Gönderim Tarihi: 03.06.2018 Kabul Tarihi: 29.08.2018

MOBİL SAĞLIK UYGULAMALARININ GÜVENLİĞİNE İLİŞKİN HABERLER ARACILIĞIYLA YAŞANAN ETİK SORUNLARIN DEĞERLENDİRİLMESİ

Erdal EKE*
Rukiye ÇELİK**
Burhan ÇETİN***

EVALUATION OF THE SECURITY OF MOBILE HEALTH APPLICATIONS ETHIC PROBLEMS WITH NEWS

Öz

Mobil sağlık uygulamaları, ihtiyaç duyulan bilgiye erişimi kolaylaştıran ve söz konusu verilerin kayıt altına alınmasına imkân veren, hasta izleme cihazları, mobil telefonlar ve daha kompleks cihazları içeren sağlık uygulamalarıdır. Çalışmanın amacı, henüz yeni olan mobil sağlık uygulamalarının yol açtığı etik sorunları tespit etmek ve bu noktada öneriler geliştirebilmektir. Çalışmanın problemi ise verilerin toplanması ve ilgililere iletilmesinde mahrem bilgilerin hastaların rıza göstermeyeceği şekilde depolanıp erişime açık hale getirilerek etik sorunların ortaya çıkmasıdır. Çalışmada nitel bir yöntem olan doküman incelemesi kapsamında pasif analiz de denilen ikincil veri araştırması yapılmış ve veri toplama aracı olarak internet haberleri ele alınmıştır. Çalışma kapsamında incelenen haber metinlerinde 4 ana tema tespit edilmiş ve mahremiyet anlamında zayıf olan mobil sağlık uygulamalarının birçok etik soruna yol açabileceği anlaşılmıştır. Çalışma sonunda hastadan alınan tıbbi bilgilerin hasta mahremiyetini ihlal edecek şekilde kullanıma açık olduğu ve kullanılan sistemlerin bu bilgileri korumada yetersiz kaldığı, dijital ortamların veri saklamada yetersiz olduğu, mobil cihazların saldırılara açık olduğu gibi bulgulara ulaşılmıştır.

Anahtar Kelimeler: Sağlık Politikaları, Mobil Sağlık Uygulamaları, Etik, Sağlık Reformu, Sağlık Sistemi.

* Dr. Öğr. Üyesi, Süleyman Demirel Üniversitesi, İİBF, Sağlık Yönetimi Bölümü, e-posta: erdaleke@sdu.edu.tr.

** Dr. Öğr. Üyesi, Süleyman Demirel Üniversitesi, İletişim Fakültesi, Halkla İlişkiler ve Tanıtım Bölümü, e-posta: rukiyecelik@sdu.edu.tr.

*** Yüksek Lisans Öğrencisi, Süleyman Demirel Üniversitesi, Sosyal Bilimler Enstitüsü, Sağlık Yönetimi Anabilim Dalı, e-posta: yl1630232105@stud.sdu.edu.tr.

Abstract

Mobile health applications are that include patient monitoring devices, mobile phones, and more complex devices that facilitate access to the information needed and enable the recording of such data. The aim of the study is to identify the ethical problems caused by new mobile health applications and to develop suggestions at this point. The problem of study is that when data are collected and transmitted to the interested parties, ethical problems arise due to the fact that confidential information is stored and accessed in a way that patients can not consent to. Within the scope of the study, a secondary data search called passive analysis was conducted a qualitative document analysis, and internet news was taken as a data collection tool. Four main themes have been identified in the news texts examined within the scope of the study and it has been understood that mobile health applications which are weak in terms of privacy may lead to many ethical problems. At the end of the study, medical information received from the patient was found to be in violation of patient privacy, and that the systems used were inadequate to protect the information, digital media was insufficient to store data, and mobile devices were vulnerable to attack.

Keywords (MeSH): Health Politics, Mobil Health Applications, Ethic, Health Reform, Health System.

1. Giriş

Son yıllardaki teknolojik dönüşüm süreci, hiç kuşkusuz dünyadaki bütün hizmet alanlarını doğrudan etkilemiş ve bu alanlarda dönüşüm sürecini beraberinde getirmiştir. Bu süreç hem hizmet sunumu sorumluluğunu üstlenen organizasyonların hem de hizmet alan bireylerin bir anlamda işlerini kolaylaştırmıştır. Özellikle dijital teknolojilerdeki baş döndürücü gelişme, devlet ve özel sektör hizmet organizasyonlarının hizmet sunumunda yeni politikaları, model ve uygulamaları gün yüzüne çıkarmıştır. Bu uygulama alanlarından birisi, sağlık sektörüdür. Sağlık sektöründe son yıllarda mobil sağlık uygulamaları ve bu uygulamalara yönelik dijital dünyanın temel sorunlarından birisi olan güvenlik ve etik konuları öne çıkmıştır.

Mobil sağlık uygulamaları, 2000'li yıllarla birlikte sağlık hizmetleri sektöründe önemli bir konu ve endüstri olarak görülmektedir (Kumar vd. 2013: 228). E-sağlığın bir boyutu olarak kabul edilen mobil sağlık hem küresel hem de ulusal olmak üzere çeşitli kurum ve kuruluşlar tarafından tanımlanmıştır (Demir ve Arslan 2017; Vélez vd. 2014; Varshney 2014). Dünya Sağlık Örgütü'ne göre mobil sağlık, akıllı telefon, hasta izleme cihazları, dijital cihazlar (tablet vb.), diğer kablosuz araçlar ve mobil cihazlar kullanılarak, tıbbi ve halk sağlığı hizmetlerinin desteklenmesi olarak ele alınmaktadır (WHO 2011: 6). Bir başka tanıma göre mobil sağlık, kısaca sağlık sektöründeki hizmetlerin mobil iletişim cihazları

kullanılarak sunulması olarak değerlendirilmektedir. Daha genel bir anlatımla mobil sağlık, kişisel sağlık bilgilerinin cep telefonu, tablet bilgisayar ve kablosuz iletişim altyapısı gibi mobil iletişim ve multimedya teknolojileri vasıtasıyla aktarıldığı, yapılandırıldığı ve farklı kullanıcılar arasında bağlantı sağlandığı bir ortamı betimlemektedir (Tezcan 2016: 33). Sağlık hizmet sektöründe hastalık sürecinde hastalar tarafından kullanılan cep telefonu aracılığıyla bilgi alışverişinde bulunulması, dijital sağlık uygulamaları ile hastalık sürecinde tanı ve tedavi sunulması, online platformlarda sağlık testleri gerçekleştirilmesi ve bilgisayarlar vasıtasıyla hastalıkların tedavisi için oyun ve uygulamalar geliştirilmesi gibi uygulamalar, mobil sağlık kapsamında değerlendirilmektedir (Kılıç 2017: 206). Özetle mobil sağlık uygulamaları biyolojik, davranışsal veya çevresel bilgilerin toplanması açısından teknoloji odaklı yeni yöntemleri ve bu yöntemler doğrultusundaki işlem süreçlerinin sonuçlarını destekleyen bir kapsama sahiptir (Kumar vd. 2013: 229).

