İLERİ SAĞLIK TEKNOLOJİLERİ III
Sağlıkta Dijitalleşmenin Önündeki Yol Haritası

ARAŞTIRMA RAPORU KASIM 2019

thinktech
STM Teknolojik Düşünce Merkezi

STM ThinkTech

1. GİRİŞ

Gelişen teknolojiyle birlikte tüm dünyada yaşanan Dördüncü Sanayi Devrimi'ne geçiş süreci pek çok sektör gibi sağlık alanında da yaşanmaktadır. Özellikle genetik ve tıp alanında ortaya çıkan büyük değişimlerle birlikte akıllı robotlar, sensörler, gelişmiş veri depolama ve analiz sistemleri ve daha birçok teknoloji sağlık sistemini yeniden şekillendirmektedir.

Sağlıklı ve gelişmiş toplum hedefine ulaşabilmek ancak iyi örgütlenmiş bir sağlık sistemiyle mümkündür. İyi örgütlenmiş bir sağlık sisteminin oluşturulmasında sağlık bilişim sistemlerinin önemi ise oldukça büyüktür. Sağlık sektöründe yer alan kurumlar, sundukları sağlık hizmetlerine yönelik karar verme aşamasında bilgi teknolojileri ve sağlık bilişim sistemlerinden faydalanmak durumundadır.

Dördüncü Sanayi Devrimi ile sistemlerin artık birbirlerine bağlı olması ve gelişen mobil cihazlar, hem uzaktan erişim hem de veri paylaşımı için yaygın olarak kullanılmaktadır. Sağlık sektöründe birbirine bağlı ekipmanlar ve bakım sistemleri yaygınlaştıkça, siber güvenlik de giderek büyüyen bir kaygı konusu haline gelmiş, hasta güvenliği, veri bütünlüğü ve genel olarak siber güvenlik, sağlık sektörünün en temel zorlukları olmaya başlamıştır.

Sağlık hizmeti sağlayan kurumlardaki kritik altyapılar, halkın refahı ve güvenliği için hayati öneme sahiptir. Hastane ortaklıkları, medikal enstitüler ve araştırma laboratuvarları benzersiz ve değerli verileri yönetirken bu sektörde önemli yeni iş akışları geliştirilmiş, bu da yeni ve hızla büyüyen güvenlik güçlüklerini beraberinde getirmiştir.

Bunun yanı sıra sigortacılık sektörü de, dijital kanal kullanımının giderek yaygınlaşması ve müşteri beklentilerinin değişmesiyle birlikte hızlı ve köklü bir dönüşümden geçmektedir. Dijitalleşme sürecini avantaja dönüştürerek sektörde öne çıkmayı hedefleyen sigorta şirketlerinin, sundukları ürün ve hizmetleri, sürekliliği olan dinamik bir yaklaşımla yeni teknolojilere adapte etmesi her zamankinden büyük önem taşımaktadır.

İleri Sağlık Teknolojileri Araştırma raporumuzun üçüncü bölümünde sağlıkta dijitalleşmenin önündeki yol haritasına bakarken, dijitalleşmenin getirdiği risklere ve bu risklerden korunmak için geliştirilen yeni sağlık ve sigortacılık modellerine değinilecektir.

2. SİBER GÜVENLİK SORUNLARI VE SAĞLIKTA KİŞİSEL VERİNİN KORUNMASI

Sağlık sektörü son yıllarda çok sayıda yoğun ve karmaşık siber güvenlik tehdidiyle karşı karşıya kalmıştır. Kimlik Hırsızlığı Kaynak Merkezi (Identity Theft Resource Center) verilerine göre, sadece son üç yılda tüm sektörler arasında en yüksek sayıda veri hırsızlığının yaşandığı sektör sağlık sektörü olmuştur[1].

Kurumların güvenlik harcamaları daha önce hiç olmadığı kadar artarken, siber suçlular da kişisel tıbbi kayıtlar gibi hassas bilgileri çalmak için yeni yollar aramaya devam etmektedir. Sağlık kuruluşları siber saldırılara en az diğer sektörler kadar maruz kalsa da farklı olan, risk

altında olanın yalnızca iş değil aynı zamanda insan sağlığı olmasıdır[2].

Sağlık sektörü sunduğu hayati hizmetlerle hastaların bakımı ve tedaviler için teknolojiyi kullanarak geliştikçe siber korsanlar bu gelişim içindeki zaafları bularak saldırılarını güçlendirmenin yollarını aramaktadır. Aslında birçok sektörü kökten etkileyen bu saldırıların sağlık sektöründeki etkileri finansal kayıpların yanında kişisel verilerin gizliliğine de dokunduğundan çok daha benzersiz bir risk oluşturmaktadır[3]

Dünyaca ünlü bulut güvenlik şirketi "Bitglass", her yıl ABD Sağlık ve İnsan Hizmetleri Departmanının "Utanç Duvarı" adı verilen bir veri bankasının analizini yapmaktadır. Bu veri bankasında bulunan kayıtlar Korumalı Sağlık Bilgileri ile ilgili kayıtların ihlal edilme durumlarını içermektedir. Raporlarda dört önemli başlık dikkat çekmektedir.

- **Hack'lenme veya Bilişim Teknolojisi Hataları:** Kötü niyetli hack'lemeler veya yetersiz bilişim teknolojisi güvenliğini kapsamaktadır.
- **İzinsiz Giriş veya İfşa:** Bütün izinsiz girişler ve korunan sağlık bilgilerinin ifşasını kapsamaktadır.
- **Kayıp veya Veri Hırsızlığı:** Verilerin kaybolması veya çalınmasıyla ilgili ihlalleri kapsamaktadır.
- **Diğerleri:** Birçok farklı ihlal ve veri sızıntılarını kapsamaktadır.

Rapora göre 2018 yılında sağlık sektöründeki ihlallerden ABD'de 11.5 milyon birey etkilenmiştir. Bu ihlallerin başında yüzde 67'yle hack'leme veya BT hataları gelmektedir[4].

2.1 Sağlık Sektöründe Olası Siber Tehditler

Küresel ölçekte değerlendirildiğinde ise 2019 ve sonrası için sağlık sektöründe beş siber güvenlik başlığı öne çıkmaktadır. Bu başlıkların her biri aslında yeni olmamakla beraber sağlık ve bilişim teknolojileri (BT) yöneticilerinin gelişen teknolojiye ayak uydurarak yeni ve güncel hamleler yapması gerekmektedir.

- **Bulut Güvenliği:** Hastanelerin artan gizli kayıtlarının ve veri havuzlarının yükünü BT çalışanlarından alarak erişimi ve kullanımı daha kolay bulut teknolojisine taşıması önemli riskleri beraberinde getirmektedir. Sistemin bulut güvenliğini ihlal etmek isteyenlerin daha önceki veri bankalarına girmek için gözetim yapması ve sabit bir noktadan girişi gerekirken bulut teknolojisinde bu zorluk ortadan kalktığından savunması zor bir alan oluşmaktadır.
- **Güvensiz Mobil Cihazlar:** Çalışanlardan hastalara, hatta ziyaretçilere kadar herkesin kullandığı mobil cihazlarla kurulan bağlantılar bir diğer endişe noktası olarak düşünülmektedir[5].
- **Ransomware:** Fidye yazılımları, bulaştığı sistemlerdeki dosyaların bir kısmının veya tümünün şifrelenerek kilitlenmesine sebep olan bir zararlı yazılımdır. Verileri kilitleyen kişi daha sonra fidye karşılığında kilidi kaldırarak tekrar erişime izin vermektedir[6].

  Hastaların hayatı sözkonusuyken, birçok kurum verileri geri almak ve hizmetlerini yeniden kullanabilmek için en iyi tercihin fidyeyi ödemek olduğunu düşünmektedir[2].

Ransomware'ın 2019 ve sonrasında en önemli bilgi güvenliği konusu olması beklenmektedir. Gizli sağlık verilerinin özellikle karaborsada yüksek değerlere satılması bu güvenlik ihlalinin önemini artırmaktadır.

