, kullanıcı adı, şifre ve biyometrik oturum açma basamaklarını geçememelidir. İşin devamlılığı açısından verilere farklı kullanıcıların erişimi gerekiyorsa, uygun yetki seviyeleri düzenlenerek, yeni kullanıcı tarafından okunabilir hale getirmek için dosyanın şifresini açabilen bir yapılanmanın olması uygundur.[15]

Sağlık Çalışanları ve Bilgi Güvenliği

Sağlık çalışanları açısından; bilgi güvenliğinin sağlanması için kimlik belirleme yöntemleri olarak kullanıcı adı ve şifre yaygın olarak kullanılmaktadır. Kullanılan şifre yapıları incelendiğinde, sağlık çalışanlarının büyük oranda birbirini takip eden rakamlar, kişisel isim/bölüm adı gibi kolay tahmin edilebilecek şifreleri kullandığı görülmektedir. Bu durumun sağlık çalışanları arasında birbirine duyulan yüksek güvenin sonucu olduğu düşünülmektedir.[16] Özellikle basit şifreli oturum açma uygulanması ciddi bir sorundur, uzun ve rakam harf kompleksi olan şifreler uygulama açısından daha güvenlidir.[15] Sağlık çalışanlarının kendine ait bir şifresi olmasına rağmen, bunlar çalışma alanına asılan bir parça kağıt üzerine yazılabilmektedir. Bu uygulamalar ile hasta verileri açısından güvenlik ihlali riskinin arttığı görülmektedir.[17]

Hastaya ait bilgilerin kurumlar arasında paylaşımı için onam formu alınması gereklidir.[18] Geleneksel hasta-hekim ilişkisi modelinde, bilgilendirilmiş onam sağlık çalışanının kontrolü altındadır.[19] Hasta verilerinin elektronik ortama taşındığı bir sistemde, tıbbi kimlik hırsızlığı rahatsız edici ve giderek daha yaygınlaşan bir durumdur. Hastaların bilgilerini korumakta başarısız olan uygulamalar, kurumların itibarını riske atmakta ve büyük olasılıkla ciddi yasal sorunlara yol açmaktadır.[20] Bu açıdan elektronik ortamda tıbbi birim çalışanları için hasta mahremiyetini korumanın giderek zorlaştığı görülmektedir.[16]

Sağlık bilgi teknolojileri, sağlık sektöründe verimliliği sağlık kalitesini ve/veya sistem verimliliğini artırmanın, bakım kalitesini iyileştirmenin ana yollarından biri olarak sunulmaktadır. Ayrıca tıbbi uygulamaları iyileştirebilirler, iyi uygulama yönergelerine erişimi kolaylaştırarak karar verme sürecini destekleyebilirler, tanı işlemlerini kolaylaştırabilirler ve önemli parametreleri hatırlatan uyarılar üretebilirler. Bu açıdan hasta verilerinin işlenmesini, alınmasını, değiştirilmesini, dağıtımını, gönderilmesini, depolanmasını ve açıklanmasını yönetecek politikalara ihtiyaç duyulmaktadır.[17]

Genel uygulama anlamında, bilgisayar güvenliğindeki en önemli konu verilerin yedeklenmesidir. Ortaya çıkan önemli sorunlar içinde, fiziksel güvenlik ve internet güvenliği (güvenlik duvarları, anti-virüs çözümleri ve şifreleme) ile hasta kayıtlarının gizliliği yer almaktadır.[17] Bilgisayar sistemi çöktüğünde uygulamaya konulacak felaket planlarına gereksinim duyulmaktadır. Yine yapılan çalışmalar, bir felaket planının bulunmamasının önemli bir risk oluşturduğunun düşünüldüğünü göstermektedir. Hasta randevularının alınması, kayıtların yapılması ve hastaların tedavi edilmesine olanak sağlayacak bir alternatif sistemin hazırda tutulmasının, hayati öneme sahip olduğu düşünülmektedir.[17] Bilgisayarların virüsler gibi zararlı yazılımlar karşısında korunamamasının, yüksek risk oluşturduğu gözlemlenmektedir. Bu durum özellikle tıbbi çalışanlar ile uygulama personelinin düzenli olarak internet erişimine sahip olduğu koşullarda geçerlidir. Bilgisayar sistemlerinin çökmesi gibi süregelen sorunların düzeltilmesi, maliyetlidir, zaman israfına yol açar ve günlük operasyonları kesintiye uğratır.[16]