Mobil uygulamaların sahip olduğu özellikler, bu teknolojilerin sağlık sektöründe kullanımına ciddi bir oranda olanak sağlamaktadır. Bu doğrultuda sağlık hizmet sektöründe önemli bir konu haline gelen mobil sağlık uygulamalarının sağlayabileceği çok sayıda imkân bulunmaktadır. Bunlardan bazıları şöyle sıralanabilir (Greenspun ve Coughlin 2012: 8):

a) Süreç içerisinde sağlık düzeyi ile ilgili gerçek zamanlı bilgileri ve mesajları paylaşan bir iletişim aracı şeklinde kullanılabilmesi,

b) Hastaların durumlarını takip eden ve raporlayan bir mekanizmaya olanak tanıması,

c) Hasta ve sağlık profesyonelleri arasında video konferans gibi yöntemlerle karşılıklı etkileşime fırsat sunması,

d) Bireylerin sağlık kurumları dışındaki yaşamlarında egzersiz, ilaç ve diğer konularda hatırlatıcı ve motive edici bir arkadaş niteliğine sahip olması ve de

e) Genel olarak sağlık hizmetlerinde bakım sürecini doğrudan hastanın bulunduğu ortama taşıyabilen bir uzaktan izleme mekanizmasını sağlaması.

Mobil sağlık uygulamalarının özellikleri itibariyle her geçen gün daha fazla kullanım alanına sahip olduğu söylenilebilir. Konuyla ilgili veriler incelendiğinde mobil teknoloji kullanımının, dolayısıyla sağlık alanındaki dijital uygulamaların da arttığı görülmektedir (Research 2 Guide 2017). Yeni iletişim teknolojilerindeki gelişmeler ve kullanan sayısındaki artış, sağlık hizmeti sunumunda mobil sağlık uygulamalarının yaygınlaşmasını, sonuç olarak teknoloji ve insan odaklı çeşitli etik sorunları ve riskleri

ortaya çıkarmaktadır (Labrique vd. 2013; Brüggemann vd. 2016). Teknoloji odaklı riskler bağlamında siber saldırılar, verilerin depolanması ve korunması açısından güvenlik, şifreleme sistemlerinin yetersiz kalabilmesi gibi riskler öne çıkmaktadır. Mobil sağlık uygulamalarını kullanan bireylerin şifre mahremiyetine özen göstermemeleri, yetkisiz bireylerle şifre paylaşımı, yetkili personelin kişisel verileri ticari bir kaygı ile başkalarıyla paylaşmaları gibi durumlar, insan odaklı risklere örnek gösterilebilir(Arslan ve Demir 2017: 23-24). Bu ve buna benzer riskler çerçevesinde mobil sağlık uygulamalarında etik konusu, hasta mahremiyeti bağlamında çok ciddi öneme sahiptir.

Hizmet sunum sürecinde bireyler tarafından izlenmesi gereken ahlaki standartlar ve kurallar şeklinde ifade edilebilen etik kavramı (Kırılmaz ve Kırılmaz 2014: 41), sağlık hizmet sektöründe geçmişten günümüze üzerinde çalışmalar yapılan konular arasında yer almıştır. Son yıllarda teknoloji kökenli sağlık hizmetlerinin sektörde daha çok kullanım alanı bulması ile hasta bilgilerinin rızası olmadan mahremiyet ve güvenlik ilkeleri çiğnenerek herhangi bir şekilde üçüncü taraflarla paylaşılması, mobil sağlık uygulamaları kapsamında önemli bir tehdit olarak karşımıza çıkmıştır. Bilindiği üzere kişisel sağlık verilerinin doğası gereği bu konuda güvenlik, gizlilik ve etik kavramları sıklıkla vurgulanmaktadır (Ay 2008). Bu bilgilerin hasta ve hekim ilişkisi dışında yer alan üçüncü kişilerce öğrenilmesi, başka kişi ve kuruluşlara aktarılması ve paylaşılması, hatta ticari olarak satılması, mobil sağlık uygulamalarına ilişkin etik açıdan sorunlu bir durumu beraberinde getirmektedir (Kluge 2004). Özellikle kişisel sağlık bilgilerinin bulunduğu veri tabanlarının ve sistemlerinin kötü niyetli yazılımlar tarafından ele geçirilmesi ya da ilgili sağlık kuruluşundaki yetkili ya da yetkisiz herhangi bir personel tarafından üçüncü kişilere yönelik paylaşılması, bu süreçte tehdit teşkil eden olası riskler olarak değerlendirilmektedir. Kişisel verileri isteği dışında paylaşılan bir birey, kötü amaçlı kişi ve kurumların adımları doğrultusunda sosyal ve ekonomik açıdan olumsuz durumlar ve hatta hayati risklerle de karşılaşabilmektedir. Dolayısıyla mobil sağlık uygulamalarının kullanılması ve bu uygulamalardaki kişisel sağlık verilerinin korunması açısından etik sorunların ve bu yöndeki sistemsel ve beşeri kaynaklı olası risklerin ortadan kaldırılması konusu, özel öneme sahip görülmektedir. Bu durum sağlık sektöründe dijital ortamdaki verilerin güvenliği ile ilgili titiz, dikkatli ve sorumlu davranılması zaruriyetini açıkça hissettirmekte diğer bir ifadeyle çeşitli çalışmalarda öngörülen etik kodları daha önemli hale getirmektedir (Albrecht ve Fangerau 2015). Bu doğrultuda mobil sağlık uygulamalarının kullanımı açısından etik sorumluluklar çerçevesinde samimiyet, dürüstlük, kalite, gizlilik, bilgilendirilmiş onay, çevrimiçi sağlık hizmetlerinde

profesyonellik, sorumlu iş ortağı ve hesap verebilirlik gibi bazı rehber ilkelerin öne çıktığı ve sağlık hizmeti sunucuları ile bu süreçte görevli personelden bu ilkelere uygun davranılmasının beklendiği anlaşılmaktadır (Rippen ve Risk 2000: 2-5).

