Sağlık Kuruluşlarındaki Bilgi Güvenliği Yönetim Sistemlerinin ISO/IEC 27001 Standardına Göre Değerlendirilmesi

Mehrdad Alizadeh MIZANI[a], Sait Can YÜCEBAŞ[a], Melahat Oya ÇINAR[a]

[a] *Tıp Bilişimi AD, Orta Doğu Teknik Üniversitesi, Ankara*

Evaluation of Information Security Management Systems in Healthcare Institutions According to ISO/IEC 27001 Standard

Özet

Sağlık alanındaki teknolojik gelişmelerin büyük ölçüde bilgiye bağımlı olması; muazzam miktarda kişisel sağlık bilgisinin elde edilmesi, saklanması ve işlenmesi gerekliliğini doğurmuştur. Hastalara güvenli ve kaliteli sağlık hizmetlerinin verilebilmesi, saklanan bilgilerin doğruluğu ve erişebilirliğine bağlıdır. Bununla birlikte sağlık bilgisi yüksek derecede kişisel ve gizli bir bilgidir, bu nedenle de hasta haklarının ve mahremiyetinin sağlanması için mutlaka korunmalıdır. Sonuç olarak sağlık bilgi sistemleri kabul edilebilir seviyede bütünlük, gizlilik ve kullanılabilirlik sağlayabilmek için sakladığı bilgileri kasıtlı veya kazara olan erişimlere, silmelere ve bozulmalara karşı korumalıdır. Sağlık bilgisini güvence altında tutmak doğru, tam, etkili, zamanında ve yüksek kalitede sağlık hizmeti sağlamakla eş değerdir. Bu sayede sağlık kuruluşları, hastalarına kaliteli hizmet sunarken, onların kişisel gizlilik haklarını da güvence altına almış olurlar. Sadece teknik güvenlik tedbirlerini uygulamak bilgiyi korumak için yeterli değildir. Güvenlik; organizasyonel politikalar, prosedürler, eğitim ve yönerge gibi bileşenleri olan bir süreçtir. Teknolojik önlemlerin ekili olarak çalışabilmesi ve teknoloji ile sağlanamayacak önlemlerin alınabilmesi için yönetim kademesinin de devreye girmesi gerekmektedir. Kısaca bilgi sistemlerini iç ve dış tehditlere, doğal felaketlere ve teknoloji kaynaklı arızalara karşı koruyabilmek için bir Bilgi Güvenliği Yönetim Sistemi'nin (BGYS) oluşturulması gerekmektedir.

Sağlık kuruluşları teknik ve prosedürel tedbirleri uygulasalar da uygulanan güvenlik tedbirlerinin etkiliğini sınayan genel bir standarda karşı değerlendirilmemişlerdir.

Bu çalışmada üç farklı sağlık kuruluşunun BGYS uygulamaları, uluslararası ISO/IEC 27001 standardına göre değerlendirilmiştir.

Anahtar Kelimeler

Bilgi; Bilgi güvenliği; Hasta hakları; Hasta bilgi güvenliği; Bilgi güvenliği yönetim sistemleri; Güvenlik standartları