# Elektronik Sağlık Kayıtlarının Gizlilik ve Mahremiyeti

**Nalin Turğut[1], Enis Karaarslan[1], Ali Murat Ergin[2], Özgür Kılıç[1]**

[1] Muğla Sıtkı Koçman Üniversitesi, Bilgisayar Mühendisliği Bölümü, Muğla

[2] Ege Üniversitesi, Biyoistatistik ve Tıbbi Bilişim AD

turgutnalin@gmail.com, enis.karaarslan@mu.edu.tr, ali.murat.ergin@gmail.com, ozgurkilic@mu.edu.tr

**Özet:** Bilgi sistemleri sayesinde kişilere ait birçok bilgi erişilebilir hale gelmiş ve kişisel verilerin korunma gereksinimini ortaya çıkarmıştır. Sağlık verisi son derece duyarlı ve kişisel olduğu için sağlık bilgi sistemleri hastanın mahremiyetini korumalıdır. Güvenlik ve gizlilik ile ilgili mekanizmaların eksikliği hastane bilgi sistemlerinde mahremiyet ile ilgili ihlallere sebep olabilir. Bu çalışmada, kişisel veriler, mahremiyet ve gizlilik kavramları; HIPAA standardı ve Avrupa Birliği politikaları kapsamında elektronik sağlık kayıtlarının gizliliğinin ve güvenliğinin nasıl korunması gerektiği açıklanmıştır. Elektronik sağlık kayıtlarının nasıl ve nerelerde tutulduğu modellenerek Türkiye'de bu kayıtların gizlilik ve mahremiyetinin hangi noktada olduğu incelenmiştir.
**Anahtar Sözcükler:** Elektronik Sağlık Kayıtı, Hasta Bilgileri, Gizlilik, Mahremiyet

**Abstract:** Personal information has become accessible as a consequence of information systems and therefore the need for protecting personal information has arosen. Health information systems should protect patient privacy since healthcare information is highly sensitive and personal. Lack of privacy and security mechanisms in healthcare information systems may lead to privacy violations. In this study, first we explain the concepts of personal data, privacy and security. Then we describe how the privacy and security of electronic health records can be established with respect to the HIPAA Privacy and Security Rules and European Union policies. We examine the current status in Turkey regarding the privacy and security of electronic health records through modeling where and how these personal data is stored.
**Keywords:** electronic health record, patient record, confidentiality, privacy

## 1. Giriş

Bilgi teknolojilerinin ortaya çıkmasıyla kağıt ortamdaki sistemlerden mevcut hizmetleri maliyet-etkin bir şekilde veren ve yeni servisler için fırsatlar yaratan bilgi sistemlerine geçiş hızlanmıştır. Bilgi sistemlerinin en önemli getirilerinden birisi de bilgiyi daha erişilebilir yapmalarıdır.

Bir hasta polikliniklerden özel veya kamu hastanelere birçok sağlık kuruluşunda bakım görebilmektedir. Bu bakım sürecinde hastanın kan örneklerinden röntgenine kendisi hakkında birçok bilgi toplanmaktadır. Bu bilgiler kurumların kendilerinde saklanmaktadır. Bunun yanı sıra, bu bilgiler farklı kurumlar arasında paylaşılmaktadır. Eczanelerden sigorta kurumlarına birçok yerde hasta bilgileri birçok kişi tarafından erişilebilmektedir. Bu erişimler sağlanırken verinin bu yeni ortamdaki gizliliği ve güvenliği de dikkatlice ele alınmalıdır. Kişisel veri saklayan bilgi sistemleri; ilgili politikalar, prosedürler, kurallar ve düzenlemelere uyumlu olmak için bilgi güvenliği ve gizliliği ile ilgili meseleleri etkin bir şekilde ele almalıdırlar.

İkinci bölümde kişisel veriler, mahremiyet, şifreleme ve anonimleştirme gibi temel kavramlar ele alınmıştır. Üçüncü bölümde Türkiye'de kişisel veriler kapsamında hastane verilerinin yasal durumu incelenmiştir. Sonrasında Türkiye'de hastane bilgi sistemleri ele alınmış ve hasta verilerine erişim modellenmiştir. Son bölümde

Türkiye'de basına yansıyan olaylar kapsamında bir durum saptaması yapılmıştır.