Bu bilgilerden yola çıkarak Türkiye'de de kişisel sağlık verilerinin güvenliğinin sağlanması çerçevesinde çeşitli adımlar atılmıştır. Örneğin 20 Ekim 2016 tarihinde "Kişisel Sağlık Verilerinin İşlenmesi Ve Mahremiyetinin Sağlanması Hakkında Yönetmelik" yayınlanmıştır. Yönetmeliğin amacı, kişisel sağlık verilerinin toplanması, işlenmesi, korunması ve veri mahremiyetinin sağlanmasına yönelik süreçle ilgili usul ve esasların düzenlenmesi şeklinde hüküm altına alınmıştır. Ayrıca kişisel sağlık verilerini işleyen veya görevi gereği kişisel sağlık verilerine erişen herkesin, bu verilerle ilgili olarak sır saklama yükümlülüğü altında olduğu; Sağlık Bakanlığının ülke genelinde hizmet vermek amaçlı kurulan sistemleri dışında kişisel verilerin hiçbir yere kopyalanamayacağı ve kaydedilemeyeceği; sisteme işlenen verilerin mahremiyet çerçevesinde belirtilen kriterler çerçevesinde korunacağı ve gizlilik ihlaline yönelik bildirim durumunda takip edilmesi gereken bir sürecin varlığı gibi hususlar, Yönetmelikte net bir şekilde ifade edilmiştir. Yönetmelikte belirtilen gizlilik ve mahremiyet ilkelerine aykırı davranılması durumunda ise ilgili kişilerin yaptırımla karşılaşacakları ayrıca hüküm altına alınmıştır(Kişisel Sağlık Verilerinin İşlenmesi Ve Mahremiyetinin Sağlanması Hakkında Yönetmelik 2016). Ancak süreç içerisinde Yönetmeliğin iptaline ilişkin dava açılmış ve bu dava sonucunda Danıştay'ın ilgili dairesi tarafından yürütmeyi durdurma kararı verilmiştir. Danıştay'ın bu kararı doğrultusunda ilgili Yönetmelik'te bazı değişiklikler yapılmış ve nihai olarak Kişisel Sağlık Verilerinin İşlenmesi ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik, 24 Kasım 2017 tarihinde 30250 sayılı Resmi Gazete'de yeniden yayımlanmıştır (Nalbantoğlu 2018). Bu çerçevede gerçekleştirilen değişiklikler, bir anlamda bu yönetmeliğin konuya ilişkin mevzuata uyumlu hale getirilmesi ve kişisel verileri koruma hukukunun geliştirilmesi açısından pozitif bir adım olarak değerlendirilmektedir (Dülger 2017).

Özetle her ülkede kullanılmakta olan mobil sağlık sunucusu topladığı ve ilettiği bilginin güvenliği ile ilgili önlemler almak zorundadır. Bu kapsamda günümüzde en geçerli önlem HIPAA (Health Insurance Portability and Accountability Act) kurallarına uyumluluk olarak ifade edilmektedir. Mobil sağlık uygulamalarının kullanımı açısından gömülü şifreleme, oto-kimlik entegrasyonu ve cihaz güvenlik özellikleri, etik ihlallere ilişkin çözümün sadece bir parçası olarak düşünülmektedir.

Ancak yazılımsal ve donanımsal hangi önlem alınırsa alınsın, bilgi güvenliği açısından en önemli unsurun insan olduğu unutulmamalıdır (Tezcan 2016: 72).

Bu çalışmada mobil sağlık uygulamalarının teknolojiden ve insandan kaynaklanabilecek riskler ve bu riskler çerçevesinde oluşabilecek etik problemlere farklı bir bakış açısı ortaya konulmaya çalışılacaktır. Dolayısıyla araştırma sorumuz; "Mobil sağlık uygulamalarının etik problemleri var mıdır ve bunlar nelerdir?" şeklindedir. Buradan hareketle çalışmanın amacı; mobil sağlık uygulamalarının yol açtığı etik sorunların web üzerinde yayınlanan haberler aracılığıyla betimlenmesidir.

2. Metodoloji

Çalışma kapsamında nitel bir yöntem olan doküman incelemesi kapsamında ikincil veri araştırması yapılmıştır. Pasif analiz de denilen ikincil veri araştırmasında veri toplama aracı olarak internet haberleri ele alınmıştır. Google tarama motorunda "mobil sağlıkta etik ihlal, sağlıkta siber saldırı, sağlık verilerinin korunaksızlığı" gibi anahtar kelimeler kullanılarak aranan mobil sağlık ve etik ihlal içerikli metinler aranmış, köşe yazıları ve özel konu sayfaları ayıklanarak yalnızca ilişkili haberler toplanmıştır. Dolayısıyla köşe yazıları ve özel konulu sayfalardan ayıklanarak elde edilen 19 Ağustos 2014-1 Haziran 2017 aralığındaki toplam 58 haber metni tematik analiz ile incelenmiştir. İncelenen haberler; ulusal ve yerel gazetelerin internet sitelerinde ve sağlık içerikli çeşitli sitelerde yer almaktadır.

2.1. Analiz Tekniği

Çalışmada elde edilen tüm haber metinleri tematik analiz ile incelenmiştir. Tematik analiz, nitel veri setinin bölümlendirilip, sınıflandırıldığı, özetlendiği nitel bir yöntemdir. Bu yöntemde çözümlenen veriler yeniden inşa edilerek önemli kavramlar ortaya çıkarılır (Given 2008: 867). Başka bir ifadeyle tematik analiz, veri setinin çalışmanın amacına yönelik olarak yeniden çerçevelendiği ve veri setindeki önemli unsurların öne çıkarıldığı bir inceleme yöntemidir.

Analizin ilk aşamasında metinler arasındaki benzerlikler farklılıklar tespit edilmiştir. Ardından bu benzerlik ve farklılıklara göre temalar ve bu temaları altında toplayabilecek niteliğe sahip şemsiye temalar, başka bir ifadeyle ana temalar oluşturulmuştur.