- **IoT İstismarları:** Nesnelerin interneti (IoT) ve bağlantılı sağlık sistemleri, sağlık kuruluşları için çok büyük fırsatlar sunmakla birlikte beraberinde büyük riskler de ortaya çıkarmaktadır. Giyilebilir ve vücuda yerleştirilebilir sağlık cihazlarının bağlantıları, saldırılara açık hale gelmelerine sebep olmaktadır. Ayrıca birçok IoT sağlık cihazının uç nokta güvenlik uygulaması içermemesi kötü niyetli bir saldırının engellenememesiyle sonuçlanmaktadır.

  Sağlık sektöründe kullanılan IoT cihazlarının aşırı çeşitliliği ve sayıca fazlalığı uç nokta güvenlik uygulamalarının geliştirilmesi ve uygulanmasında hem teknik hem de lojistik anlamda büyük bir zorluk yaratmaktadır.

- **İnsan Faktörü:** Sağlıkta siber güvenlik risklerinin artmasında en yaygın etken ise insan faktörüdür. Yeterli eğitime sahip olmayan çalışanlar, bireylerin hassas ve kişisel verileriyle ilgili doğru önlemleri uygulayamadıklarından bu verilerin dışarıdan ihlal edilmesi kolaylaşmaktadır[5].

  Sağlık sektörünü dış tehditlere karşı korumak kadar önemli bir diğer unsur ise korumalı sağlık bilgilerinin uygun şifreleme ve güvenlik önlemleri olmadan kurumun dışına çıkarılmasını engellemektir. Sağlık alanı, çalışanların sızıntıdaki en önemli tehdit olduğu tek sektördür[7].

  Ağ ve paylaşım kaynaklı risklerin azaltılması için çalışanların, uygun güvenlik eğitimleri ve günlük hatırlatma notları alması veya çalışanların daha farklı uygulamalarla güvenlik sistemleriyle ilgili işlem ve değişiklikler hakkında sürekli bilgi alması gerekmektedir[5].

2.2 Sağlık Sektörüne Yönelik Siber Saldırılar Artıyor

STM Savunma Teknolojileri, Mühendislik ve Ticaret A.Ş. (STM) ye bağlı Teknolojik Düşünce Merkezi "ThinkTech" tarafından yayınlanan ve Ocak-Mart 2019 dönemini kapsayan "Siber Tehdit Durum Raporu"na göre, nesnelerin interneti teknolojisini kullanan "Uzaktan Hasta Takip Sistemi", hasta verilerinin gerçek zamanlı olarak sağlık görevlilerine iletilmesinde kullanılan kablosuz ağlardan oluşmaktadır[8].

Siber saldırganlar, kablosuz ağlara farklı yöntemlerle saldırarak hasta bilgilerinin ifşa olmasını sağlayabildikleri gibi, hastayla ilgili manipüle edilmiş veriler üreterek sistemleri yanıltabilmektedir. Bu tür saldırılar, hastanın hayatını kaybetmesine kadar uzanan sonuçlara yol açabilmektedir.

2022'de 14 milyar dolarlık bir büyüklüğe erişmesi beklenen sağlık alanındaki nesnelerin interneti pazarıyla birlikte, bu sistemlerin daha büyük bir risk faktörü olması öngörülmektedir[8].

Genel bir bakış açısıyla sağlık sektörünün siber güvenlik konusunda diğer alanlara kıyasla daha geride kalmış olması en büyük zayıflığı olarak gösterilmektedir[7].

Kimlik Hırsızlığı Kaynak Merkezinin (Identity Theft Resource Center) yayınladığı verilere göre, 2017'nin ilk yarısında gerçekleşen ve çok gizli kişisel verilerin çalınmasıyla sonuçlanan saldırıların yaklaşık yüzde 25'i sağlık veya ilaç sektörüyle ilgili kurumlara yöneliktir. Sağlık kurumlarındaki hasta verileri giderek artmakta ve bu veriler arasında siber suçluların kimlik sahtekârlığı yapabilmesini sağlayacak kişisel ve finansal bilgiler yer almaktadır.

Dünya genelinde sağlık kurumlarına yönelik saldırılardaki artış, potansiyel tehditlerin farkına varılmasını sağlamıştır. Ancak bazı grupların sağlık sistemlerine çok kolayca saldırabilmeleri, bu saldırıların hacker'lar için ne kadar kârlı olduğunu da ortaya çıkarmaktadır. Sağlık

hizmeti verenlerin önümüzdeki beş ila on yıl içerisinde daha sıkı güvenlik için güncel teknolojilere yatırım yapmaları beklenmektedir.

2.3 STM Sağlık Sektörünü Siber Tehditlere Karşı Koruyacak

Bu alanda Türkiye'de de hizmet veren kurumların sayısı artmaktadır. Sağlık sektörüne yönelik siber saldırılar konusunda çalışmalar yapan STM de bunlardan biridir. Kurum 2019'un Haziran ayında sağlık sektöründe kullanılan internete bağlı cihazların siber güvenliğine yönelik Başkent Üniversitesi ile protokol imzalamıştır. Projeyle geliştirilecek IoT-Medic, hastanelerde kullanılan medikal IoT cihazların envanterinin çıkarılmasını, bu tür cihazlara karşı yapılabilecek saldırıların tespit edilerek raporlanmasını sağlayacaktır. Kullanıcılar, bu sistem sayesinde hastane ortamındaki tüm medikal IoT cihazlarını tek noktadan takip ederek bu cihazların oluşturduğu trafikteki anormallikleri ve olası saldırıları canlı olarak takip edip müdahale edebilecektir[9].

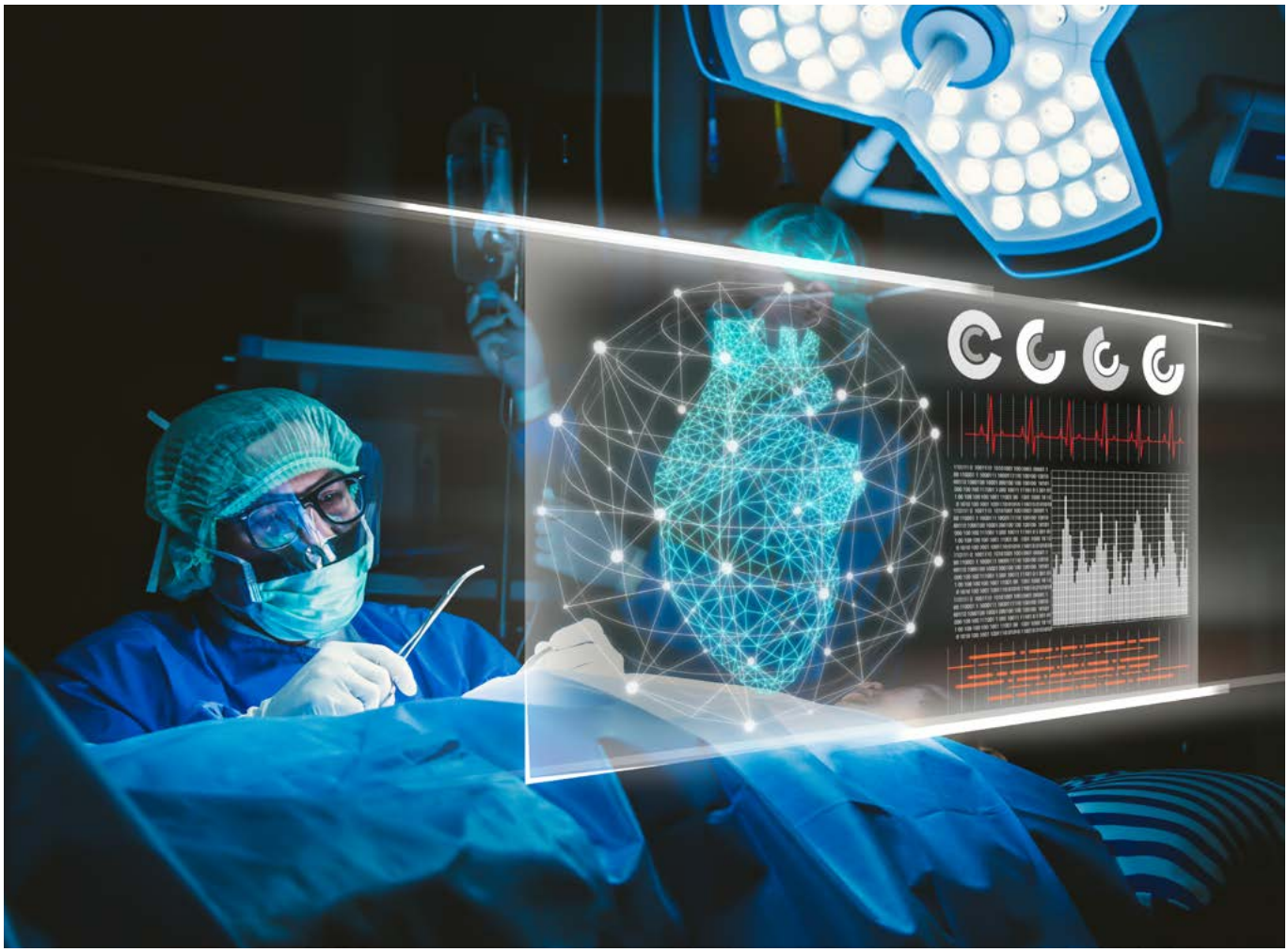
2.4 Sağlık Sektörü Verilerine Yapılan Saldırılar

