Kişisel Sağlık Bilgilerinin Güvenliği Açısından Medula'da Kullanılan Yasa ve Standartların HIPAA ile Karşılaştırılması

Öznur Esra PAR[a], Ergin SOYSAL[a]

[a] *Sağlık Bilişimi ABD, Hacettepe Üniversitesi, Ankara*

Comparison of Standards and Acts Used in Medula with HIPAA In Terms Of Security Of Personal Health Records

Abstract: *Circulation of personal health records in digital media has increased by intensive usage of technology on health sector. Circulation of personal health records in electronic media brings with security and privacy issues. Medula was analysed in terms of security of personal health records. Medula is an online system that declares transactions to SGK electronically (Health Safety Agency)relevant with pricing and performing of health services, medical supplies and drugs in health facilities. Standarts and acts used on Medula were compared with HIPAA(Health Insurance Portability and Accountability Act) applied in USA. HIPAA is a regulations set that includes administrative, physical and technical reserves in terms of security of personal health records.*
Digitization of personal health records also brings with security risks. A number of technical and legal infrastructure is needed to eliminate these risks.

Key Words: Medula; HIPAA; Security of Personal Health Records; ISO 20000; ISO 27000

Özet: *Sağlık alanında artan teknoloji kullanımı ile birlikte kişisel sağlık bilgilerinin elektronik ortamda dolaşımı artmış ve olası güvenlik ve mahremiyet sorunlarına zemin hazırlamıştır. Sağlık kuruluşlarında verilen sağlık hizmetlerinin, kullanılan tıbbi malzeme ve ilaçların ücretlendirme ve gerçekleştirme işlemlerinin elektronik ortamda Sağlık Güvenlik Kurumu'na bildirilmesini sağlayan çevrimiçi bir sistem olan MEDULA'nın kişisel sağlık bilgilerinin güvenliğine yönelik olarak uyguladığı kurallar incelenmiş, ilgili literatür taraması yapılmıştır. Medula; sağlık kuruluşlarında verilen sağlık hizmetlerinin, kullanılan tıbbi malzeme ve ilaçların ücretlendirme ve gerçekleştirme işlemlerinin elektronik ortamda Sağlık Güvenlik Kurumu'na bildirilmesini sağlayan çevrimiçi bir sistemdir. Medula'da kullanılan standartlar ve bağlayıcı yaptırımlar Amerika Birleşik Devletleri'nde uygulanan HIPAA (Health Insurance Portability and Accountability Act) , Sağlık Sigortası Taşınabilirliği ve Sorumluluğu yasası ile karşılaştırılmıştır. HIPAA yasası; kişisel sağlık bilgilerinin gizliliğine yönelik idari, fiziki ve teknik ihtiyatları ve yaptırımları içeren düzenlemeler bütünüdür.*
Kişisel sağlık bilgilerinin sayısallaştırılması güvenlik risklerini de beraberinde getirmektedir. Söz konusu riskleri ortadan kaldırmak için bir takım teknik ve yasal altyapılara ihtiyaç duyulmaktadır.

Anahtar Kelimeler: Medula; HIPAA; Kişisel Sağlık Bilgilerinin Güvenliği; ISO 20000; ISO 27000

Giriş

Sağlık sektöründe güncel teknolojinin hissedilir şekilde kullanılmasıyla birlikte teknolojinin taşıdığı bazı risklerle de yüz yüze gelinmiştir. Elektronik ortamdaki tüm veriler gibi, kişisel sağlık bilgilerini tehdit eden riskler için güvenlik önlemlerinin alınması zorunlu hale gelmiştir.
Kişsel sağlık bilgileri, kişinin doğum öncesinden ölüm sonrasına kadar geçen süreyi kapsayan sağlık bilgilerinin tümüdür. Sağlık kayıtlarının sayısallaştırılması etkin sağlık hizmeti için yadsınamayan ciddi bir hamledir. Güncel teknolojilerin kişisel sağlık bilgilerinin gizlilik , bütünlük ve erişilebilirlik risklerini artırmasından dolayı sağlık bilgilerinin güvenliği zedelenmektedir. Kişisel sağlık bilgilerinin mahremiyeti esastır . Bu nedenle önlemlerin alınması, risklerin saptanıp indirgenmesi zorunlu hale gelmiştir.
Teknolojinin ülkemiz sağlık alanındaki ilk etkilerinden biri, sağlık sisteminde, geri ödemeleri hızlandırmak ve düzenlemek için Sosyal Güvenlik Kurumu (SGK) tarafından 2006 yılında kullanılmaya başlayan MEDULA (MEDikal Ulak) sistemidir. Medula; sağlık hizmetlerine ilişikin bilgilerin elektronik ortamda SGK ile hastaneler arasında transferinin sağlandığı, fatura bilgilerinin toplandığı ve geri ödemelerin yapıldığı bütünleşik bir sistemdir.[1]