2.2. Bulgular

İncelenen haberlerde ele alınan konular "Türkiye, İngiltere, İspanya gibi bazı ülkelerin çalınan sağlık kayıtları, çalınan sağlık kayıtlarının yayınlanması, bazı hastanelere yapılan siber saldırılar, kalp pillerinin uzaktan kumanda edilerek hastalara zarar verilmesi tehlikesi, sağlık sigortası şirketlerinin siber saldırıya uğraması, çalınan sağlık kayıtlarının para karşılığında satılması, sağlık verilerinin kredi kartlarından da değerli olduğu, akıllı insülin pompası gibi sağlık cihazlarının korsanlar tarafından ele geçirebileceği, siber saldırıların maliyetleri ve mobil sağlık uygulamalarının saldırılara karşı savunmasız olması"dır. Bu konu başlıkları araştırma amacı doğrultusunda değerlendirildiğinde dört ana tema altında kümelendikleri görülmektedir: "Çalınan ve Yayınlanan Sağlık verileri, Sağlık Kurumlarına Yönelik Siber Saldırı, Mobil Sağlık Cihazları ve İnternet Bağlantılı Medikal Cihazlara Siber Saldırı ve Korumasız Sağlık Verileri"

2.2.1. Çalınan Ve Yayınlanan Sağlık Verileri (19 Ağustos 2014-12 Mayıs 2017)

Bu ana tema altında Türkiye'de bazı hastanelerden hastaların kayıtlarının siber saldırı ile çalındığı tespit edilmiştir. Sağlık Bakanlığının açıklamasına göre Diyarbakır, Siirt, Tekirdağ ve Kocaeli illerinde bulunan bazı hastanelere siber saldırı neticesinde ilgili sağlık verilerinin çalındığı belirtilmiştir (URL1, URL 3). Söz konusu hastanelerin veri yedekleme tedbiri sayesinde hastaların herhangi bir mağduriyet yaşamadığı ifade edilmiştir. Buna karşın çalınan sağlık kayıtlarının akıbeti hakkında herhangi bir bilgiye rastlanmamıştır (URL 4, URL 5).

Başka bir örnekte ise Amerika'da 5,6 milyon kişinin sosyal güvenlik numaraları, isimler, adresler, finansal bilgiler ve sağlık verilerinin çalındığı görülmektedir. Ayrıca yine Amerika'da Kaliforniya Üniversitesi Sağlık Sistemi'nde milyonlarca hastanın kişisel bilgilerinin çalındığı ve çalınan verilerin şifreli olmamasından dolayı dolandırıcılık amaçlı rahatlıkla kullanılabileceği açıklanmıştır. 4,5 milyon hastanın verilerini içeren bu siber saldırı örneğinde hastalara kimlik koruma hizmeti sunulmuştur (URL 6, URL 7, URL 8).

Hollywood'daki Presbyterian Sağlık Merkezi ve Methodist Hastanesi'nin sistemlerine yerleştirilen ransomware virüsü ile hastane kayıtlarının çalınması olayını üstlenen Türk Hacker gruplarına bir karşılık olarak Anonymous ile özdeşleşmiş olan Guy Fawkes maskesi takan bir kişi "#OpTurkey Revenge on Turkey" isimli videoda Türk sağlık kurumları sistemlerine sızdığını ve sistemlerde ki bilgileri çaldığını iddia etmiştir.

Sağlık Bakanlığına bağlı 33 devlet hastanesinin veri tabanındaki bilgilerin hackerlar tarafından silindiği ortaya çıkmıştır. Anonymous isimli hacker grubu tarafından yapıldığı ifade edilen siber saldırıda; söz konusu hastanelerin silinen verilerin yedeklerini sisteme yüklemeye çalıştığı ancak grubun bunu engellediği tespit edilmiştir. Bu saldırıdan sonra Sağlık Bakanlığının Sağlık Bilişim Özel Ağını kurduğu ve tüm sağlık kurumlarını bu ağa taşımaya çalışarak verilerin güvenliğini sağlamaya çalıştığı görülmüştür. Çalınan milyonlarca verinin sosyal medyada yayınlandığı ve bunlar arasında HIV test sonuçları, kürtaj bilgileri gibi mahrem kayıtların da yer aldığı tespit edilmiştir (URL 9, URL 1, URL 10, URL 5, URL 11).

Bir başka haber metninde; Bursa'daki sağlık kurumlarından 267 bin hastanın tedavi gördüğü doktor, aldığı sağlık raporları, test, tahlil gibi laboratuvar bilgileri gibi verilerinin çalındığı ifade edilmiştir (URL 13). Tüm bu haberler değerlendirildiğinde E-sağlık uygulamalarının etik ihlaller içerdiği görülmektedir.

2.2.2. Sağlık Kurumlarına Yönelik Siber Saldırı (19 Ağustos 2014-12 Mayıs 2017)

Bu ana tema altında Sağlık Bakanlığı tarafından açıklanan ve yaklaşık 33 ildeki hastanelere yapılan siber saldırı, İngiltere'nin Ulusal Sağlık Sistemine yapılan saldırı, Türkiye'nin de içinde bulunduğu 74 ülkeye yapılan siber saldırı, Sağlık Bakanlığı sitelerine yapılan siber saldırı, İspanya'da büyük şirketlere yapılan siber saldırı, Türkiye, Amerika, İngiltere, Amsterdam gibi ülkelerdeki hastanelere yapılan siber saldırılar, bazı büyük sağlık sigortası şirketlerine yapılan siber saldırılar ve Barack Obama'nın da verilerinin çalındığı bir sigorta şirketine yapılan siber saldırı yer almaktadır.

İngiltere'de NHS'ye bağlı 16 sağlık kurumunun etkilendiği siber saldırıda, hackerların 300 dolar karşılığında dijital para birimi Bitcoin talep ettiği tespit edilmiştir. Söz konusu saldırı sonrasında NHS sağlık bilgi işlem ağının tamamen çöktüğü bildirilmiştir. NHS'yi vuran virüs yazılımın Türkiye'nin de içinde bulunduğu 74 ülkeye yayıldığı ve 57 binden fazla bilgisayarı etkilediği tespit edilmiştir (URL 14; URL 15; URL 16; URL 17; URL 19; URL 20; URL 21).

Ek olarak Sağlık Bakanlığı sitelerine siber saldırı yapıldığı ve bu saldırı sonucu Sağlık Bakanlığı sayfalarının erişime kapatıldığı haber metinlerinde yer almaktadır. Ayrıca İspanya'daki en büyük şirketlere siber saldırı yapıldığı, güvenlik şirketleri ya da askeri kuruluşların dahi bu

saldırılardan etkilendiği, bu sebeple söz konusu ülkelerde acil durum ilan edildiği de ilgili haber metinlerinde yer almaktadır (URL 22).