Tıbbi veriye erişimin değerlendirmesine yönelik temel gereksinim veriye kimin eriştiğinin (ya da erişmeye çalıştığının) kaydedilmesidir. Sonuç olarak, her kullanıcı doğrulanması mümkün olan, kendisine özgü bir kimlik tanımlayıcısına sahip olmalıdır. Günümüzde, sağlık kurumu içindeki sistemde bir çok noktaya erişim kullanıcılara sınırlıdır. Dolayısıyla bir dosya, belirli erişim haklarının tanımlanmış olduğu kullanıcılar tarafından açılabilmektedir. Kullanıcılar sıklıkla kendilerini bir kullanıcı adıyla tanıtırlar ve kendilerine verilen kişisel bir şifre ile kimlik doğrulaması yaparlar. Şifre korumasının zayıf yönlerine karşı ek tedbirler önerilebilmektedir. Erişim yetkileri standart olmayıp bunların bazıları kullanıcının mesleğini esas alırken, diğerleri kullanıcının rolü ve hasta ile ilişkisini göz önünde bulundurmaktadır.[11] Hangi verilere kimlerin erişebileceğini gösteren anlaşılabilir bir protokolün bulunması, hem klinik hem de finansal bilgilere uygun olmayan erişim riskinin azaltılması için önemlidir.[17]

Sağlık bilgi teknolojileri uygulamalarının hastanelerde, hekimlerin çalışma pratikleri üzerine (hızlı yanıt, hataların önlenmesi) bir etkiye sahip olduğu görülmektedir. Bu teknolojilerin uygulanması, sağlık çalışanlarından oluşan bir grubun yerine getirdiği görevlerin doğasını değiştirebilir. Örneğin bazı rutin görevlerin gerçekleştirilmesinde hemşirelerin harcadıkları süre, hasta merkezli bakıma daha iyi odaklanması gerekirken, onları diğer görevlere yönlendirilebilmektedir. Yine geçmişte mesleki uzmanlık gerektiren bazı görevler (reçetelerin eczacı tarafından onaylanması vb.) kısmen otomasyona bağlanmış olup bu mesleklerin sergiledikleri rolleri önemli ölçüde değiştirmektedir. Bu açıdan sağlık bilgi teknolojilerinin kullanımı, mesleklerin kendilerine atanmış rollerini ve sorumluluklarını planlı ya da beklenmedik şekilde değiştirebilir.[4]

Günümüzde sağlık bilgi teknolojileri hizmet sunumunun önemli bir bileşeni durumundadır. E-sağlık uygulamalarına paralel olarak; sağlık çalışanlarının bilgi teknolojilerini kullanmadan hizmet üretimeleri söz konusu değildir. Bu noktada sağlık çalışanlarının bilgi güvenliğini sağlamada gerekli önlemleri alması ve kurumsal politikalara uyum göstermesi, ileriye dönük gelişebilecek hukuki süreçleri elimine etmek açısından büyük önem taşır. Türkiye'de sağlık bilgilerinin saklanması ve gizliliği ile ilgili çeşitli düzeylerde düzenlemeler yürürlüktedir. Sağlık bilgilerinin gizliliği konusunda hekimlerin sorumluluğu bu düzenlemelerin bazıları ile hüküm altına alınmıştır. Öncelikle Türkiye Cumhuriyeti Anayasası'nda belirlenen temel ilkeler dikkatten çıkarılmamalıdır. Ayrıca Medeni Kanun ve Türk Ceza Kanunu'nda yer alan genel hükümler de bu alanda geçerlidir. Hekimlerin ve diğer sağlık personelinin sır saklama yükümlülüğünü ihlal etmesi, ceza kanunları çerçevesinde suç olarak düzenlenmiştir ve tazminat sorumluluğunu gerektirmektedir. Sağlık verilerinin gizliliği ile ilgili hukuksal düzenlemeler incelenirken, Türkiye'nin onayladığı ve taraf olduğu bazı uluslararası sözleşmeler de dikkate alınmalıdır. Burada öncelikle Avrupa İnsan Hakları Sözleşmesi gibi temel insan hakları metinleri akla gelir. Ancak İnsan Hakları ve Biyotıp Sözleşmesi gibi konu ile ilgili farklı sözleşmeler de bulunmaktadır. Türkiye'de sağlık verilerinin gizliliğine ait temel kaynağın, Hasta Hakları Yönetmeliği olduğu söylenebilir. Yönetmelikteki ilgili hükümler ile kişisel verilerin korunmasının temel ilkeleri büyük oranda karşılanmaktadır. Yasa ile izin verilen durumlar ve tıbbi zorunluluk dışında, hastanın özel ve aile yaşamının gizliliğine dokunulamayacağı, hasta hakları ile ilgili ilkeler kapsamında yer almaktadır.[21]