HIPAA(Health Insurance Portability and Accountability Act) , Sağlık Sigortası Taşınabilirliği ve Sorumluluğu Talimatı; kişisel sağlık bilgilerinin güvenliğini sağlamak için sağlık çalışanları ve diğer kuruluşlarca sağlık bilgilerine hangi koşullarda ulaşılabileceğine dair kurallar getirmektedir. ABD'de 1996 yılından beri yürürlükte olan HIPAA, sağlık kayıtlarına erişimi kısıtlayan prosedür ve protokolleri içeren, kişisel sağlık billgilerinin izinsiz kullanımı ve ifşa edilmesinde gerekli yaptırımları (para ve hapis cezası gibi) kapsayan, kişisel sağlık bilgilerinin güvenliğini artıcı bir takım idari, fiziksel ve teknik standartları içeren düzenlemeler içermektedir.

Gereç ve Yöntem

Kişisel sağlık bilgilerinin güvenliği açısından Medula'nın teknik altyapı standartları ve yasal dayanakları ABD'de bu amaçla düzenlenen HIPAA yasası ile karşılaştırılmıştır. Bu çalışmada Medula sistemi incelenerek ilgili mevzuat araştırılmış ve literatür taraması yapılmıştır.

Bulgular

Kişisel sağlık kayıtlarının güvenliğine yönelik olarak Medula'da kullanılan ISO 20000, ISO 27001 standartları, ilgili yasalar ve Amerika Birleşik Devleti'nde uygulanan HIPAA yasası karşılaştırılmış, elde edilen bulgular Tablo – 1'de özetlenmiştir.

HIPAA Yasası

Amerika Birleşik Devletleri'nde sağlık sektöründeki bilgi ve bilgi akışının güvenliğini oluşturmak ve devamlılığını sağlamak için 21 Ağustos 1996 tarihinde HIPAA yasası uygulanmaya başlanmıştır.[2]
HIPAA güvenlik kurallarına göre kişisel sağlık bilgilerinin gizliliği, bütünlüğü ve erişilebilirliği garanti edilmelidir. Kişisel sağlık bilgilerinin bütünlüğünü tehdit edici ve/veya gizliliğini, mahremiyetini tehlikeye sokacak her türlü izinsiz erişime karşı önlemler alınmalıdır. Kişisel sağlık bilgilerinin gizliliğini standardize etmek, güvenliliğini sağlamak ve devam ettirmek için HIPAA kapsamında geliştirilen standartlar ve özellikleri aşağıdaki gibidir. [3]

1) Güvenlik Standartları : Uyulması gereken genel şartları içerir; yaklaşımın esnekliğini kurar; standartları ve uygulama özelliklerini tanımlar; kişisel sağlık bilgilerinin makul ve uygun korunmasının devamı için gerekli olan güvenlik bakımlarını belirler.

2) Yönetimsel Önlemler : Örtülü sağlık kuruluşlarının (sağlık planları, sağlık takas büroları, sağlık sektöründe faaliyet gösteren kuruluşlar) denetimi; erişilebilirliğinin sınıflandırılması; tüzükler; seçme, geliştirme, uygulama prosedürlerinin yönetimi; kişisel sağlık bilgilerinin korunması için gerekli güvenlik tedbirlerinin bakımı ve güvenliği sağlamak için gerekli iş gücünün yönetimini içerir.