4,5 milyon hastanın verilerinin çalındığı siber saldırıda Amerika'daki en büyük ikinci hastane zincirinin veri tabanına sızılmıştır. Yanı sıra Barack Obama ve ailesinin kayıtlarının da bulunduğu sigorta şirketi Anthem siber saldırıya uğramış ve 80 milyon kişinin sağlık kayıtları çalınmıştır. Buna ek olarak Sigortacılıkta Öngörülen Riskler 2017 raporuna göre siber riskler ikinci sırada yer almaktadır. Güvenlik uzmanları, siber suçluların ABD sağlık sektöründen 3 trilyon dolar kazanmayı hedeflediğini belirtmişlerdir (URL 23; URL 24; URL 25).

2.2.3. Mobil Sağlık Cihazları ve İnternet Bağlantılı Medikal Cihazlara Siber Saldırı (14 Nisan 2015-1 Haziran 2017)

Bu tema altında akıllı sağlık cihazlarının, internete bağlı tıbbi cihazların ve özellikle de kalp pillerinin siber saldırı tehdidine açık olduğu temaları tespit edilmiştir. Akıllı cihazların siber saldırılara karşı korunaksız olduğu ifade edilen haber metinlerinde akıllı sağlık cihazlarının yoğunlukla kullanıldığı Amerika'nın özellikle tehdit altında olduğu vurgulanmıştır.

Denetim, vergi ve danışmanlık hizmetleri sunan KPMG 2017 raporuna göre; yeni teknolojiyle üretilmiş, ağa bağlı ve birbiriyle bağlantılı sağlık cihazları siber risklere de kapı açıyor. 2000'li yıllardan itibaren hızla büyüyen erişilebilir, takılabilir ve giyilebilir tıbbi cihaz teknolojisi siber saldırılar karşısında savunmasız. Türkiye'de de kullanılan akıllı medikal cihazların bağlantılı olduğu ağların siber güvenlik açısından yetersiz olduğu tespit edilmiştir. Rapora göre; sağlık kuruluşlarının %81'inin 2016 yılında en az bir kez siber saldırıya uğradığı da göz önünde bulundurulduğunda durumun ciddiyeti ortaya çıkmaktadır (URL 12; URL 26; URL 27).

Başka bir cihaza bağlanacak şekilde yapılandırılmış her cihazın siber risk altında olduğu vurgulanan haber metinlerinde kişisel sağlık bilgilerinin karaborsada kredi kartı bilgilerinden 10 kat daha değerli olduğu da ifade edilmiştir. Medikal cihazlara yönelik olan siber saldırılarda; tıbbi hizmetlerin kesintiye uğraması, kötü amaçlı yazılımların sisteme bulaşması, verilerin çalınması ve para karşılığında satılması gibi sonuçlar doğabilmektedir (URL 28).

Siber suç ekonomisinin hedefinde yer alan ve iyi korunamayan sağlık sektöründeki başka bir tehlike ise hayati önem taşıyan akıllı cihazlar. Kalp pili ya da insülin pompası gibi akıllı sağlık cihazlarının kötü amaçlı yazılımlarca kolayca erişilebilir olması tehlikeyi arttırmaktadır. Amerikan Gıda ve İlaç Dairesi, sağlık cihazı üreticilerine bir uyarı göndermiş ve

siber saldırganların akıllı kalp pillerini bile hackleyebileceğini bildirmiştir. Amerikan Gıda ve İlaç Dairesi, ritim bozukluğu gibi hastalıkların tedavisinde son birkaç yıldır kullandığı akıllı kalp pillerinin güvenlik zafiyetini öğrenmek için bir dizi teste tabi tutmuş ve bu cihazların siber korsanlar tarafından ele geçirilebileceğini ifade etmiştir. Aynı şekilde; akıllı insülin pompaları siber güvenliğinin hackerlara karşı zayıf olduğu gerekçesiyle piyasadan kaldırılmış ve hastanelerin bu cihazı kullanmasına izin verilmemiştir (URL 18, URL 29, URL 30; URL 31, URL 32, URL 34).

Cihazların güvenliğinin test edildiği araştırmada; kalp piline kablosuz internet üzerinden ulaşılabileceği, korsanların cihazı durdurmakla kalmayıp ölümcül bir elektroşok oluşturabileceği, çok fazla sayıda kişinin kullandığı vücutta taşınan insülin pompasının uzaktan kontrol edilerek dozajının yeniden ayarlanabileceği ve acilde kullanılan ilaç pompalarının uzaktan ele geçirilip bu pompalardan akan sıvıların alt ve üst sınırlarının aşılarak hastaya zarar verilebileceği tespit edilmiştir (URL 35; URL 33; URL 36).

Nesnelerin interneti uygulamalarının sağlık sektöründe yoğun bir şekilde kullanıldığı düşünüldüğünde milyonlarca hastanın tehdit altında olduğu gerçeği ortaya çıkmaktadır. Akıllı tıbbi cihazların ara yüzlerinin internet üzerinden erişilemez olduğu ve sadece hastane içerisindeki bir bilgisayardan çalıştığı varsayımı bu cihazları tehlikelere daha da açık kılmaktadır. Nitekim bu varsayımdan ötürü alınması gereken güvenlik tedbirleri asgari düzeyde alındığında yeter görülmektedir (URL 37; URL 38).

National Institute of Standards and Technology'nin tehlike derecelendirmesine göre; ShellShock güvenlik açığı nedeniyle telefonlar, dağıtıcılar, medikal cihazlar ve web sunucuları da dâhil olmak üzere yaklaşık 500 milyon internet bağlantılı cihaz ve servis tehlike on üzerinde on derecesiyle en yüksek tehlike altında bulunan cihazlardır (URL 39). İncelenen haberlerde E-sağlık uygulamalarının bahsedilen tehlikelere karşı oldukça korunaksız olduğu dikkat çekmektedir. Bu durum çalışmanın temel savını da desteklemektedir.

2.2.4. Korumasız Sağlık Verileri (19 Ağustos 2014-1 Haziran 2017)

Bu ana tema altında sağlık verilerinin siber saldırılara karşı güvenliğinin yetersiz olduğu, sağlık kayıtlarının para karşılığında satılabileceği ve dolayısıyla korsanlar için çok değerli olduğu gibi alt temalar bulunmaktadır.