## 2. Temel Kavramlar

### 2.1. Kişisel Veri, Hassas Veri ve Mahremiyet

Hassas veriler, kişisel verilerin daha fazla korunma uygulanması gereken bir alt kümesi olarak düşünülebilir. İnsanların temel haklarını ve özel yaşamın gizliliğini ihlal edebilecek verilerdir. Sağlık yaşamı ve cinsellik ile ilgili kişisel veriler de hassas veri olarak tanımlanmaktadır [1].

Gizlilik (confidentiality), bilginin yetki verilmemiş kişilerin eline geçmesine ve yetkisiz erişime karşı korunmasını hedefleyen bir servistir. Mahremiyet (privacy), ise özel hayata dair bilgilerin uygun görülen kişiler dışındaki kişilerin görmesinden uzak tutulması durumu, isteğidir[2]. Özel hayat hakkı, uluslararası sözleşmelerle korunan temel bir haktır. Kural olarak dokunulmaz, vazgeçilmez, devredilemez niteliktedir, ancak yasayla sınırlanabilir ama bu sınırlama da hakkın özüne dokunulmayacak şekilde yapılmalıdır [3-14].

Mahremiyet kişinin özlük haklarının gizli olması durumudur. Kişisel verilerin korunması, bilgi güvenliğinin sağlanması ve bireyin özgür hareket etmesi mahremiyet kavramının sağladığı durumlardır. Mahremiyetin korunması için mevzuat yeterli değildir, mahremiyet koruma teknolojileri de kullanılmalıdır [4].

### 2.2. Hasta Verilerinin Mahremiyeti

Mahremiyet kavramı sağlık alanında ilk olarak Hipokrat Yemini 'yle ortaya çıkmıştır. Hipokrat yemininde, "Gerek sanatımın icrası sırasında gerekse insanlarla gündelik ilişkideyken edindiğim bilgileri ortalığa saçmayacağım, bir sır olarak saklayacağım ve kimseye açmayacağım." cümlesi geçer [5]. Hasta bilgileri kişisel veri olarak kabul edilir. Hastaya ait bilgilerin mahremiyetinin sağlanması önemli bir konudur. Hastanın sağlık kayıtları başka amaçlar için kullanılabilir. Hasta, bilgilerinin gizli ve güvenli bir şekilde tutulduğundan emin olmak ister. Bazı hastalar sağlık bilgilerinin birinci derece akrabalarıyla bile paylaşılmasını istemeyebilir. Hastane bilgi sistemlerinde yaşanabilecek güvenlik ve mahremiyet açıkları sonucunda bu bilgileri kendi amaçları için kullanabilecek kişilerin eline geçmesi söz konusudur.

### 2.3. Şifreleme ve Anonimleştirme

Kriptografi, gizli yazma sanatı/bilimidir. Kriptografinin sağladığı en temel servis şifrelemedir. Şifreleme (encryption) ile veriler sadece hedeflenen alıcıların okuyabileceği bir biçime (ciphertext) dönüştürülmektedir. Burada amaç gizliliğin sağlanmasıdır [6].

Anonimleştirme, verilerin gizlenmesi noktasında kişilerin kimliklerini saklamaya yarayan bir yöntemdir[4]. Burada amaç mahremiyetin sağlanmasıdır.

Anonimleştirme ve şifreleme güvenlik araçlarıdır. Bu iki aracın da farklı algoritma ve yöntemle uygulanması mümkündür. Bu yöntemlerin kıyaslanmasındaki başlıca kriterler olarak başarım ve sağlayacakları güvenlik seviyesi verilebilir.

Sistemlere girilirken kullanılan parolalar da Türkçe'de şifre olarak adlandırıldığından, şifreleme kullanılan sistemler derken ülkemizde anlam karışmaları yaşanmaktadır.

### 2.4. Hastane Bilgi Yönetim Sistemleri (HBYS) ve Hasta Verileri

Hasta verileri deyince öncelikle hastanelerde bulunan Hastane Bilgi Yönetim Sistemleri (HBYS) akla gelmektedir. HBYS kompleks sistemlerdir. Şekil 1'de görüldüğü üzere, PACS ve Tele-Tıp olmak üzere birçok alt modülünden söz etmek mümkündür. Üniversite/eğitim ve araştırma hastanelerinde buna ek olarak eğitim amaçlı olarak eklenen modüllerden de söz edilebilir. Bu tür bir sistemde hasta verilerine erişim bölüm 4'de modellenecektir.