Veri güvenliğine daha kesin çözümler bulunana kadar, sağlık sektöründe çalışan BT profesyonelleri yeni teknolojilerin yaygın olarak kullanılmasının önündeki büyük engellerle uğraşmaya devam edecektir. Bu nedenle, sağlık hizmeti sunanların önümüzdeki yıllarda güvenilir erişim yönetimi prosedürleri ve sistemleri uygulayarak güvenliği geliştirmeleri beklenmektedir. Bunun yanı sıra, işletim sistemlerinin, tarayıcıların ve uygulamaların güncel tutulması da güçlü erişim güvenliği kontrolü sağlamak için gerekenler arasında yer almaktadır[2].

2015 yılında ABD'nin önemli sağlık sigortası firmalarından olan Anthem'de hacker'ların neden olduğu devasa bir veri ihlali yaşanmış ve bu durum 78,8 milyon kişiyi etkilemiştir. Anthem, yaşanan saldırı sonrası yaptığı açıklamada, içlerinde üye ve çalışanlarının da bulunduğu kişilerin isim, doğum tarihi, sosyal sigorta numarası ve bazı başka bilgilerini de içeren verilerinin çalındığını, yapılan kontroller sonrasında kredi kartı veya sağlık kayıtları gibi önemli verilerin korunduğunu bildirmiştir[10].

Anthem'in saldırıya uğradığı yıl başka bir grup hacker UCLA Sağlık Sistemi'nin bilgisayar ağına girerek yaklaşık 4,5 milyon hastanın bilgilerine erişmiştir. Üniversite Sağlık Grubu yaşanan bu olayı saldırıdan ancak iki ay sonra bütün hasar tespiti yapılınca açıklayabilmiştir. Yaşanan bu olay sonrası hastane grubu hastalara ve çalışanlarına bir yıl boyunca kimlik hırsızlığı kurtarma servisi sunacağını bildirmiştir[11].

Mayıs 2017'de Wannacry olarak da bilinen zararlı yazılım İngiltere'deki 80 hastane ve 603 sağlık merkezini etkiledi. Hastanelerin çalışamamasından dolayı yaklaşık



19 bin randevu iptal edildi. Etkilenen hastanelerde görüntüleme cihazları uzun süre çalışmadı. Hasta verilerine ulaşılamadı veya ilgili yerlere gönderilemedi. Beş hastane acil hasta kabulünü yapamadığından ambulansları diğer hastanelere yönlendirdi. Hastanelerin tekrar sağlıklı çalışmaya başlaması üç, dört günü buldu[12].

Temmuz 2018'de, ABD'nin Atlanta şehrinde 10 milyon dolar civarında maddi hasara yol açan SamSam zararlı yazılımı LabCorp isimli şirketin tüm makinelerini şifreleyerek kilitlemiştir. Aynı anda Kanada'da CarePartners, 80 bin hastanın tıbbi geçmişini ve iletişim bilgilerini benzer bir saldırıya kurban vererek bu alanda bir rekora imza atmıştır. İşin ilginç yanı ise *CBC*'nin haberine göre saldırganların CarePartners'ın ağında iki yıldır güncellenmemiş bir güvenlik açığı bulduklarını ve bu sayede tüm bilgilere kolayca ulaştıklarını paylaşmalarıdır[13].

2.5 Sağlık Sektöründe Güvenlik İçin Segmentasyon Şart

Bu gelişmeler, segmentasyona dair önemli bir noktayı da akıllara getirmektedir. Sağlık sektörünün her daim çalışan bir sektör olduğu bilinmektedir. Örneğin, acil servis ağının hafta sonu dahil olmak üzere sürekli çalışıyor olması, bir saldırı sebebiyle çalışmasının durmaması ya da yavaşlamaması gerekmektedir. Öte yandan, her zaman çalışır durumda olması gerekmeyen departmanların da olduğu bilinmektedir. Her zaman çalışamayan bir departmanda, mesai süresi dışında bir cihaza giriş yapılması bir saldırı habercisi olabilmektedir. Saldırıları başlatmak, genişletmek ya da ağda yatay hareket etmek için düzensiz çalışma saatlerinde çalışan ele geçirilmiş cihazlar, acil servisteki gibi son derece gerekli olan ağları etkileyebilmektedir. Bu sebeple, sağlık sistemlerinin ek bir savunma katmanı ekleyerek önemli ağlarda segmentasyona başvurmaları ve ne amaçla kullanıldıkları anlaşılana kadar anormal davranışlar gösteren cihazları izole etmeleri önerilmektedir[14].

Bir ülkenin bütün sağlık sektörü ağının siber güvenliği her bir hastane ve kuruluşun siber saldırılara karşı zaaflarıyla etkilenebilmektedir. İster hastane içinde izolasyon yöntemleri olsun ister geniş ağlarda sınırlandırmalar yapılsın sektör birbiriyle bağlantılı çalıştığı sürece siber suçlular bir noktadaki zafiyeti sisteme sızmak ve zarar vermek için kullanabilmektedir. Bu nedenle bütün hastane ve sağlık kuruluşlarının birlikte ilerlemesi ve önlemlerini geliştirmesi, sistemlerindeki siber saldırılara karşı zayıf yönlerini azaltması ve siber saldırganlar için daha az çekici hale gelmesini sağlaması gerekmektedir[15].

3. DÖRDÜNCÜ SANAYİ DEVRİMİNİN SAĞLIK SEKTÖRÜNDEKİ ETKİLERİ

Tüm dünyada gelişen teknolojiyle birlikte sağlık alanında da Dördüncü Sanayi Devrimi'ne geçiş süreci yaşanmaktadır. Bilim ve teknoloji alanında özellikle de genetik ve tıp alanında büyük değişimler ortaya çıkmaktadır.

Yeni dönem, sağlık kuruluşlarını hızlı ve sürekli bir değişime yöneltmiştir. Dördüncü Sanayi Devrimi'yle sağlık kuruluşları; küresel yöntemlerle teknolojiyi kullanarak mekân sınırlamasını kaldırmış, hizmetini gereken her yere ulaştırabilen, son teknolojilere hâkim, kişiye özel teşhis ve tedavi sunabilen merkezler haline gelmiştir[16].

Sağlık endüstrisi, yönetmeliklere uyum sağlama ve uygulamada oldukça kapsamlı bir alandır. Hasta güvenliğinin bir parçası olan bu yönetmelikler, sağlık hizmetlerindeki hızın azalması gibi olumsuz bir etkiye

neden olabilmektedir. Ancak Dördüncü Sanayi Devrimi çözümleri bu alanda da önemli yenilikleri beraberinde getirmektedir[17].

ABD Gıda ve İlaç İdaresi (FDA) tarafından onaylanmış ilk otonom yapay zekâ olan Idx-DR, Dördüncü Sanayi Devrimi'nin sağlık sektöründe sunulan hizmetlere kazandırdığı hızın bir örneği olarak gösterilmektedir. Oküler görüntülerde diyabetik retinopati bulgularını saptayarak çalışan program birkaç dakika içinde ikili tanı üretebilen bir algoritmayla çalışmaktadır. Bu sayede hastaların tanıları çok daha hızlı konulabilmektedir.