Elektronik sağlık kayıtları ve mobil cihazları düşünüldüğünde sağlık sisteminin tamamının risk altında olduğu ve güvenlik zafiyetinin olduğu haber metinlerinde yer almaktadır. Sağlık cihazlarının çoğunun üretim aşamasında belirlenen şifrelerle kullanıldığı ve bu şifrelerin kullanıcı kurumlar tarafından değiştirilmeye lüzum görülmediği ifade edilmiştir. Bu şifrelerin "1234" gibi basit şifreler olduğu göz önünde bulundurulursa; cihazların güvenliklerinin çok zayıf olduğu ortaya çıkmaktadır. Sağlık sisteminde kayıtlı bilgilerin organ mafyaları ya da biyolojik silah üreticileri için oldukça cazip bilgiler olduğu belirtilmiştir. Hayati önemi olan bu kayıtların internette milyon dolarlık değerlerinin olduğu ve online ortama taşınan sağlık kayıtlarının güvenlik düzeylerinin iyileştirilmemesi halinde bu pazarın büyüyeceği öngörülmektedir. Ayrıca internet ortamına bir şahsa ait sosyal güvenlik numarasının değeri 15 dolar iken bir sağlık verisinin değerinin 60 doları bulduğu ve bir kişinin sağlık kaydının kuruma 4 milyon dolara mal olacağı da ifade edilmektedir (URL 40; URL 41; URL 13; URL 42; URL 43; URL 44; URL 45).

Intel Security, McAfee Labs Sağlık Uyarıları raporuna göre; sağlık sektörü siber suç ekonomisinin hızla yükselen trendlerinden biri olmuştur. Bunun nedeni sağlık sektöründe verilerin güvenliğinin bulunmaması olarak gösterilmiştir (URL 2).

Tüm bu ana tema ve alt temalar değerlendirildiğinde; mobil sağlık uygulamalarının güvenlik açıkları nedeniyle etik ihlallere yol açacağı söylenebilir. Mahremiyet içeren kişisel sağlık kayıtları ve hayati önem taşıyan mobil sağlık cihazlarının internet ortamındaki korunaksızlığı; bu uygulamaların etik boyutunun problemli olduğunu göstermektedir.

3. Sonuç

Sağlık hizmet sektöründe teknolojinin kullanılması önemli bir gelişmedir. Ancak teknolojinin getirmiş olduğu yenilikler, diğer taraftan da çeşitli riskleri beraberinde getirmektedir. Bu risklerin en çok hissedildiği alanlardan birisi E-sağlık ve daha spesifik olarak mobil sağlıktır. Günümüzde mobil sağlık uygulamaları her geçen gün daha fazla önem kazanmaktadır. Akıllı telefonlar, tabletler, akıllı saatler, giyilebilir teknolojiler ve akıllı gözlükler başta olmak üzere çok sayıda cihaz, mobil sağlık uygulamaları kapsamında kullanım alanı bulmaktadır. Çalışma yöntemi doğrultusunda elde edilen veriler değerlendirildiğinde; günümüz dünyasının yeni hayat biçiminde yerini almaya başlayan mobil sağlık uygulamalarının güvenlik açıkları nedeniyle etik ihlallere yol açacağı söylenebilir.

Türkiye'de Sağlık Bakanlığı'nın kişisel sağlık verilerinin işlenmesi, korunması, saklanması, mahremiyetinin sağlanması gibi konulara önem verdiği ve bu yönde çalışmalar yürüttüğü gözlemlenmiştir. Örneğin kişisel sağlık verilerinin işlenmesi ve mahremiyetinin sağlanması doğrultusunda yayımlanan yönetmelik, bu alandaki etik ihlallerin ve sorun alanlarının engellenmesi için bir nevi önemli bir misyon üstlenmiştir. Hem bu yönetmelik hem de diğer hukuki düzenlemeler çerçevesinde kamu ve özel sağlık hizmet sunucularının kişisel verilerin gizliliği ve güvenliği açısından daha sorumlu davrandıkları ve bu yöndeki politika ve uygulamalarını hastalarla da web sayfası kanalı başta olmak üzere çeşitli şekillerde paylaştıkları gözlemlenmiştir. Ancak mobil sağlık uygulamalarının kullanımı açısından etik ihlallerin sistem ve insan kaynağı odaklı olabileceği gerçeğinden hareketle kişisel verilerin korunması çalışmalarının genişletilerek ve güçlendirilerek sürdürülmesi ciddi bir önem arz etmektedir.

Çalışma sonucunda başlıca öneriler şu şekilde sıralanabilir:

a) Politika yapıcılar ve sağlık organizasyonları bilişim alanında yetenekli bireyleri keşfederek özel ekipler kurmalıdır.

b) Sistem ve insan kaynağı ile ilgili sürdürülebilirlik konusunun, yetkililer tarafından güvence altına alınması gerekir.

c) Sistem kontrolünün birden fazla kişiye ve birbirilerini tamamlayıcı şekilde verilmesi önerilmektedir.

d) Politika yapıcılar ve diğer sorumlular tarafından bu alandaki hukuki alt yapının güçlendirilmesi gerekmektedir.

e) Sonuç olarak yerel sağlık bilgi sistemlerinin geliştirilmesi ve bu sistemlerin olası siber saldırılara dayanıklı hale getirilmesi önerilmektedir.

Kaynaklar

Albrecht, Urs-Vito ve Fangerau, Heiner (2015). "Do Ethics Need to Be Adapted to mHealth? A Plea for Developing a Consistent Framework". *World Medical Journal* 61(2):72-75.

Arslan, E. Türkan ve Demir, Hüseyin (2017). "Üniversite Öğrencilerinin Mobil Sağlık ve Kişisel Sağlık Kaydı Yönetimine İlişkin Görüşleri". *Aksaray Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi* 9(2):17-36.

Ay, Fatma (2008). "Elektronik Hasta Kayıtları: Güvenlik, Etik Ve Yasal Sorunlar". *Anadolu Üniversitesi Bilim Ve Teknoloji Dergisi* 9(2):165-175.

Brüggemann, Thomas, Hansen, Jon, Dehling, Tobias ve Sunyaev, Ali (2016). "An Information Privacy Risk Index for mHealth Apps". In: Schiffner S., Serna J., Ikonomou D., Rannenberg K. (eds) *Privacy Technologies and Policy*. APF 2016. Lecture Notes in Computer Science, Vol 9857. Springer, Cham.