Hasta verileri, kişiye ait özel bilgileri ve hastalık bilgilerini kapsar. Her hastane kullandığı otomasyon sistemine göre kayıt tutar. Ancak Sağlık Bakanlığına gönderilen veriler USVS'de tanımlanan veri setleri halinde toplanır ve ana sisteme gönderilir[20].

### 2.5. Web Servisleri ve HL7

Hastane verilerinin farklı modüller veya farklı kurumlar arasında iletiminde iki ana yöntemden söz edilebilir.

**Web servisleri:** SOAP gibi web servisleri kullanılarak HBYS ortamlarında gereksiz bilgi tekrarını engeller. Sadece istenen bilgilerin transferini ve modüllerin Veritabanı Yönetim Sistemiden (VTYS) bağımsız hale gelmesini sağlar.

**HL7 (Health Level 7) protokülü:** Medikal sistemlerin iletişiminde kullanılan bir dünya standartıdır. Version 2.x'e kadar olan iletişimlerde TCP soket ile iletişim kurar ve web servislerine göre yönetimi zordur. Modüllerin VTYS den bağımsız hale gelmesini sağlar. HBYS ortamlarında gereksiz bilgi tekrarını engeller.

### 2.6. HIPAA ve Avrupa Birliği politikaları

HIPAA, 1996 yılında Amerika'da kabul edilen The Health Insurance Portability and Accountability Act'ın kısaltılmasıdır. Yasa, bir standartlar bütünü olarak; Dünya genelinde sağlık sektöründe referans bir güvenlik standardı olarak kullanılmaktadır. HIPAA standartları 3 temel başlıkta incelenmektedir[7].

**İdari Tedbirler:** Sağlık Sistemi içerisindeki, konu ile ilgili idari sorumlunun tanımlanması, organizasyonun uyması gereken prosedürlerin tanımlanması, elektronik ortamdaki bilgileri seviyelendirerek kimlerin, nelere ulaşabileceğinin tanımlanması, organizasyon dışı yüklenici firmaların bu standartlar çerçevesinde rolünün tanımlanarak, sözleşme yapılması, acil durumların tanımlanarak, yapılacakların tanımlanması ve veri bütünlük kontrollerinin yapılandırılmasını içermektedir.

**Fiziksel Tedbirler:** Sağlık bilgilerini içeren ortamlara olan fiziksel erişimlerin, dikkatlice kontrol edilmesi ve izlenmesinin sağlanmasını içermektedir.

**Teknik Tedbirler:** Sağlık Sistemi içerisindeki bilgi kaynaklarına yapılacak siber saldırılara karşı korunması, izlenmesi ve kayıt altına alınması. Veri iletimlerinde gelişmiş şifreleme metotlarının kullanılması, verinin bütünlüğünün garanti edilmesi, düzenli risk analizlerinin gerçekleştirilerek, organizasyon risk yönetiminin belgelenmesini içermektedir.

### 2.7. Ulusal Sağlık Bilgi Sistemi

Ulusal Sağlık Bilgi Sistemi (USBS), Türkiye'de sağlık hizmeti sunan kurum ve kuruluşlardan sağlık hizmeti alan kişilerin sağlık bilgileri ile bu kurumlar ve kuruluşlar ile ilgili insan gücü, taşınır, taşınmaz, idari ve mali verilerin merkezi bir yapı altında toplandığı bir sistemdir.

Ulusal Sağlık Bilgi Sisteminin temel amaçları şu şekilde özetlenmiştir[11]:

- Sağlık veri standardizasyonunun sağlanması
- Veri analiz desteği ve karar destek sistemleri oluşturulması
- e-Sağlık paydaşları arasında veri akışının hızlandırılması
- Elektronik kişisel sağlık kayıtlarının oluşturulması
- Kaynak tasarrufunun sağlanması ve verimliliğin artırılması
- Bilimsel çalışmalara destek verilmesi
- e-Sağlık kavramının ulusal anlamda benimsenmesinin hızlandırılması

USBS kapsamında Sağlık-NET projesi 2009 yılı başında itibaren hizmete girmiştir.
Sağlık-NET Sistemi üç ana bileşenden oluşmaktadır[11]:

- **Ulusal Sağlık Veri Sözlüğü (USVS**); sağlık kurum ve kuruluşlarından toplanan verilerin tanımlandığı ve Sağlık-NET ile entegre olan tüm sağlık bilgi

sistemlerince referans olarak kullanılan veri kümesidir.