Yapay zekâ yazılımları kardiyovasküler hastalıkların tanılarında da oldukça önemli avantajlar sağlamaktadır. Dünyada yılda ortalama 17.9 milyon insanın kardiyovasküler hastalıklardan yaşamını yitirdiği bilinmektedir. Koroner arter hastalıkların işaretlerinin ekodiyagramlarda çıplak gözle tespiti oldukça zor olduğundan hastaların yüzde 20'si teşhis edilemeyebilmektedir. FDA'da onay bekleyen EchoGo yazılımı yapay zekâyı kullanarak eko diyagramlarda çıplak gözle incelendiğinde kaçırılabilecek detayları yakalayarak teşhislerin güçlenmesine olanak vermektedir[18].

Hastaya özgü cihazların geliştirilmesini sağlayan Dördüncü Sanayi Devrimi, tıbbi imalat alanında da önemli avantajlar sağlamaktadır. Dördüncü Sanayi Devrimi ile ürünler ve yazılımla geliştirilmiş donanımlar, kendi yönetiminin ve üretim hattının optimizasyonunu sağlamak için akıllı bilgi alışverişinde bulunabilmektedir. Hasta ihtiyaçları için tamamen kişiselleştirilmiş ürünlerin otomatik olarak üretilmesi sadece pratik olmakla kalmayıp, aynı zamanda yüksek verimli ve ekonomik hale gelmektedir[17].

ESCAD Medical GmbH, Dördüncü Sanayi Devrimi'ni sağlık sektöründe başarılı bir şekilde uygulayan şirketlerden biridir. Endoskopide uzmanlaşan küçük tıbbi cihaz şirketi, endoSTORE® adlı bir depolama sistemi kullanmaktadır. Bu sistem, endoskopide ortaya çıkabilen enfeksiyonun önlenmesini sağlamaktadır. Endoskoplar, bir barkod tarayıcıyla kaydedilmekte ve bir güvenlik sorgusuyla uygun olmayan şekilde dezenfekte edilmiş endoskopun hastaya ulaşması önlenmektedir. Şirket bu ve benzeri girişimleriyle "Baden-Württemberg'de Endüstri için 100 Yer Listesi" yarışmasının kazananlarından biri olmuştur.

Dördüncü Sanayi Devrimi uygulamalarıyla güçlendirilmiş akıllı fabrikalar da tedarik hızlarını artırarak sağlık sektörüne destek olmaktadır. Aesculap AG'nin inovasyon fabrikası 2015 yılında faaliyete geçtiğinden bu yana hastaneler ve cerrahi motorlar için steril kaplar üretmektedir. Firma açtığı akıllı fabrikayla personel sayısını değiştirmeden steril kap üretimini iki katına çıkarmayı hedeflemektedir[19].

Dördüncü Sanayi Devrimi'nin önemli kavramlarından biri olan büyük veri, doktorların klinik araştırmalarında daha iyi kararlar almalarına destek olmaktadır. Birbirine bağlı sistemlerle verilerin güvenli bir şekilde paylaşıldığı araştırma ve çalışmalarda birçok doktorun tecrübesi ve bulguları bir araya gelerek muazzam bir veri havuzu oluşturabilmektedir. Bu sayede özel durumlarda bile en etkili tedaviler uygulanarak hasta güvenliği korunmaktadır.

Tedavilerin yanında giderlerin ve kullanılan ekipmanların uygunluklarının değerlendirilmesi ve doğru işe doğru personel ve ekipmanın atanması gibi avantajlar büyük veriyle mümkün olmaktadır[20].

Dördüncü Sanayi Devrimi teknolojileri sağlık sektörünün önemli bir parçası olan ilaç üreticilerini de etkilemektedir. Gelişmiş dijital kodlarla işlenmiş ilaçlar takibi kolay ve daha güvenli hale gelmektedir. Dijital kod ile işlenmiş bir ilaç, şirketten ayrıldıktan sonra açıkça tanınabilir durumda olmaktadır. Bu, tüm lojistik zincirinde izlenebilirliği sağlamakta ve sahte ilaçların önüne geçilmesine olanak vermektedir. Avrupa Birliği'nde 2019'dan itibaren ilaçlar, yalnızca ambalajında dijital kodlu seri numarası olması ve hasar görmemiş olması halinde satılabilmektedir. Dördüncü Sanayi Devrimi, ilaç sektörüne sağladığı avantajla üretimin ötesine geçerek tüm değer zincirini kapsamaktadır[17].

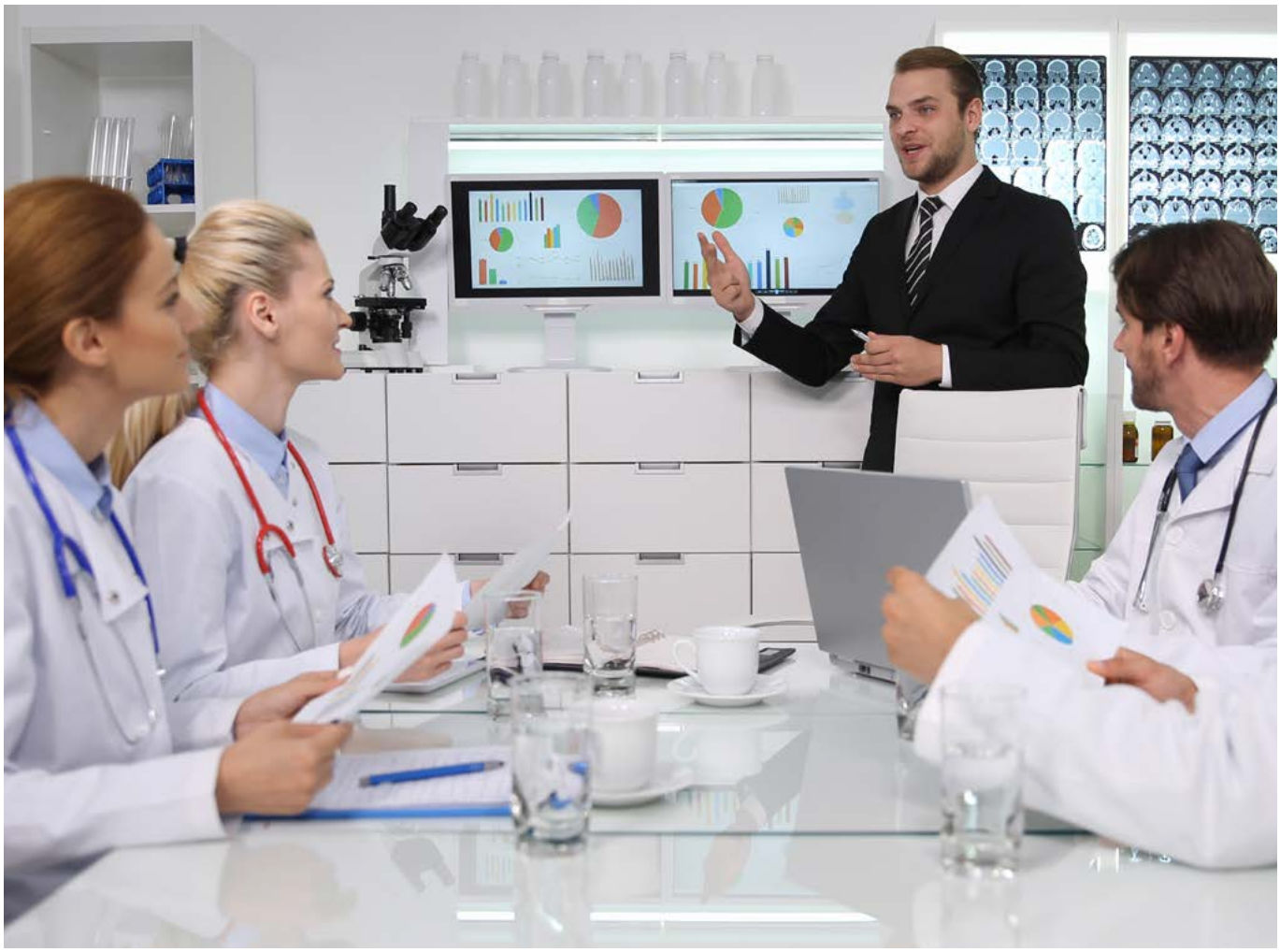
Dördüncü Sanayi Devrimi ile gelişen sağlık sektörü içinde sağlık kuruluşlarının da dijital dönüşüme ayak uydurması ve gelişmesi gerekmektedir. Sağlık kuruluşlarında dijital dönüşüm için dört önemli unsur bulunmaktadır. Bunlar dijital veriler, bağlanabilirlik, otomasyon ve dijital müşteri arayüzü olarak öne çıkmaktadır. Veriler ve bağlanabilirlik unsurları uzaktan yapılan cerrahi operasyonlar, eğitimler, bakım işlemleri ve hizmet operasyonları açısından ele alındığında bu başlıklar içindeki en önemlileri olarak değerlendirilmektedir[21].