Demir, Hüseyin ve Arslan, E. Türkan (2017). "Mobil Sağlık Uygulamalarının Hastanelerde Kullanılabilirliği: Hastane Yöneticileri Üzerine Bir Araştırma". *KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi* 19 (33):71-83.

Dülger, Murat Volkan (2017). "Kişisel Sağlık Verilerinin İşlenmesine Dair Yönetmelik'in Getirdikleri Ve Dikkat Edilmesi Gereken Hususlar", (http://www.hukukihaber.net/kisisel-saglik-verilerinin-islenmesine-dair-yonetmelikin-getirdikleri-ve-dikkat-edilmesi-gereken-hususlar-makale,5557.html, 13.08.2018 tarihinde erişildi).

Given, Lisa M. (2008). *The SAGE Encyclopedia of Qualitative Research Methods*, Los Angeles: Sage Publications.

Greenspun, Hanry ve Coughlin, Sheryl (2012). *mHealth in An mWorld: How Mobile Technology is Transforming Health Care,* Deloitte Center for Health Solutions.

Kılıç, Taşkın (2017). "e-Sağlık, İyi Uygulama Örneği; Hollanda". *GÜSBD* 6(3):203-217.

Kırılmaz, Harun ve Kırılmaz, S. Kılıç (2014). "Sağlık Hizmetlerinde Etik İkilemlerde Ampirik Etik Çalışmalarının Yararları". *İnsan&İnsan* Volume 1, Summer 2014:35-44.

Kişisel Sağlık Verilerinin İşlenmesi Ve Mahremiyetinin Sağlanması Hakkında Yönetmelik (2016). Resmi Gazete Tarihi: 20.10.2016 Sayısı: 29863.

Kluge, Eike-Henner W. (2004). "Informed Consent And The Security Of The Electronic Health Record (EHR): Some Policy Considerations". *International Journal of Medical Informatics* 73(3):229-234.

Kumar, Santosh, Nilsen, Wendy J., Abernethy, Amy, Atienza Audie, Patrick, Kevin ve Pavel, Misha (2013). "Mobile Health Technology Evaluation: The mHealth Evidence Workshop". *Am J PrevMed 45(2):*228-236.

Labrique, Alain, B., Kirk, Gregory D., Westergaard Ryan, P. ve Merritt, Maria, W. (2013). "Ethical Issues in mHealth Research Involving

Persons Living with HIV/AIDS and Substance Abuse". *AIDS Research and Treatment* Volume 2013, Article ID 189645, http://dx.doi.org/10.1155/2013/189645.

Nalbantoğlu, Lerzan (2018). "Kişisel Sağlık Verilerinin İşlenmesi Ve Mahremiyetinin Sağlanması Hakkında Yönetmelikte Yapılan Değişiklikler", (https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/the-deloitte-times/TDT_Subat%202018_hukuk.pdf, 13.08.2018 tarihinde erişildi).

Research 2 Guide (2017). mHealth App Economics 2017 Current Status and Future Trends in Mobile Health. https://research2guidance.com/product/mhealth-economics-2017-current-status-and-future-trends-in-mobile-health/ (15.01.2018)

Rippen, Helga ve Risk, Ahmad (2000). "e-Health Code of Ethics (May 24)". *Journal of Medical Internet Research*, 2(2), e9:1-6.

Tezcan, Cenk (2016). "Sağlığa Yenilikçi Bir Bakış Açısı: Mobil Sağlık". *TÜSİAD Yayınları,* Yayın No: TÜSİAD-T/2016-03/575.

URL 1, http://www.haberturk.com/saglik/haber/1241415-anonymous-turkiyedeki-saglik-kayitlarini-caldi-mi, 10 Ekim 2017'de erişildi.

URL 2, http://www.haberturk.com/ekonomi/teknoloji/haber/1544235-wannacrydan-sonra-petya-oldugu-tahmin-edilen-saldiri-dunyayi-esir-aliyor, 10 Ekim 2017'de erişildi.

URL 3, http://haber.sol.org.tr/toplum/saglik-bakanligindan-siber-saldiri-aciklamasi-o-ilin-saglik-kayitlari-calindi-156362, 10 Ekim 2017'de erişildi.

URL 4, https://journo.com.tr/8-adimda-50-milyon-kisinin-verileri-calinmasi-olayi-ve-riskler, 10 Ekim 2017'de erişildi.

URL 5, http://www.cumhuriyet.com.tr/haber/saglik/535900/Kim_kurtaj__kim_kalp_ameliyati_oldu__Turk_hastalarin_bilgileri_ortaliga_sacildi.html, 10 Ekim 2017'de erişildi.

URL 6, http://www.bbc.com/turkce/haberler/2015/09/150924_abd_parmak_izi, 10 Ekim 2017'de erişildi.

URL 7, http://www.habersaglikcilar.com/saglik-bakanligi-sitelerine-siber-saldiri-var.html, 10 Ekim 2017'de erişildi.

URL 8, http://www.bsha.com.tr/Haber/hastanelere-siber-saldiri-iddiasi/290, 10 Ekim 2017'de erişildi.

URL 9, http://t24.com.tr/haber/saglik-verileri-calinan-1-milyona-yakin-vatandasin-arasinda-50-hivnin-de-listesi-yayimlandi,341496, 10 Ekim 2017'de erişildi.

URL 10, http://www.gazetesaglik.com/kisilerin-saglik-verileri-calindi-haberi-21149.html, 10 Ekim 2017'de erişildi.

URL 11, https://www.medikalakademi.com.tr/akilli-tibbi-cihazlar-siber-tehdit-altinda-saglik-verileriniz-guevende-mi/, 10 Ekim 2017'de erişildi.

URL 12, https://www.medikalakademi.com.tr/hacker-grubu-anonymous-tuerkiyedeki-tuem-saglik-verilerini-hackledi/, 10 Ekim 2017'de erişildi.

URL 13, http://www.milliyet.com.tr/son-dakika-siber-saldiri-dunya-2449398/, 10 Ekim 2017'de erişildi.

URL 14, https://www.sabah.com.tr/dunya/2017/05/12/ingilterede-saglik-sistemine-siber-saldiri, 10 Ekim 2017'de erişildi.

URL 15, http://www.aksam.com.tr/guncel/son-dakika-ulkelere-siber-saldiri-duzenleniyor-siber-saldiri-nedir/haber-623071, 10 Ekim 2017'de erişildi.