- **Sağlık Kodlama Referans Sunucusu (SKRS);** USVS kapsamında toplanan verilerde kullanılan kodlama kullanılan alanlarda alabilecek değerlerin web servisleri paylaşıldığı referans sistemidir.
- **Web Servisleri;** USVS'de tanımlanmış verilerin gönderimi için oluşturulmuş entegrasyon noktalarıdır.

Sağlık-NET projesinde mesajlaşma standardı olarak HL7 V3 kullanılmıştır[12]. Hastane Bilgi Sistemleri kendi veritabanında topladığı verileri Sağlık-NET web servislerini kullanarak göndermek için Sağlık Bakanlığı'nca tarif edilen HL7 V3 uyumlu mesaj yapısına çevirmelidir.

## 3. Türkiye'de Kişisel Veriler Kapsamında Hastane Verilerinin Yasal Durumu

Türkiye'de kişi mahremiyetini korumak için yasalarda bazı maddeler bulunmaktadır, ancak bunlar kişi mahremiyetini korumak için yeterli değildir. Türkiye'de bir yasal düzenleme gereksinimi ilk olarak 2003 yılında Avrupa Birliği'ne Katılım Ortaklığı Belgesi'nde kişisel verilerin korunmasıyla ilgili özel bir düzenleme yapılması amacından dolayı ortaya çıkmıştır[8]. 12 Eylül 2010 tarihindeki referandum sonrasında 1982 Anayasası'na "Özel Hayatın Gizliliği" başlıklı 20. maddeye eklenen 3. Fıkra ile kişisel veriler koruma altına alınmıştır: "Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir."[9] Bununla birlikte Türk Medeni Kanunu'nda 'Kişilik Haklarının Korunması'nı düzenleyen 23. ve 24. maddeleri uyarınca da, kişisel veriler korunmaktadır. 5237 sayılı Türk Ceza Kanunu'nun Kişisel Verilerin Kaydedilmesi başlıklı 135. maddesinde kişisel verilerin hukuka aykırı olarak kaydedilmesi; 136. maddesinde ise kişisel verileri hukuka aykırı olarak yayma veya ele geçirme fiili suç olarak düzenlenmiştir.

"Kişisel Verilerin Korunması Hakkındaki Kanun Tasarısı" adlı yasa tasarısı ile kişi mahremiyetinin daha fazla korunması hedeflenmiştir. Bu yasa tasarısı birçok kez TBMM'ye sunulmuştur. En son 2014 yılında Meclis'e sunulan tasarı henüz yasalaşmamış ve resmi gazetede yayınlanmamıştır[10]. Tasarının tüm maddeleri açık olmayacak, ancak herhangi bir hastaya ait bilgiler işlendiğinde, hastanın kendisi bundan haberdar edilecek diye belirtiliyor. Bu yasanın kanunlaşmasıyla yasalardaki mahremiyet hakkı boşluğu biraz da olsa doldurulmuş olacaktır. Tasarıya göre Kişisel Verileri Koruma Kurulu kurulacak ve Bakanlar Kurulu tarafından seçilmiş üyelerden oluşacaktır. Bu kurulun görevleri yasa tasarısının 31. maddesinin 1. fıkrasında belirtilmiştir. Bir başka maddede ise "Kişilerin ırk, siyasi düşünce, felsefi inanç, din, mezhep veya diğer inançları, dernek, vakıf ve sendika üyeliği, sağlık ve özel yaşamları ve her türlü mahkûmiyetleri ile ilgili kişisel veriler işlenemez"[18] cümlesi ile verilerin mahremiyetinden bahsedilmektedir.