4. YENİ HASTANE YÖNETİMİ MODELLERİ VE HASTANELERİN YENİ İŞLEVLERİ

Dördüncü Sanayi Devrimi'nin sağlık sektörüne sağladığı katkılar sağlık kuruluşlarının yönetimleri ve protokolleri üzerinde de değişime gitmelerini sağlamıştır. Hastaneler için en önemli konu sağlık endüstrisinde değişen ihtiyaçlara karşı nasıl uyum sağlanacağıdır. PwC'nin Sağlık Araştırma Enstitüsü, geleceğin hastane yönetim modellerine dört önemli örnek göstermektedir.

- **Üründe Lider Hastane Modeli:** Bu modelin odak noktası hastanelerin en üst kalitede, gelişmiş tedaviler sunmasıdır. Daha maliyetli veya kompleks olan özel sağlık ihtiyaçlarını karşılamaya yönelik düşünülen model Tele Sağlık gibi teknolojik marka ve ürünlere odaklanarak işlemektedir[22].

  Minesota'da hizmet veren Mayo Clinic ve Ohio'da hizmet veren Cleveland Clinic üründe lider hastane yönetim modellerinin örneklerindendir. Cleveland Clinic, 2020'de Londra'da açacağı tesisle Birleşik Arap Emirlikleri, Çin ve Kanada'da faaliyette olan sağlık sistemlerine eklemede bulunarak uluslararası alanda yaygınlığını artırmayı hedeflemektedir[23].



- **Tecrübede Lider Hastane Modeli:** Bu model mümkün olan en iyi müşteri deneyimini hedeflemektedir. Daha çok müşteri sadakatine dayanan model iyileştirme, hasta tercihleri ve maliyet şeffaflığını ön plana çıkarmaktadır. Hastaların tedavilerinde neye, ne kadar harcama yapılacağının üzerinde tam kontrolü olması sistemin en önemli özelliği olmaktadır[22].

  Sistemin hedef kitlesi daha çok sağlığı düzgün seyreden hasta popülasyonları olsa da tek bir organ veya vücut sistemini etkileyen kronik hastalıklı hastalara ve basit tedavi gereken rahatsızlıklara da odaklanılmaktadır.

  "Teksas Sağlık Kaynakları" bütün Teksas sağlık organizasyonlarına kesintisiz ve bütünleşik bir şekilde veriler sağlayan ve ticari amaç gütmeyen tecrübede lider hastane modeli olarak örnek gösterilebilir[23].

- **Entegratör Hastane Modeli:** Bu model ölçekleme ve kapsam ile tüketicilerine en iyi değeri sunmayı hedeflemektedir. Ulusal ve uluslararası olarak uygulanabilmesiyle PwC'nin araştırmasında geleceğin modelleri arasında en büyük olanı olarak değerlendirilmektedir. Markaya odaklanılmayan modelde sunulan düşük maliyetli çözümler için hastane dışı kaynaklara yönelmek ve ekonomik teşviklerle maliyetleri düşük tutmak amaçlanmaktadır[22].

  Utah'da bulunan Intermountain Health, ortaklık sağladığı altı diğer sağlık sistemiyle ticari amaç gütmeyen bir ilaç firması mantığıyla reçeteli ilaç maliyetlerini düşürmeyi ve ilaç kıtlığını önlemeyi planlamaktadır[23].

- **Sağlık Yöneticisi Hastane Modeli:** Bu modelin odak noktası karmaşık ve geniş popülasyonları yüksek maliyetli sistemlerden uzak tutmaktır. Popülasyonların iyi anlaşılması, risk ve sağlık eşitliğinin dengeli olması ve kamu ile ortak hareket edilmesi aranan özellikler olmaktadır[22].

  Bir sağlık yöneticisinin görevi bütün bir popülasyonun sağlığını zaman içinde geliştirmektir. Bu model yönetim direkt olarak kamu ve işverenlerle sözleşme yaparak işlemektedir. Sağlığın sosyal risk faktörlerini ele almak hastane yöneticisi modelinin anahtar özelliğidir. Sosyal risk faktörlerinden kaynaklanan sağlık eşitsizliklerinin tıbbi maliyetleri yıllık 102 milyar dolar olarak hesaplanmaktadır[23].

4.1 Türkiye'de Şehir Hastaneleri Dönemi

Türkiye'de ise Sağlık Bakanlığının 2002 yılında başlattığı Sağlıkta Dönüşüm Programı'nın ikinci fazı olan "Şehir Hastaneleri", yeni bir hastane yönetim modeli olarak köklü değişikliklere imza atmaktadır[24].

Sağlıkta "Şehir Hastaneleri Dönemi" olarak adlandırılan bu yeni süreçte çalışan planlamasından finansmana, ek ödeme sisteminden sağlık hizmet fiyatlarına, yerli tıbbi cihaz üretiminden sağlık eğitimlerine kadar birçok alanda yeniden yapılandırma gerekmektedir.

Kamu Özel İşbirliği (KÖİ) modeline dayanan Şehir Hastaneleri'nin genel amaçları hizmetlerin ekonomik, etkili ve verimli bir şekilde sunulması, özel sektörün gelişimine fırsat tanınması ve rekabet ile genel ekonomik gelişime katkı, uygun bir risk ve ödül paylaşımı ile kamunun, özel sektörün ve hizmet verilen popülasyonun en üstün yararı elde etmesi olarak öne çıkmaktadır[25].

Türkiye Cumhuriyeti Sağlık Bakanlığı 2019 verilerine göre 10 adet açılmış ve faaliyette olmak üzere toplamda planlanmış 20 Şehir Hastanesi bulunmaktadır. En büyük hastane olan Ankara Bilkent Şehir Hastanesi yatak kapasitesi 3.704 adet olmakla beraber, planlanan bütün şehir hastanelerinin toplam yatak kapasitesinin 30.815 adet olacağı belirtilmektedir[26].

Hastanelerin gelecekte teknolojiden ve yeni modellerden etkilenerek değişmesi ve yeni özellikler kazanması da mümkün görülmektedir. Gelişen ve değişen sağlık sektöründe hastanelerin gerçekten akut bakım gereken hastalar için öncelikli kullanılması, evde tedavi edilebilir hastaların Tele Sağlık sistemi gibi teknolojilerle izlenmesi, parakende kliniklerle sağlıkta tüketimin artması, gelişmiş ve iyileştirilmiş hasta deneyimleri için süreçlerin yeniden planlanması ve sağlık sektörünün gelişimi için tüm sağlık kuruluşlarının işbirliği hastanelere ve sağlık kuruluşlarına yeni ve öngörülemez fonksiyonlar kazandırabilir[27].

5. SAĞLIK SİGORTALARI VE YENİ YAPILARI İÇİNDE RİSK YÖNETİMİ

Teknoloji ile gelişen sağlık sektöründe riskler ve yeni modeller yeni önlemleri de beraberinde getirmektedir. Sağlık sigortacılığındaki yaşanan değişim de bu gelişmelerle ortaya çıkmıştır.

Sigortalar, başımıza kötü bir şey gelmesi durumunda bizlere finansal koruma ve güvence sağlayan uygulamalar olarak bilinmektedir. Birçok sigorta formatı genellikle başımıza gelebilecek şeylerin gerçekleşme oranının düşük olmasına bağlı olarak çalışmaktadır. Ancak sağlık sigortaları daha özel bir konumda bulunmaktadır. Oluşum esasları diğer sigorta formatlarıyla benzerlik gösterse de sağlık sigortaları aslında çok

daha karmaşık ve sıklıkla kullanılan uygulamalar olarak karşımıza çıkmaktadır[28].