3) Fiziksel Önlemler: Fiziksel tedbirleri, doğal ve çevresel tehlikelerde ve/veya yetkisiz erişimlerde ilgili yapı ve araçların korunması ve denetlenmesi için gerekli prosedürleri tanımlar.

4) Teknik Önlemler: Kişisel sağlık bilgilerinin korunması ve erişimi ile ilgili prosedürleri, teknolojileri, tüzükleri, risk analizlerini ve risk yönetimlerini içerir.

5) Organizasyonel Gereksinimler: İş ortaklığı sözleşmeleri, üçüncü parti organizasyonların belirlenmiş standartlara uyacağına dair yapılan anlaşmaları ve diğer düzenlemeleri içerir.

6) Tüzükler, Prosedürler ve Dokümantasyon Gereksinimleri : Uygulama özellikleri ve güvenlik kurallarının diğer gereksinim standartları ile çelişmeyen makul,uygun tüzüklü prosedürler olması beklenir.

Medula'nın Teknik Altyapı Standartları ve Yasal Dayanağı

Medula, sağlık harcamalarının geri ödemesini elektronik ortamda düzenlemeyi amaçlayan bir sistemdir. Medula, 5510 Sayılı Sosyal Sigortalar ve Genel Sağlık Sigortası Kanununun 78 inci maddesinin birinci fıkrası, 100 üncü maddesinin ikinci

fıkrasınca 1/9/2006 tarihinde Sağlık Bakanlığı'na bağlı hastanelerde uygulanmaya başlanmıştır. Daha sonra sistem özel ve üniversite hastanelerinde uygulamaya alınmıştır. Sistem hakkındaki tebliğ ise 07/12/2006 tarihinde resmi gazetede yayınlanmıştır.[1] 01/09/2007 tarihinden itibaren tüm faturalandırma işlemleri Medula üzerinden yapılmaktadır. 12 /12/2006 tarihinde ikinci verisyonu (Medula V2), 01/04/2009 tarihinde üçüncü versiyonu (Medula V3) yayınlanmıştır.

Medula'da hizmetlerin ISO 20000 Bilgi Teknolojileri Servis Yönetimi standartına uygun olarak verilmesi hedeflenmektedir. [4]
2005 yılında bilgi teknolojileri yönetim servisi için geliştirilen ilk standarttır, 2011 yılında revize edilmiştir. BS 15000 standartını temel alan ISO 20000 standartı iki bölümden oluşur.[5]

1. Bölüm: Bilgi teknolojileri hizmet yönetimini kapsar. Bilişim operasyonlarının nasıl yönetilimesini gerektiğini standardize eder ve sunulan hizmetin belirli bir kalite seviyesinde olması için gerekli şartları içerir.