## 4. Hasta Verilerine Erişimin Modellenmesi

Hasta verilerine erişimi modellemek istediğimizde, Türkiye'deki hasta bilgi sisteminin ana elemanları olarak aşağıdakilerden söz etmemiz mümkündür:

- Sosyal Güvenlik Kurumu (SGK)
- Sağlık Bakanlığı (SB)
- Hastaneler: Özel, Devlet, eğitim ve araştırma veya üniversite hastaneleri, poliklinikler
- Eczaneler
- İlaç firmaları: Hasta bilgilerine anonim olarak da olsa ulaşmak isteyen kurumlar
- Özel ve diğer kamu sigorta kurumları (Sandıklar, TSK, vb.)
- Sigorta Firmaları: Özel sigorta birimleri sağlık kurumları ile yaptıkları sözleşme kapsamında tek taraflı bilgi aktarımı ile yapılmaktadır.
- Adli ve İdari Kolluk Makamları: Mahkemelerden hastalara ait tetkik

ve ilaç/malzeme geçmişi bilgileri dökümü istekleri gelebilmektedir. MİT ya da Emniyet Müdürlüğü'nden hastaneye başvuru yapan bazı hastalar hakkında bilgi istenebilmektedir.

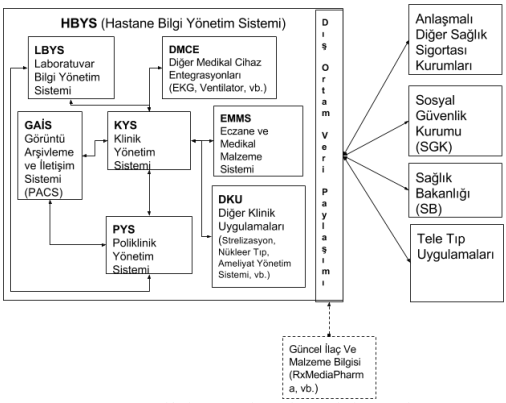
Kurum dışından hizmet veren firmalar da bu hasta verilerine erişebilmektedir. Özellikle biyomedikal cihazlar için dışarıdan alınan bakım hizmetlerinde, hastalara ait verilerinin gizliliği ve mahremiyeti riske atılmaktadır. Bu firmaların verilere erişiminin denetlenmesi ve düzenlenmesi gerekmektedir [13].

Bilgiye erişebilecek insanlar her kurumda farklı olmakla birlikte, öncelikle hastanelerdeki ana elemanları şu şekilde özetlemek mümkündür:

- İdari Birim Çalışanları:
  - Başhekim ve yardımcıları
  - Finans sistemleri personeli (Döner Sermaye Saymanlığı)
  - Malzeme planlama ve tedarik personeli (Ayniyat, Satınalma)
  - Bilgi İşlem Personeli (Sistem ve veritabanı yöneticileri, Yazılım destek personeli)
- Sağlık Çalışanı: Tıbbi sekreter, hemşire/ebe, Sağlık memuru, memur, sağlık teknisyeni/ teknikeri[19], Eczacı
- Tıbbi görevli: Doktor, hemşire

HBYS kullanan sağlık hizmeti veren kurumlarda bilgi güvenliğinin sağlanması gereklidir. Günümüzde HBYS yazılımları, kurum içinde çalışan personelin bilgilere erişimi için yukarıdaki maddelerde tanımlanmış olan çalışma alanlarına göre belirlenmiş rol tabanlı güvenlik algoritmaları kullanmaktadırlar. Ayrıca kritik bilgilerin tutulduğu veritabanı tablolarında verilerin okunması dışında veri girişi, değişikliği ve silinmesi operasyonlarını sadece VTYS yöneticisinin ulaşabileceği zaman damgalı raporlama mekanizmaları da kullanılmaktadır. Elektronik sağlık kayıtlarının tutulmasında en önemli yaklaşımlardan biri de, girilen veri yanlış veya eksik dahi olsa fiziksel silinmesini engellemek gerekliliğidir. HBYS yazılım algoritması, girilen veri yanlış veya eksik olsa bile bu kayıtın fiziksel silinmesi yerine geçersizleştirilmesini ve yeniden doğru kayıtın girilmesi yönünde olmalıdır.

Bir hastane içindeki ve hastaneden dış kurumlara iletilen verileri incelemek istediğimizde, medikal ve finansal (SGK) süreçleri içeren hastane modeli Şekil 1'de verilmiştir. Bu şekilde idari süreçlere ait modüller yer almamaktadır.