URL 16, http://www.hurriyet.com.tr/ingilterede-sok-saglik-sistemi-bugunku-son-siber-saldiri-ile-tamamen-coktu-40456278, 10 Ekim 2017'de erişildi.

URL 17, https://www.ntv.com.tr/dunya/ingiliz-saglik-sistemi-veri-tabanina-siber-saldiri,WFVv1BiF3UW52ptRukpOUQ, 10 Ekim 2017'de erişildi.

URL 18, https://www.ntv.com.tr/saglik/kalp-pilleri-bilgisayar-korsanlarinin-eline-gecebilir,IotlDCHeW06Lp9XIqHgDfg, 10 Ekim 2017'de erişildi.

URL 19, https://www.medimagazin.com.tr/dis-haberler/ekonomi/tr-ingilterede-saglik-sistemine-siber-saldiri-76-684-73831.html, 10 Ekim 2017'de erişildi.

URL 20, http://www.gazetevatan.com/ingiltere-de-saglik-sistemine-siber-saldiri-1066269-teknoloji/, 10 Ekim 2017'de erişildi.

URL 21, http://www.haber10.com/dunya/ingiltere_de_saglik_sistemine_siber_saldiri-703862, 10 Ekim 2017'de erişildi.

URL 22, http://tr.euronews.com/2017/05/12/ingiltere-de-hastanelerin-bilgisayar-sistemlerinin-bagli-oldugu-ulusal-saglik-hizmeti-nsh-

agina-buyuk-olcekli-bir-siber-saldiri-duzenlendi, 10 Ekim 2017'de erişildi.

URL 23, https://shiftdelete.net/4-5-milyon-hasta-kaydi-calindi-54215, 10 Ekim 2017'de erişildi.

URL 24, http://www.sigortacigazetesi.com.tr/saglik-sigortasi-sirketi-antheme-siber-saldiri/, 10 Ekim 2017'de erişildi.

URL 25, http://portal.jlt.com.tr/abd-nin-en-buyuk-sigorta-sirketinden-80-milyon-kisinin-bilgileri-calindi, 10 Ekim 2017'de erişildi.

URL 26, https://home.kpmg.com/tr/tr/home/media/press-releases/2017/03/akilli-tibbi-cihazlar-siber-tehdit-altinda.html, 10 Ekim 2017'de erişildi.

URL 27, https://epnext.com/akilli-tibbi-cihazlar-siber-tehdit-altinda/, 10 Ekim 2017'de erişildi.

URL 28, http://www.netinternethaber.com/siber-saldirilar-kalp-pillerini-de-vuruyor/232134/, 10 Ekim 2017'de erişildi.

URL 29, http://lepicallidus.com/teknoloji/siber-guvenlikte-yeni-sorun-medikal-cihazlar, 10 Ekim 2017'de erişildi.

URL 30, http://www.marmarahaber.net/haber/akilli-cihazlar-icin-siber-saldiri-uyarisi-52137.html, 10 Ekim 2017'de erişildi.

URL 31, http://www.haber7.com/teknoloji/haber/2240398-kalp-piline-siber-saldiri, 10 Ekim 2017'de erişildi.

URL 32, https://h4cktimes.com/arastirma-ve-analiz/siber-suc-ekonomisi-saglik-sektorundeki-iyi-korunmayan-verilerle-zenginlesiyor.html, 10 Ekim 2017'de erişildi.

URL 33, https://h4cktimes.com/arastirma-ve-analiz/tibbi-cihazlarin-hacklenmesi.html, 10 Ekim 2017'de erişildi.

URL 34, http://www.kanalahaber.com/haber/saglik/saglik-bakanligindan-siber-saldiri-ve-telefon-dolandiriciligi-uyarisi-314595/, 10 Ekim 2017'de erişildi.

URL 35, http://www.teknolojiks.com/kalp-pilleri-siber-saldiriya-karsi-savunmasiz-mi/420/, 10 Ekim 2017'de erişildi.

URL 36, http://www.itnetwork.com.tr/akilli-cihazlar-guvenlik-engeline-takiliyor/, 10 Ekim 2017'de erişildi.

URL 37, https://www.kaspersky.com.tr/blog/vulnerable-medical-equipment/2208/, 10 Ekim 2017'de erişildi.

URL 38, http://www.computerworld.com.tr/dosya-konulari/guvenlik/saklanacak-yeriniz-yok-hedefinde-sizin-oldugunuz-9-yeni-saldiri/, 10 Ekim 2017'de erişildi.

URL 39, https://www.technopat.net/2014/09/26/500-milyon-cihaz-tehlike-altinda/, 10 Ekim 2017'de erişildi.

URL 40, http://www.aljazeera.com.tr/haber/abd-hastanelerine-cin-saldirisi, 10 Ekim 2017'de erişildi.

URL 41, http://www.sozcu.com.tr/2016/saglik/calinti-saglik-bilgileri-kredi-karti-bilgilerinden-daha-degerli-1496125/, 10 Ekim 2017'de erişildi.

URL 42, https://www.uyumsoft.com/dunyada-son-35-yilda-veri-hirsizligi-sonucu-37-milyar-kayit-calindi/, 10 Ekim 2017'de erişildi.

URL 43, https://www.cnnturk.com/teknoloji/saglikta-buyuk-tehdit-siber-saldiri, 10 Ekim 2017'de erişildi.

URL 44, http://www.bthaber.com/saglikta-bilisim-ve-beklentiler/siber-saldirilar-saglik-sektorune-de-kayiyor/1/18036, 10 Ekim 2017'de erişildi.

URL 45, http://www.globaltechmagazine.com/siber-suclularin-yeni-hedefi-saglik-sektoru-mu/, 10 Ekim 2017'de erişildi.

Varshney, Upkar (2014). "Mobile health: Four Emerging Themes of Research". *Decision Support Systems* Volume 66, October 2014: 20-35.

Vélez, Olivia, Okyere, Portia B., Kanter, Andrew, S. ve Bakken, Suzanne (2014). "A Usability Study of A Mobile Health Application For Rural Ghanaian Midwives". *J Midwifery Womens Health* 59(2), 184-191.

WHO (2011). "mHealth-New Horizons For Health Through Mobile Technologies". *Global Observatory for eHealth series* Volume 3, www.who.int/goe/publications/ehealth_ series_vol3/en/ (11.01.2018).