2. Bölüm : Hizmet yönetim uygulamalarının açıklandığı kılavuz standarttır.

ISO 20000 gereksinim analizleri, hizmet sisteminin belirlenmesini ve hizmet sürekliliği, erişilebilirlik, finans, kapasite, iş ilişkileri, bilgi güvenliği, sistem yönetim süreci gibi birbiri ile ilişkili birçok bütünleşik süreci kapsar.
ISO 20000 bilgi güvenliğinde yeterli ve orantılı güvenlik denetimlerinin seçilmesine yol gösteren ISO 27000 Bilgi Güvenliği Yönetim Sistemi'ni referans alır.
Bilgi güvenliğinin temel ilklerini oluşturan gizlilik, bütünlük ve erişebilirlik kavramlarının sağlanması ve devam ettirilmesi için geliştirilmiş bir standarttır. Kritik güvenlik risklerinin belirlenip minimize edilmesine yardımcı olur.
Bilgi güvenliğinde olası ve mevcut risklerin saptanmasına ve indirgenmesine yardımıc ı olan ISO 27001 standartı, Bilgi Güvenliği Yönetim Sistemi standartı olan ISO 27000 standart ailesinin ana standartıdır.
ISO 27001 Bilgi Güvenliği Yönetim Sistemi risklerin belirlenmesi, değerlendirilmesi; güvenlik politikalarının oluşturulması; fiziksel, çevresel ve iş gücü güvenliği; erişim güvenliği; bilgi güvenliği yönetimi gibi bilgi güvenliliğin oluşturulması ve devamlılığı için gerekli aşamaları kapsar ve bu aşamaları standardize eder.[6]
Sağlık sektöründe ise kişisel sağlık bilgilerinin gizlik, bütünlük ve erişilebiliriliğinin korunması ve devamına yönelik olarak ISO 27000 ailesinin alt standartı olan ISO 27799 Sağlık Kurumlarında Bilgi Güvenliği Yönetim Sistemi uygulanır. ISO 27001 Bilgi Güvenliği Yönetim Sistemi'nin kapsamı dışında sağlık kurumlarında bilgi güvenliğini, korunması gereken sağlık bilgilerini, sağlık sektörüne yönelik riskleri de içerir.
Hastaların özel hayatı, mahremiyet hakkı Hasta Hakları Yönetmeliği'nde, Türk Ceza Kanunu'nda ve şuan kanun tasarısı halinde olan "Kişisel Verilerin Korunması" yasasında özel hükümlerce koruma altına alınmıştır ve ilgili yasalarca kişisel sağlık bilgilerinin izinsiz kullanımı ve/veya ifşası durumunda yaptırımları belirlenmiştir. Bu yaptırımlar :

- 5237 sayılı Türk Ceza Kanunu'nun 2 nci kitabının 134 üncü madde ile "Özel hayatın gizliliğini ihlal" suç kabul edilerek müeyyideye bağlanmıştır.[7]
- Hasta Hakları Yönetmeliğinin 16 ncı maddesine göre kişisel sağlık verileri, sadece hastanın tedavisi ile doğrudan ilgili olanlar tarafından bilinebilecektir.

- Türk Ceza Kanunu Madde 136- (1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.
- Hasta Hakları Yönetmeliği Madde 23-Sağlık hizmetinin verilmesi sebebiyle edinilen bilgiler, kanun ile müsaade edilen haller dışında, hiçbir şekilde açıklanamaz.[8]
- Türk Medeni Kanunu Madde 24- Hukuka aykırı olarak kişilik hakkına saldırılan kimse, hâkimden, saldırıda bulunanlara karşı korunmasını isteyebilir. Kişilik hakkı zedelenen kimsenin rızası, daha üstün nitelikte özel veya kamusal yarar ya da kanunun verdiği yetkinin kullanılması sebeplerinden biriyle haklı kılınmadıkça, kişilik haklarına yapılan her saldırı hukuka aykırıdır.

Tablo 1 – Medula'nın Teknik altyapı standartları ve yasal dayanağının HIPAA Yasası ile karşılaştırılması

	Standartlar ve Yasalar			
Özellikler	**HIPAA**	**ISO 20000**	**ISO 27000**	**Kanun ve Yasalar**
Uluslararası Geçerlilik	-	+	+	-
Genel Sistem Gereksinimlerinin Belirlenmesi, Tüzükler, Anlaşmalar	+	+	-	-
Bilgi Güvenliği Sağlanması	+	-	+	-
Kişisel Bilgilerin Korunması ile İlgili Yaptırımlar	+	-	-	+
Bilgi Güvenliği Risk Analizi	+	-	+	-
Bilgi Güveliği için Gerekli Fiziksel ve Teknik İhtiyatlar	+	-	+	-
İnsan Kaynakları Güvenliği	+	-	+	-

Medula'da kullanılan teknik alt yapının yasal dayanağının olmadığı gözlemlenmiştir. Kişisel sağlık bilgilerinin güvenliğine yönelik olarak teknik alt yapıların yasal dayanağı oluşturulabilir ayrıca ilgili yasalar ivedilikle yürülüğe girmelidir.