**Şekil 1.** Hastane Bilgi Yönetim Sisteminin Veri Paylaşımı Modeli

Hasta verilerinin iletiminde kullanılan Bilgi İletişim Standartlarını iki ana başlıkta incelemek mümkündür:

- **İç Ortam (HBYS) veri iletişimi:** HBYS Modüller (KYS, PYS, LBYS, GAİS, EMMS, DCME, DKU) arası iletişim web servisleri veya HL7 protokolü ile olmalıdır. Bununla beraber modüller aynı yazılım üreticisi tarafından kodlanmış ise modüller arası iletişim ortak VTYS üzerinden olabilir. Farklı yazılım firmaları tarafından yazılan modüller için firma hasta ve hastane bilgi güvenliği kurallarını sözleşmede imzalar. Örnek sözleşme metni 4.1'de verilmiştir.

- **Dış Ortam Veri İletişimi:** Şekil 1'de gözüken dış birimlerle iletişimde genellikle SSL Web servisleri (SOAP) aracılığıyla yapılması tercih edilmektedir.

**4.1 Örnek Sözleşme Metni: Gizlilik Şartı**

Firma iş bu sözleşme ile üstlenmiş olduğu bakım onarım işlerinin ifası sırasında vakıf olabileceği hasta (hasta hakları yönetmeliğinin 23. maddesi hükmü gereği) ve hastaneye ilişkin her türlü bilgi, istatistik veri ve kayıtları Hastane Başhekimliğinin önceden yazılı izni olmaksızın hiçbir amaç için hiçbir ortamda kullanamaz, depolayamaz, kopyalayamaz, yayınlayamaz ve 3. kişilerle paylaşamaz. Aksi davranış firma açısından ilgili yasal düzenlemeler uyarınca cezai ve hukuki müeyyideyi gerektireceği gibi İdareye sözleşmeyi ihbarsız olarak fesih hakkı tanır.

**4.2. Hastanelerin Tuttuğu Veriler**

Hastaneler verilerini kendilerine özgü bir şekilde modelleyip tuttuklarından burada bir standarttan söz edilememektedir. Birçoğunda kişisel verileri şifrelenmeden tutulmakta ama kişi bazlı erişim politikaları ile hangi kullanıcıların hangi bilgileri görebileceği kısıtlanmaktadır. Bu da farklı hastane bilgi sistemlerinde farklı olmaktadır.

Hastanelerin öncelikle ağ güvenliklerini sağlamaları ve bu bilgilere erişimi denetlemeleri gerekmektedir. Hastanelerin elektronik sağlık verilerini korumak için daha ayrıntılı güvenlik süreçlerini devreye alması gerekmektedir. Bu tür önlemler ne yazık ki birçok hastanede alınmamaktadır [13].

**4.3. İletilen Veriler**

İç Ortamda İletilen Verilerin, özellikle web servisleri kullanımında bazı hastane uygulamalarındaki URL yapılarında TC kimlik numarası gibi kişisel verilerin açık olarak iletildiği gözlenmiştir.

Sağlık bakanlığına iletilen verilerin bazıları (bunlar tanımlı) şunlardır [15]:

- Hasta muayene bilgisi
- Hastaya verilen malzeme/ilaç bilgisi
- Hasta Laboratuvar sonuç bilgisi
- Hasta patoloji sonuç bilgisi
- 15-49 Yas kadın izlem verisi
- Ağız ve Diş sağlığı bilgisi
- Gebelik izlem bilgisi
- Anne ve bebek sağlık verisi
- Kadına yönelik şiddet verisi
- Aşı Takip Sistemi
- Bulaşıcı hastalıklara ait veri setleri
- İntihar vakalarına ait bilgiler

Sosyal Güvenlik Kurumuna gönderilen verilerin bazıları şunlardır [16]:

- **Hasta kabul Sistemi:** Bu aşamada sağlık kurumuna başvuran hastanın sigortalılık durumu kontrol edilerek ona provizyon kodu döndürülür. Provizyonu onaylanmışsa bir takip numarası alınarak bir birime sevk başlatılır. Bir hasta birden fazla takip numarasına sahip olabilir.
- **Hizmet kayıt:** Sağlık kurumunda ayaktan ya da yatarak tedavi olan hastaların tüm tetkik, tedavi, ilaç ve malzeme bilgileri toplanır.
- **Fatura bilgisi kayıt:** Sağlık kurumuna başvurmuş hastalar için onların hizmet kayıtlarının toplamına ait kuruma ödenmek üzere elektronik fatura bilgisi oluşturulur.
- **Rapor bilgisi kayıt:** Hastaların uzun dönemli tedavilerine temel oluşturan ve ülke çapında her sağlık kurumunda da geçerli olan kullanacağı ilaç/malzeme, maluliyet, tedavi ve iş görmezlik raporlarının oluşturulmasını sağlar.