Sağlık sigortalarının hemen hemen hepsinde bir risk paylaşım uygulaması bulunmaktadır. Bu uygulama birden fazla bireyin aynı riski paylaştığı ortak bir havuzda primlerin toplanması ve ihtiyaç halinde hastalanan bireye ödeme yapılması prensibine dayanmaktadır. Sonuç olarak bu prensiple risk paylaşımı ya da risk havuzu uygulaması üyeler içinde sağlığı daha kötü olan bireylerin ödeyecekleri yüksek maliyetlerin, sağlığı daha iyi olan bireylerin ödeyecekleri düşük maliyetlerle dengelenerek daha ekonomik primler ödenmesine imkân vermektedir[29].

Sağlık sigortalarında risk paylaşımı üç farklı şekilde uygulanabilmektedir.

- İlk olarak sigorta şirketi ve sigorta planını alan üyeler arasında bir risk paylaşımı uygulanabilmektedir. Bu şekilde riskler sigorta şirketi ve üyelere uygun oranlarla dağıtılmaktadır.
- İkinci olarak sigorta şirketiyle sağlık hizmetlerini verecek olan sağlık profesyonelleri risk paylaşımını aralarında uygulayabilmektedir. Burada risklerle ilgili oranlar üyelere yansıtılmadan verilecek hizmetlerin belirlenmesi kapsamında sigorta şirketi ve sağlık profesyonellerine uygulanarak bir plan oluşturulabilmektedir.
- Üçüncü olarak da sigorta planını aynı sigorta şirketi, pazar veya devlet destekli programdan alan herkesin riski paylaştığı bir yöntem uygulanabilmektedir.

Risk paylaşım uygulaması 2010'da yürürlüğe giren Obamacare olarak da bilinen "Ödenebilir Bakım Yasası" (Affordable Care Act -ACA) ile birlikte uygulanmaya başlanmıştır. Bu yasadan önce sigorta şirketlerinin bireylere risklerine göre daha yüksek veya düşük prim uygulaması veya sigorta başvurusu yapan bireyi reddetmesi gibi durumlar yaşandığı bilinmektedir. Yasayla birlikte bireylerin veya küçük toplulukların yaşına veya geçmiş rahatsızlıklarına bakılmaksızın aynı primi ödemesi sağlanmıştır.

ACA ile birlikte sigortacılıkta köklü değişiklikler sağlandığı gözlemlenmektedir. Bunlar şu şekilde sıralanabilir[28]:

- Sigorta şirketlerinin, geçmiş rahatsızlıklarından ötürü veya yaş durumundan kaynaklı riski yüksek dahi olsa insanların başvurularını reddetme uygulaması sonlandırılmıştır.
- Sağlığı daha kötü olan insanların daha iyi olanlara göre daha fazla prim ödemesi uygulaması kaldırılmıştır.
- Kadınların erkeklerden daha fazla prim ödeme uygulaması kaldırılmıştır.

Sigorta planına dahil her bireyin; check-up, aşılama, doğum, yenidoğan bakımı, kronik rahatsızlıkların yönetimi, akıl sağlığı servisleri gibi bazı çekirdek hizmetleri kesintisiz alması sağlanmaktadır.

Yeni uygulamalarla birlikte sağlık sektöründe hizmet veren firma ve bireylerin de sigortalanarak belirli risklerden korunması için gelişen uygulamalar bulunmaktadır. Kuruluşların veya hizmet veren bireylerin sigortalanmadan önce bir risk yönetimiyle mevcut ve olası risklerini belirlemeleri gerekmektedir. Riskler belirlendikten sonra oluşma olasılıklarına ve etkilerine göre sınıflandırılarak öncelik sıralaması yapılmalıdır[30].

Bu riskler göz önünde tutularak işyeri veya hizmet veren birey yapacağı değerlendirmeye göre uygun bir sigorta planına dahil olabilmektedir. Planların seçiminde ise risklerle beraber fiyatlandırmada rol oynayan üç unsur bulunmaktadır[31]:

- **Hasta Güvenliği/Kalitesi:** Hastaların güvenliği ve hizmet kalitesi açısından bazı faktörler fiyatlandırmayı etkilemektedir. Maliyetlerin düşürülmesi esnasında kalitenin artırılması, hekim istihdamı ile klinik entegrasyon sağlanması, stratejik ortaklıklarla farklı tedarikçilerle çalışılması, hemşire hizmetlerine daha fazla öncelik verilmesi, yeni bakım standartları, hasta beklentilerinin artırılması ve yeni formatta elektronik sağlık kayıtlarının kullanılması sigorta işlemlerinde değerlendirilen önemli bazı faktörler olarak bilinmektedir.
- **Doktor/Bakıcı Stratejisi:** Çok sayıda doktor çalıştırılması sağlık bakım sistemlerinde bir avantaj sağlayabilmektedir. Ancak değişken risk profilleri fiyatlandırmada değişikliklere neden olabilmektedir. Bu sebeple sağlık kuruluşları kendi kendine sigorta yaptıran hekim ve bakıcıları tercih etmektedir.
- **Geri Ödeme Riski:** Hizmetin ücretlendirilmesinden, alınan hizmetin değerinin ücretlendirilmesine geçiş yapan sağlık kuruluşları için ciddi risk artışı olduğu bilinmektedir. Geri ödeme maliyetlerinin düşürülmesi için uygun kuruluşlarla kurulacak stratejik ortaklıklar veya girişimler fayda sağlayabilmektedir.

Sağlık sektöründe değişen bir diğer alan da gelişen teknolojilerle ilgili doğan riskler olarak bilinmektedir. Bu alan için uygulanan "Sağlıkta Siber Risk Sigortası" dönüşen ve gelişen sağlık sektörünün etkilerinden biri olarak görülmektedir.

5.1 Sağlıkta Siber Risk Sigortası

Siber risk sigortası; belirli bir gizlilik düzeyine sahip ve korunması gereken bilgilerin açığa çıkması veya zarar görmesi sonucu yaşanabilecek hasarlara karşı işletmeleri koruyan sigorta poliçesidir. Siber risk sigortası, kişisel veya kurumsal verilerin ihlali nedeniyle doğabilecek zararları, ağ güvenliğine yapılan saldırılar veya ağ kesintisi nedeniyle yaşanan aksaklıklardan doğabilecek kayıp ve zararları, yaşanan bu tarz durumların itibar kaybına neden olmaması için yapılması gereken masrafları içermektedir[32].

Sağlık sektöründe uygulanan siber risk sigortasında diğerlerine ek olarak hastaların bilgilerinin ihlali veya

sağlık sistemlerinin zarar görmesiyle hastaların tedavilerinin aksaması gibi ek bazı durumlar da güvence altına alınmaktadır.

Radware adlı güvenlik firmasına göre; sağlık sektöründe ortalama bir siber saldırıdan sonra zararların telafi edilebilmesi için 1.4 milyon dolar harcama yapılması gerekebilmektedir[33].

Nisan 2017'de Erie County Tıp Merkezine (ECMC) yapılan Ransomware saldırısı siber risklerin önemini ciddi bir şekilde kanıtlamaktadır. Saldırıyla devre dışı kalan 6000 ECMC bilgisayarı altı hafta boyunca çalıştırılamamıştır. Saldırı aslında birkaç saat içinde fark edilse de sistemler bu sürede çoktan kilitlenmiş ve sonrasında ECMC çalışanları altı hafta boyunca sadece kalem ve kâğıtlarla çalışabilmiştir. İlk iki hafta e-posta ile iletişim kurulamadığından kayıtlar manuel olarak girilmiş, ancak üç haftanın sonunda laboratuvar sonuçları hastalara iletilebilmiştir. Barkly raporu, bu saldırının ECMC'ye maliyetinin yaklaşık 10 milyon dolar olduğunu göstermektedir.

Sağlık kuruluşları siber saldırılara karşı alınan bütün önlemlere rağmen yüzde 100 korunduklarından emin olamamaktadır. Hacker'lar medikal cihazlara, bilgisayarlara veya ağlara sızmak için yeni yollar buldukça risk de devam edecektir.

Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA) gibi kanunların da kapsandığı ve riskleri iyi değerlendirilmiş bir siber risk sigortası sağlık kuruluşları için hayati öneme sahip olabilmektedir[34].