Tartışma

Bilgi teknolojilerin hızlı bir şekilde yaygınlaşmasıyla bilgi teknolojilerini kullanarak yapılan elektronik saldırılar da artmaktadır [3].Kişisel sağlık bilgileri açısından bu saldırılar kişisel bilgilerin izinsiz ele geçirilmesi ve değiştirilmesi olarak özelleştirilebilir. Kişisel sağlık bilgilerinin mahremiyeti esastır fakat kişisel sağlık bilgileri farklı, ayrık

sistemlerden gelen sağlık bilgilerini içerdiğinden ve yapısında farklı roller ve kurumlar olduğundan, Medula'da uygulanan bilgi ve güvenlik teknolojilerinin yeterli olmadığı durumlar ortaya çıkmaktadır. HIPAA; kişisel sağlık bilgilerinin gizlilik, bütünlük ve erişilebilirliğini sağlayan bütünleşik bir yasadır. Ülkemizde sağlık bilgi teknolojileri uygulamalarında ISO 20000, ISO 27001 ile bilgi güvenliği sağlanmaya çalışılmakta ve yaptırımlar için ise ilgili kanunlara ve yönetmeliklere başvurulmaktadır. Sistem gereksinimleri HIPAA'da yasal dayanaklarla analiz edilmesi gerekirken, Medula'da ISO 20000 standartının kriterlerine göre analiz edilmektedir. Kişisel sağlık bilgilerinin güvenliğine yönelik risk analizlerinin yapılması, fiziksel ve teknik ihtiyatların belirlenmesi, insan kaynaklarının güvenliğinin sağlanmasına yönelik teknik altyapı standartlarının yasal çerçevesi çizilmiş olmasına rağmen ISO 27000 Bilgi Güvenliği Yönetim Sistemi standartına göre bilgilerin güvenliğine yönelik teknik altyapının herhangi bir yasal dayanağı yoktur. HIPAA'da kişisel sağlık bilgilerinin izinsiz kullanımı ve/veya ifşasında uygulanacak olan yasal yaptırımlar tanımlanmış olmasına rağmen, kişisel bilgilerin güvenliğine yönelik yaptırımlar ilgili yasa ve yönetmeliklerle tanımlanmaktadır. HIPAA yasaları ISO standartları gibi uluslararası bir standart formu haline getirilebilir, yaptırımlar her ülkeninin hukuk sistemine göre uyarlanabilir. HIPAA gibi tümleşik yasaların oluşturulması elektronik sağlık kayıtlarının güvenliğini en üst düzeyde sağlayacaktır.

Medula'da kullanılan teknik alt yapının yasal dayanağının olmadığı gözlemlenmiştir. Kişisel sağlık bilgilerinin güvenliğine yönelik olarak teknik alt yapıların yasal dayanağı oluşturulabilir ve ayrıca ilgili yasalar ivedilikle yürülüğe girmelidir.

Kaynakça

[1] Genel Sağlık Sigortası Kapsamında Uygulanan "MEDULA" Sistemi Hakkında Tebliğ (Seri No: 1), 26369 sayılı Resmi Gazete, 7 Aralık 2006.

[2] Prajesh Chhanabhai, Alec Holt, Inga Huntur, "Consumers, Security and Electronic Health Records", New Zelland, 2006.

[3] National Institiue of Standarts and Technology, "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountabilit Act (HIPAA) Security Rule", USA, 2008

[4] Sosyal Güvenlik Kurumu, Medula Servisleri Kullanım Kılavuzu, 2006.

[5] ISO/IEC 20000 Certification and Implementation Guide, Claire Engle,Gerard Blokdijk,Jackie Brewster, Emereo Publishing, Australia, 2008.

[6] Information Security Based on ISO 27001/ISO 27002: A Management Guide, Alan Calder, Van Haren Puplishing, NL, 2006.

[7] Türk Ceza Kanunu , 25611 sayılı Resmi Gazete, 12 Ekim 2004.

[8] Hasta Hakları Yönetmeliği, 23420 sayılı Resmi Gazete, 1 Ağustos 1998.

Sorumlu Yazarın Adresi

Öznur Esra Par
Hacettepe Üniversitesi
Bilişim Enstitusu
par@hacettepe.edu.tr