**4.4. Verilerin veya İletişimin Şifrelenmesi**

Her hastanede kullanılan veritabanları ve yazılımları bağımsız olduğu için, hasta verilerinin genelde şifrelemeden tutulduğu düşünülmektedir. Bu da sistem yöneticisi, yazılımcı gibi kullanıcıların sistemdeki bilgilere ulaşması demektir. Şifreleyerek tutmanın birkaç olumsuz etkisi söz konusudur.

- Tek bir tane şifreleme standardının olmaması veya şifreleme yönteminin yetkilendirilmiş bir organizasyon

tarafından belirlenmemiş olması hastaneyi belli bir yazılıma ve/veya veritabanına mecbur edebilir. Bu da hastanenin yazılımını veya veritabanını değiştirmede kısıtlanmasına ve belli yazılım ve veritabanı firmalarına bağlanmasına yol açacaktır.

- İlişkisel veritabanı sistemlerinde tüm verilerin şifrelenmesi şifreleme ve şifre çözme aşamalarında performans kayıplarına yol açmaktadır. Sağlık kurumları doğaları gereği hizmetin sürekliliğini sağlamak üzere sistemlerini OLTP (On-Line Transaction Processing) sistemleri kullanırlar. Bu nedenle şifreleme ve şifre çözme işlemleri vakit kaybına bu da hasta işlemlerinde uzayan kuyruklara neden olmaktadır.

Kurumlar arasındaki (dış ortam) veri iletişiminin SSL Web servisleri (SOAP) ile yapılması tercih edilmektedir ama bütün iletişimin böyle olduğu konusunda bir bilgimiz bulunmamaktadır. Kurumun iç ortam veri iletişimi performans gözetilerek muhtemelen şifresiz yapılmaktadır.

### 4.5. Verilerin Paylaşımında Yaşanan Sorunlara Örnekler

Elektronik sağlık kayıtlarının paylaşımında mahremiyetin gözetildiğine dair herhangi bir bilgi bulunmamaktadır. Hastane verilerinin anonimleştirilerek ilaç firmalarına satıldığı iddia edilmektedir[17]. Gerçekten anonimleştirmenin olup olmadığı bir yana, hangi alanların anonimleştirildiği de önemli bir bilgidir. Ayrıca araştırmalarımız esnasında yaptığımız görüşmelerde aşağıdaki olayların yaşandığı iddia edilmektedir:

- Hasta verilerinin bilimsel araştırmalarda kullanılması için anonimleştirilmeden paylaşılması,
- Muayene sonrasında hastalara vakaları ile ilgili reklam sms'lerinin gönderilmesi,
- Hasta verilerinin yedeklendiği DVD'lerin fiziksel güvenliklerinin sağlanmadan tutulmasıdır.

## 5. Sonuç ve Öneriler:

Hasta verilerini işleyen birçok süreç ve bu verilere erişim sağlayan birçok kurum bulunmaktadır. Elektronik sağlık kayıtları kurumlar arasında taşınırken şifrelenmekte ama kurumların iç süreçlerinde bu tür bir şifrelemeye dair bir bilgi bulunmamaktadır. Bu tür bir şifrelemenin yapılmama nedeni olarak sistemlerin yavaşlaması ve belirli bir ürüne bağımlı olmama yaklaşımı gösterilebilir.

Elektronik sağlık kayıtlarında gizlilik ve mahremiyetinin kabul edilebilir bir seviyede yapılması teknik olarak mümkündür. Anonimleştirme yapılırken gelişmiş algoritmaların kullanılması ve mahremiyet seviyesinin açıklanması gereklidir.

Hasta verileri özellikle bilimsel araştırmalar için paylaşılmak durumundadır. Bu durumda verinin mahremiyetinin sağlanması gerekmektedir. Mahremiyetin sağlandığına dair herhangi bir bilgiye ulaşılamamıştır.

Hasta verilerine yetkisiz erişimin olması durumunda kurumlara yasal yaptırımlar uygulanmalıdır. Hastane bilgi sistemlerinde fiziksel güvenlikten başlayarak, siber güvenliğe kadar ayrıntılı önlemlerin alınması gerekmektedir. Bu konudaki ayrıntılı incelemeyi sonraki çalışmalarımızda iletmeyi hedeflemekteyiz.