Günümüzde klinik araştırmalar açısından bakıldığında; hasta verilerinin kayıt altına alınabilmesinde hastanın bilgilendirilmesi, onamının alınması ve seçim hakkının olduğu bildirilmektedir. Ancak bilgi güvenliği kapsamında hasta kimliğinin gizlenmesi ve anonimleştirilmesinde sağlık çalışanlarının sorumluluğu vardır.[22]

Sağlık çalışanları gerekli politika ve protokolleri uygulayarak hasta bilgilerinin gizliliğini sağlamalıdır. Ayrıca sağlık çalışanı telefon, e-posta ve faks gibi yöntemlerle hasta bilgilerini hastalara, refakatçilerine ve/veya hukuki temsilcilerine, meslektaşlarına aktarırken güvenliğin diğer önemli bir unsuru olan mahremiyeti de göz önünde bulundurarak hareket etmelidir. Üçüncü kişilerle verilerin paylaşımı ancak iletilen tarafta uygun veri korumanın benimsemiş olması ile mümkündür.[22]

Tablo 1. Sağlık çalışanlarının bilgi güvenliği ile ilgili dikkat etmesi gereken hususlar

• Çalışanlar bilgisayarda kendi oturumlarının başkaları tarafından kullanılmadığından emin olmalıdır.
• Bilgisayar ve HBYS kullanımı sırasında, sayı ve harfin bir arada kullanıldığı uygun kalitede şifre kullanmalıdır.
• Şifrelerini kimseyle paylaşılmamalı ve belirli aralıklarla değiştirmelidir.
• Çalışma alanından ayrılındığında, mutlaka bilgisayarı/oturumu kapatmalıdır.
• Bilgisayar ekranlarının ve varsa hasta bilgisi içeren yazılı dökümanların, yetkilendirilmiş çalışanlar dışındaki kişilerin görmesini engellemelidir.
• Hastalardan bilgilendirilmiş onam almalıdır.
• Anti-virüs programlarının kullanıldığından emin olmalı, ihtiyaç halinde yazılım ve donanım güncellemelerinin yapılmasını talep/takip etmelidir.
• Ilgili ve yetkili olmayan kişiler ile hasta verilerini sözel ya da yazılı olarak paylaşmamalıdır.
• Ihtiyaç halinde bilgi güvenliği eğitimi talep etmelidir.
• Kurum bilgi güvenliği politikalarından haberdar olmalı ve prosedürlere uymalıdır.
• Sistemde izin verilmeyen uygulamalar konusunda bilgi sahibi olmalıdır.
• Güvenlik ihlali ile ilgili bir sorun olduğunu/olabileceğini düşündüğünde, yardım için başvuracağı kişiyi bilmeli ve haber vermelidir.

Sonuç olarak; kurumunun bilgi güvenliği yaklaşımı çalışanın davranışına odaklanmalıdır çünkü kurumun başarısı büyük oranda çalışanlarının gerçekleştirdiği ya da gerçekleştiremediği unsurlara bağlıdır (**Tablo 1**). Bilgi güvenliği farkındalığı kültürü, bilgi varlıkları üzerindeki riskleri minimum seviyeye indirecek ve özellikle bir çalışanın hatalı davranış riskini ve bilgi varlıklarına zarar verici etkileşimini azaltacaktır. Bilgi güvenliği sadece basit bir teknik ya da yasal bir konu değildir. Bu yönergelere uygunluk büyük oranda sahip oldukları verilerin değerini anlayan sağlık çalışanlarına bağlıdır.