Siber risklere yönelik sigorta pazarının, ABD ve Avrupa'da geçtiğimiz yıllarda yüzde 20-30 seviyesinde büyüdüğü belirtilmektedir. Küresel siber risk sigortası pazarının da 2020 yılında 10 milyar dolarlık hacme ulaşacağı tahmin edilmektedir. Ülkemizin sigortacılık piyasasının çok ciddi yol katetmiş olması sebebiyle artık siber risk sigortaları da yeni bir pazar olarak sunulabilmekte ve risklerin teminat altına alınması sağlanabilmektedir[35].

Türkiye'deki firmalara "Siber Risk Sigortası" hizmeti sağlayan CSC Türkiye'nin Genel Müdürü Alev Alp Esen'in verdiği bilgilere göre, siber risklere yönelik sigorta pazarının yıllık bazda büyümesinin yüzde 100'ü bulması ve pazar büyüklüğünün 10 yıldan daha kısa süre içinde 20 milyar dolara kadar çıkması beklenmektedir[36].

5.2 Sigortacılığın Geleceğini Şekillendiren Teknolojiler

Sigortacılık sektörü siber risklere karşı müşterilerini korurken teknolojiye de ayak uydurmak zorundadır. Uluslararası denetim ve danışmanlık şirketi EY, 2017 yılında yayınladığı "Dijital Sigortacılık Vizyonu" adlı raporda[37] gelişen teknolojinin yarattığı araçların sigortacılık sektörünü nasıl değiştireceği detaylandırılmaktadır. Rapor bu konuda şu noktalara işaret etmektedir:

- **Drone:** Ödeme talepleri, prim hesaplanması, poliçe hazırlanması ve ticari sigortacılıkta tesislerin incelenmesi gibi alanlarda bilgi toplama süreçleri drone'lar aracılığıyla yürütülecektir.
- **Blockchain:** Yeni ürün ve ödeme modelleri geliştirilmesi, dolandırıcılık tespiti, risklerin önlenmesi, ödeme taleplerinin yönetilmesi ve reasürans gibi alanlarda kullanılarak sigortacılık sektöründe güven ve şeffaflık güçlendirilecektir.
- **Telematik:** Uzaktan algılama sistemleri olarak bilinen bu teknoloji, araç ve sabit ekipman sigortalarında kullanılarak gerçek zamanlı veri akışı sağlayacaktır.
- **Yapay Zekâ (AI):** Robo-danışmanlarla birlikte sigortacılık sektörüne girecek olan bu teknoloji, müşteri sorularının yanıtlanması, şikâyetlerin değerlendirilmesi, teklif sunulması ve fiyatlandırma gibi alanlarda kullanılacaktır.
- **Robotik Süreç Otomasyonu:** Düşük riskli ödeme taleplerinde sürecin yürütülmesi, poliçenin yenilenmesi veya değişiklik yapılması gibi alanlarda kullanılacaktır.
- **Nesnelerin İnterneti (IoT):** Risklerin etkin biçimde önlenmesi, devam eden operasyonların takip edilmesi ve denetlenmesi, müşteri verisinin değerlendirilmesi ve ürün inovasyonunda kullanılacaktır.

6. SONUÇ

Geleneksel sağlık sistemleri, hastaneler, tedavi süreçleri, hasta-doktor ilişkileri günümüzde dijital bir dönüşüm yaşayarak yeni bir yapıya bürünmektedir. Özellikle elektronik, bilgi ve iletişim teknolojilerinde yaşanan gelişmeler bu dönüşümü daha da hızlandırmıştır. Akıllı robotlar, sensörler, gelişmiş veri depolama ve analiz sistemleri ve daha birçok teknoloji bu dönüşümde kilit rol oynamaktadır. Kendi kendini yönetebilen, denetleyen ve optimize eden bu otonom sistemler hayatımızı ve sağlık sistemini şekillendirmeye başlamıştır. Hastaneler de gelecekte teknolojiden ve yeni modellerden etkilenerek değişecek ve yeni özellikler kazanacaktır.

Bulut, IoT ve dijital BT sistemlerindeki gelişmeler, sağlık kuruluşlarının hastalara sunduğu bakımın kalitesini büyük ölçüde artırmasına yardımcı olmuştur. Bu teknolojiler bilgilerin çok kolay bir şekilde paylaşılabilmesi ve kişiselleştirilmiş tedavi imkânı sunmasıyla sağlık sektörünü tamamen dönüştürmüştür. Ancak elektronik sağlık kayıtları bu kuruluşları büyük veri hırsızlıkları ve operasyonel kesinti risklerine de maruz bırakmaktadır. Bu da sağlık sektörünü, siber saldırıyla karşılaşan alanlar içerisinde en fazla risk taşıyan sektör durumuna getirmektedir. Bu riskler sağlıkta sigortacılığın da önemini artırarak, sigorta şirketlerini teknolojiyi daha iyi kullanmaları ve siber risklerin de değerlendirildiği güvence poliçeleri hazırlamaları konusunda geliştirmektedir.

Bu risklerle ve güvenlik tehditleriyle mücadele etmek için veri yönetimi ve güvenliği göz önünde bulundurularak geliştirilen sistemleri kullanmak ve bu alanlara yatırım yapmak oldukça önem taşımaktadır. Bu sayede hayatımızı olumlu yönde dönüştüren sağlık teknolojilerini güvenle kullanabildiğimiz bir geleceğin oluşmasına imkân sağlanacağı düşünülmektedir.

KAYNAKÇA

[1] *Sigorta Gündem*, (2018), "Bilgisayar korsanlarının gözü sağlık sektöründe", (3 Mayıs 2018), http://www.sigortagundem.com/haber/bilgisayar-korsanlarinin-gozu-saglik-sektorunde/1302457. (Erişim Tarihi: 1 Kasım 2019)

[2] *Computer World*, (2018), "Sağlık hizmetlerinde BT güvenliğinin rolü", (12 Ocak 2018), http://www.computerworld.com.tr/haberler/saglik-hizmetlerinde-bt-guvenliginin-rolu/. (Erişim Tarihi: 1 Kasım 2019)

[3] Center for Internet Security, "Cyber Attacks: In the Healthcare Sector", https://www.cisecurity.org/blog/cyber-attacks-in-the-healthcare-sector/. (Erişim Tarihi: 1 Kasım 2019)

[4] *Help Net Security*, (2019), "Healthcare industry: Key trends and cybersecurity challenges", (26 Şubat 2019), https://www.helpnetsecurity.com/2019/02/26/healthcare-cybersecurity-challenges/. (Erişim Tarihi: 1 Kasım 2019)

[5] Eddy, Nathan; (2019), "5 cybersecurity threats healthcare faces in 2019 and beyond", *Healthcare IT News*, (8 Şubat 2019), https://www.healthcareitnews.com/news/5-cybersecurity-threats-healthcare-faces-2019-and-beyond. (Erişim Tarihi: 1 Kasım 2019)

[6] Fruhlinger, Josh; (2018), "Ransomware explained: How it works and how to remove it", *CSO*, (19 Aralık 2018), https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html. (Erişim Tarihi: 1 Kasım 2019)

[7] Öztürk Derya, (2018), "Siber Saldırganlar İçin En Büyük Hedef: Sağlık Sektörü", *Siber Güvenlik 101*, (2 Ocak 2018), http://siberguvenlik101.com/siber-guvenlik-saglik-sektoru/. (Erişim Tarihi: 1 Kasım 2019)

[8] *STM*, (2019), "Siber Tehdit Durum Raporu (Ocak - Mart 2019)", (19 Nisan 2019), https://thinktech.stm.com.tr/detay.aspx?id=226. (Erişim Tarihi: 1 Kasım 2019)

[9] *STM*, "Başkent Üniversitesi ile sağlık sektöründe kullanılan IoT temelli medikal cihazların siber güvenliğine yönelik protokol imzaladık.", https://www.stm.com.tr/tr/haberler/duyurular/baskent-universitesi-ile-saglik-sektorunde-kullanilan-iot-temelli-medikal-cihazlarin-siber-guvenligine-yonelik-protokol-imzaladik. (Erişim Tarihi: 1 Kasım 2019)

[10] Wilde Mathews, Anna; (2015), "Anthem: Hacked Database Included 78.8 Million People", *The Wall Street Journal*, (24 Şubat 2015), https://www.wsj.com/articles/anthem-hacked-database-included-78-8-million-people-1424807364. (Erişim Tarihi: 1 Kasım 2019)