## Kaynaklar

[1] Kaya, Cemil. "Avrupa Birliği Veri Koruma Direktifi Ekseninde Hassas (Kişisel) Veriler ve İşlenmesi." İstanbul Üniversitesi Hukuk Fakültesi Mecmuası 69.1-2 (2011): 317-334.

[2] Kaufman, Charlie, Radia Perlman, and Mike Speciner. Network security: private communication in a public world. Prentice Hall Press, 2002.

[3] Korkmaz, Ali. "İnsan Hakları Bağlamında Özel Hayatın Gizliliği Ve Korunması.", 2014

[4] Karaarslan, Enis vd. (2014), Çevrimiçi Mahremiyet: Teknik ve Hukuksal Durum İncelemesi, Türkiye'de İnternet Konferansı Bildirisi, İzmir.

[5] Hipokrat Yemini, 2014, http://tr.wikipedia.org/wiki/Hipokrat_Yemini

[6] Kaufman, Charlie, Radia Perlman, and Mike Speciner. *Network security: private communication in a public world*. Prentice Hall Press, 2002.

[7] HIPAA 2015, https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act

[8] AB Katılım Ortaklığı Belgesi 2003 http://www.ab.gov.tr/files/AB_Iliskileri/AdaylikSureci/Kob/Turkiye_Kat_Ort_Belg_2003.pdf

[9] 1982 Anayasası Madde 20

[10] Kanunlar Genel Müdürlüğü TBMM İhtisas Komisyonlarında Bulunan Kanun Tasarıları http://www.kgm.adalet.gov.tr/Tasariasamalari/Tbmmkms/TbmmKom.html

[11] Türkiye Sağlıkta Dönüşüm Programı Değerlendirme Raporu (2003-2011), http://sbu.saglik.gov.tr/Ekutuphane/kitaplar/SDPturk.pdf

[12] Y. Kabak , A. Dogac , I. Kose , N. Akpinar , M. Gurel , Y. Arslan , H. Ozer , N. Yurt , A. Ozcam , S. Kirici , M. Yuksel and E. Sabur "The use of HL7 CDA in the national health information system (NHIS) of Turkey", 9th Int. HL7 Interoperability Conf. (IHIC\'08)

[13] Namoglu, Nihan, and Yekta Ulgen. "Network security vulnerabilities and personal privacy issues in healthcare information systems: A case study in a private hospital." Biomedical Engineering Meeting (BIYOMUT), 2014 18th National. IEEE, 2014.

[14] Sevimli, K. Ahmet, İşçinin Özel Yaşamına Müdahalenin Sınırları, Legal Yayıncılık, İstanbul, 2006.

[15] Sağlık bakanlığı web servisleri veri paketleri, http://sys.sagliknet.saglik.gov.tr/dokumanonline/

[16] Sosyal Güvenlik Kurumu MEDULA web servisleri kılavuzu, http://www.sgk.gov.tr/wps/wcm/connect/0d00b6b7-09aa-41dd-8417-31b069ac76ef/MEDULA_Kullanim_Kilavuzu_201501014.pdf?MOD=AJPERES

[17] Sağlık Bakanlığı SGK Bilgilerinin Satıldığını Doğruladı, Muhalefet e-dergi, 25 Ekim 2014, http://muhalefet.org/haber-saglik-bakanligi-sgk-bilgilerinin-satildigini-dogruladi-23-12498.aspx

[18] Kişisel Verileri Koruma Kanunu Tasarısı, Madde 7, 1.Fıkra http://www.kgm.adalet.gov.tr/Tasariasamalari/Tbmmkms/Tbmmkom/ki%C5%9Fisel%20veriler.pdf

[19] Işık, O., and Mahmut Akbolat. "Bilgi Teknolojileri ve Hastane Bilgi Sistemleri Kullanımı: Sağlık Çalışanları Üzerine Bir Araştırma The Use of Information Technology and Hospital Information Systems: A Study on Health Employees." Bilgi Dünyası 11 (2010): 365-89.

[20] T.C. Sağlık Bakanlığı Ulusal Sağlık Veri Sözlüğü, http://www.saglik.gov.tr/TR/belge/1-4095/ulusal-saglik-veri-sozlugu-usvs.html