Kaynaklar

1. T.C. Sağlık Bakanlığı. Türkiye Sağlıkta Dönüşüm Programı. Ankara: Sağlık Bakanlığı; 2008.
2. Borzekowski R. Measuring the cost impact of hospital information systems: 1987-1994. J Health Econ 2009;28:938–49.
3. Blazona B, Koncar M. HL7 and DICOM based integration of radiology departments with healthcare enterprise information systems. Int J Med Inform 2007;76: 425–32.
4. Singh D, Spiers S, Beasley BW. Characteristics of CPOE systems and obstacles to implementation that physicians believe will affect adoption. South Med J 2011; 104:418–21.
5. Shortliffe EH, Cimino JJ. Biomedical informatics. Computer applications in health care and biomedicine. New York: Springer; 2006;475–511.
6. Jaana M, Ward MM, Paré G, Wakefield DS. Clinical information technology in hospitals: a comparison between the state of Iowa and two provinces in Canada. Int J Med Inform 2005;74:719–31.
7. Karahoca A, Bayraktar E, Tatoglu E, Karahoca D. Information system design for a hospital emergency department: a usability analysis of software prototypes. J Biom Inform 2010;43:224–32.
8. Robertson M, Callen J. The educational needs of health information managers in an electronic environment: what information technology and health informatics skills and knowledge are required? HIM J 2004;32:95–101.
9. Dodge CR, Carver C, Ferguson JA. Phishing for user security awareness. Computer and Security 2007;26:73.
10. Canberk G, Sarıoğlu Ş. Bilgi güvenliği ve süreçleri üzerine bir inceleme. Politeknik Dergisi 2006;3:165–74.
11. International Medical Informatics Association. Working Group 1: Health and medical informatics education. recommendations of the International Medical Informatics Association (IMIA) on education in health and medical informatics. Methods Inf Med 2000;39:267–77.
12. Aslandağ K. Bilgi güvenliği kavramı ve bilgi güvenliği yönetim sistemleri ile şirket performans ilişkisine dair bir uygulama. Kocaeli, Gebze Yüksek Teknoloji Enstitüsü Sosyal Bilimler Enstitüsü, Kocaeli, Yüksek Lisans Tezi, 2010; s. 18–19.
13. Whitman ME, Mattord HJ. Principles of information security. [Internet] Available from: http: http://www.cengagebrain.com/content/whitman38214_1111138214_01.01_toc.pdf [2015 March 15].
14. Hirakis O, Karakounos S. Goals and benefits of knowledge management in healthcare. In: Murray EJ, editor. Knowledge management: concepts, methodologies, tools, and applications. New York: Information Science Reference, 2008:2232–9.
15. Tengilimoglu D, Çelik Y, Ulgu M. Comparison of computing capability and information system abilities of state hospitals owned by Ministry of Labor and Social Security and Ministry of Health. J Med Syst 2006;30:269–75.
16. Kılıç Aksu P. Hastane bilgi yönetim sisteminin çalışanlar tarafından değerlendirilmesi. Marmara Üniversitesi Sağlık Bilimleri Enstitüsü, İstanbul, Doktora Tezi, 2014.
17. Mumcu G. Elektronik sağlık kayıt sistemi: sağlık hizmetlerinde bilişim teknolojisinin uygulama alanları. İstanbul: Bedray Yayıncılık; 2011;1–13, 61–7.
18. Hamill JT, Deckro RF, Kloeber JM Jr. Evaluating information assurence strategies. Decision Support Systems 2005;39:463–84.
19. Turkish Ministry of Health (TMH). Statistical yearbook of health care institutions in 2006. Ankara: TMH; 2006.
20. Whitman M, Mattord H. Principles of information securitiy. 1st ed. Boston: Thomson Learning Course Technology; 2003.
21. Küzeci E. Kişisel verilerin korunması. Ankara: Turhan Kitabevi; 2010.
22. http://www.qub.ac.uk/methics/HarperMcClelland.pdf (Erişim Mart 2015).