[11] Pagliery, Jose; (2015), "UCLA Health hacked, 4.5 million victims", *CNN*, (17 Temmuz 2015), https://money.cnn.com/2015/07/17/technology/ucla-health-hack/. (Erişim Tarihi: 1 Kasım 2019)

[12] *National Audit Office*, (2018), "Investigation: WannaCry cyber attack and the NHS", (25 Nisan 2018), https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf. (Erişim Tarihi: 1 Kasım 2019)

[13] *NETAŞ*, "2018'de dünyayı kasıp kavuran siber güvenlik olayları", https://www.netas.com.tr/media/102533/cyberwiz_linked.pdf. (Erişim Tarihi: 1 Kasım 2019)

[14] *Global Tech Magazine*, (2019), "Sağlık sektörünü hedef alan 3 önemli siber saldırı trendi", (1 Ağustos 2019), https://www.globaltechmagazine.com/2019/08/01/saglik-sektorunu-hedef-alan-3-onemli-siber-saldiri-trendi/. (Erişim Tarihi: 1 Kasım 2019)

[15] S Jalali, Mohammad; P Kaiser, Jessica; (2018), "Cybersecurity in Hospitals: A Systematic, Organizational Perspective", National Center for Biotechnology Information, (28 Mayıs 2018), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5996174/. (Erişim Tarihi: 1 Kasım 2019)

[16] Şimşek, Tolga; "Endüstri 4.0 ile Geleceğe Bakış ve Beklentiler", *www.endustri40.com,* https://www.endustri40.com/endustri-4-0-ile-gelecege-bakis-ve-beklentiler/. (Erişim Tarihi: 1 Kasım 2019)

[17] Kesayak, Burak; "Sağlık 4.0: Sağlıkta Dijital Dönüşüm", *www.endustri40.com*, https://www.endustri40.com/saglikta-dijital-donusum-saglik-4-0/. (Erişim Tarihi: 1 Kasım 2019)

[18] *Diognostic and Interventional Cardiology*, (2019), "How Will Artificial Intelligence Impact Healthcare?", (7 Mayıs 2019), https://www.dicardiology.com/article/how-will-artificial-intelligence-impact-healthcare. (Erişim Tarihi: 1 Kasım 2019)

[19] Pott, Ariane; (2016), "Industry 4.0 in the medical technology and pharmaceutical industry sectors", *Healthcare industry BW* (20 Ekim 2016), https://www.gesundheitsindustrie-bw.de/en/article/dossier/industry-40-in-the-medical-technology-and-pharmaceutical-industry-sectors. (Erişim Tarihi: 1 Kasım 2019)

[20] *Iron Mountain*, "Three Ways to Use Big Data in Healthcare", https://www.ironmountain.com/resources/general-articles/t/three-ways-to-use-big-data-in-healthcare. (Erişim Tarihi: 1 Kasım 2019)

[21] Hosseini, Morris; (2015), "Digital transformation in healthcare", *Roland Berger*, (21 Nisan 2015), https://www.rolandberger.com/en/Publications/Digital-transformation-in-the-healthcare-space.html. (Erişim Tarihi: 1 Kasım 2019)

[22] Rappleye, Emily; (2018), "PwC: 4 hospital business models of the future", *Becker's Hospital Review*, (5 Ekim 2018), https://www.beckershospitalreview.com/hospital-management-administration/pwc-4-hospital-business-models-of-the-future.html. (Erişim Tarihi: 1 Kasım 2019)

[23] LaPointe, Jacqueline; "4 Hospital Business Models for Consumer-Centric Healthcare", *Revcycle Intelligence*, https://revcycleintelligence.com/news/4-hospital-business-models-for-consumer-centric-healthcare. (Erişim Tarihi: 1 Kasım 2019)

[24] *Sağlık Aktüel*, (2019), "2 yılda 8 şehir hastanesi açıldı, 2019'da 3 tane daha açılacak", (9 Ocak 2019), https://www.saglikaktuel.com/haber/2-yilda-8-sehir-hastanesi-acildi-2019da-3-tane-daha-acilacak-64831.htm. (Erişim Tarihi: 1 Kasım 2019)

[25] Atasever, Mehmet; Gözlü, Mehmet; Özaydin, Mehmet Merve; Güler, Hasan; Örnek, Mustafa; Barkan, Onur Burak; Kavak,Yusuf; İlhan, M. Necmi; (2018), "Şehir Hastaneleri Araştırması", *SASAM*, (Temmuz 2018), http://www.sasam.org.tr/wp-content/uploads/2018/07/Sehir-Hastaneleri-Arastırması.pdf. (Erişim Tarihi: 1 Kasım 2019)

[26] *T.C. Sağlık Bakanlığı Sağlık Yatırımları Genel Müdürlüğü*, (2019), "Şehir Hastaneleri", (1 Ağustos 2019), https://sygm.saglik.gov.tr/TR,33960/sehir-hastaneleri.html. (Erişim Tarihi: 1 Kasım 2019)

[27] Dyrda, Laura; (2017), "45 hospital and healthcare executives outline the hospital of the future", *Becker's Hospital Review*, (17 Temmuz 2017), https://www.beckershospitalreview.com/hospital-management-administration/45-hospital-and-healthcare-executives-outline-the-hospital-of-the-future.html. (Erişim Tarihi: 1 Kasım 2019)

[28] Anderson, Ashley Taylor; "How health insurance works: An intro to risk sharing", *Oscar*, https://www.hioscar.com/blog/how-health-insurance-works-risk-sharing. (Erişim Tarihi: 1 Kasım 2019)

[29] *American Academy of Actuaries*, "Risk Pooling: How Health Insurance in the Individual Market Works", https://www.actuary.org/content/risk-pooling-how-health-insurance-individual-market-works-0. (Erişim Tarihi: 1 Kasım 2019)

[30] *Nejm Catalyst*, (2018), "What Is Risk Management in Healthcare?", (25 Nisan 2018), https://catalyst.nejm.org/what-is-risk-management-in-healthcare/. (Erişim Tarihi: 1 Kasım 2019)

[31] *Marsh*, (2015), "Three Key Risks Affecting Insurance Pricing for Health Care Organizations", https://www.marsh.com/us/insights/research/three-key-risks-affecting-insurance-pricing-for-health-care-orgs.html. (Erişim Tarihi: 1 Kasım 2019)

[32] Şahin, Alev; (2018), "Artan siber riskler, sigortacıları canlandırdı", *Fortune Türkiye*, (14 Ocak 2018), https://www.fortuneturkey.com/artan-siber-riskler-sigortacilari-canlandirdi-50378. (Erişim Tarihi: 1 Kasım 2019)

[33] Davis, Jessica; (2019), "Healthcare Cyberattacks Cost $1.4 Million on Average in Recovery", *Health IT Security*, (22 Ocak 2019), https://healthitsecurity.com/news/healthcare-cyberattacks-cost-1.4-million-on-average-in-recovery . (Erişim Tarihi: 1 Kasım 2019)

[34] Davis, Jessica; "What Is Cyber Insurance for Healthcare Organizations?", *Health IT Security*, https://healthitsecurity.com/features/what-is-cyber-insurance-for-healthcare-organizations. (Erişim Tarihi: 1 Kasım 2019)

[35] *STM*, (2017), "2017 Nisan Haziran Dönemi Siber Tehdit Durum Raporu", (Temmuz 2017), https://www.stm.com.tr/documents/file/Pdf/Siber%20Tehdit%20Durum%20Raporu%20Nisan-Haziran%202017.pdf. (Erişim Tarihi: 1 Kasım 2019)

[36] *SağlıkAktüel*, (2016), "Sağlık sektöründe siber risk ve sigorta", (2 Haziran 2016), https://www.saglikaktuel.com/haber/saglik-sektorunde-siber-risk-ve-sigorta-51853.htm. (Erişim Tarihi: 1 Kasım 2019)

[37] *EY*, (2017), "EY's Digital Underwriting Survey - Underwriting transformation in the digital era", https://www.ey.com/Publication/vwLUAssets/ey-2017-Digital-underwriting-survey/$FILE/ey-digital-underwriting-survey-thought-leadership-brochure.pdf. (Erişim Tarihi: 1 Kasım 2019)

thinktech
STM Teknolojik Düşünce Merkezi
http://thinktech.stm.com.tr