SAĞLIK BİLGİ SİSTEMLERİ GENEL MÜDÜRLÜĞÜ -
STANDART VE AKREDİTASYON DAİRESİ BAŞKANLIĞI
03/12/2021 16:23 - E-75730711 - 719 - 465
00153602111

T.C.
SAĞLIK BAKANLIĞI
Sağlık Bilgi Sistemleri Genel Müdürlüğü

Sayı : E-75730711 02.12.2021
Konu : Sağlık Bilgi Yönetim Sistemlerinde Yetki Matrisi Oluşturma ve Hasta Mahremiyeti Hk.

DAĞITIM YERLERİNE

İlgi : a) Kişisel Verileri Koruma Kurulunun 31.01.2018 tarihli ve 2018/10 sayılı Kararı.
b) Kişisel Verileri Koruma Kurulunun 06.08.2021 tarihli ve 2021/761 sayılı Kararı.
c) 6698 sayılı Kişisel Verilerin Korunması Kanunu.
ç) Bakanlığımız Bilgi Güvenliği Politikaları Kılavuzu.

İlgi (b) Karar'da, ilgili kişinin boşanma davası devam eden eşi ile müşterek çocuklarının sağlık ve epikriz raporlarının ilgili kişinin eşinin vekili ile vekilin vekaletnamesinde bu konuda özel bir yetkisinin bulunmadığı halde paylaşıldığı, bu kapsamda ilgili kişinin boşanma davası devam eden eşi ile müşterek çocuklarının kişisel verilerinin gerektiği gibi korunmadığı ve bu verilerin üçüncü kişiler ile paylaşılması sebebiyle Kişisel Verileri Koruma Kurumuna Bakanlığımız aleyhine başvurduğu ifade edilmekte ve hastane otomasyon sisteminde görüntüleme de dahil olmak üzere erişim loglarının tutulması için sistemin güncellenmesinin, hastanedeki tüm doktor ve hasta kayıt personelinin tüm hasta kayıtlarına erişmesi yerine yalnızca hastaların muayene ve tedavisi ile ilgili olarak çalışan personelin ve doktorların söz konusu verilere erişmesine dair yetki matrisinin net şekilde ortaya konulmasının ve hastane otomasyon sisteminden çıktı alma hususunda sadece belirli personele yetki verilmesinin güvenlik risklerini azaltacağı göz önünde bulundurularak, hasta kayıt örneklerinin alınması konusunda belirli prosedürlerin ve yetkili personelin belirlenmesinin gerektiği ifade edilmektedir.

Anılan karar doğrultusunda;

1- "Özel nitelikli kişisel veriler" ilgi (c) Kanun'un 6 ncı maddesinde; "kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik verileri" olarak tanımlanmıştır.

"Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler" başlıklı ilgi (a) Karar'da: *"Özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar, elektronik ortamda ise verilerin üzerinde gerçekleştirilen tüm*

Üniversiteler Mah. 6001. Cad. No: 9 06800 Bilkent, Ankara Bilgi için: Av. Bilgenur KARA
Telefon No: 0 (312) 471 83 50
e-Posta: bilgenur.kara@saglik.gov.tr İnternet Adresi: https://sbsgm.saglik.gov.tr
Kep Adresi: sb@hs01.kep.tr

hareketlerin işlem kayıtlarının güvenli olarak loglanması gerektiği" belirtilmiştir. İlgi (ç) Kılavuz'da *"Kişisel sağlık kayıtlarının (tüm tetkik sonuçları, hasta dosyaları, barkodlar, gözlem formları vb.) özel nitelikli kişisel veri kategorisinde olduğu ve 6698 sayılı Kanun ile özel koruma uygulanması gerektiği her zaman dikkate alınır."* ifadesi, *"Özel nitelikli kişisel verilere (kişisel sağlık verileri) erişim için KVKK'nın 2018/10 sayılı kararında belirtilen teknik ve idari tedbirlerin alınmış olması gerekir."* ifadesi ve *"KVKK'nın 2018/10 sayılı Kararı uyarınca özel nitelikli kişisel verilerin işlendiği yazılımlarda veriler üzerinde gerçekleştirilen tüm hareketlerin iz kayıtlarının bir başka ortamda güvenli olarak saklanması gerekir."* ifadesi yer almaktadır.

İlgi (b) Karar'da; ilgi (a) Karar ve ilgi (ç) Kılavuz kapsamında veriler üzerinde gerçekleştirilen tüm hareketlerin işlem kayıtlarının güvenli olarak loglanması gerektiğinin belirtildiği ancak somut olayın gerçekleştiği hastanedeki Sağlık Bilgi Yönetim Sisteminde (SBYS) sadece ekleme, silme ve değiştirme işlemlerinin log kaydının tutulduğu, hasta bilgilerinin görüntülenmesinin log kaydının tutulmadığının ifade edildiği bu kapsamda sadece özel nitelikli kişisel veriler değil tüm kişisel veriler açısından kullanılan teknik bir tedbir olan erişim log kayıtlarının tutulmasının önemli bir eksik olduğu belirtilmiştir. Bu doğrultuda kişisel verilerin güvenliğinin sağlanması açısından önemli bir teknik tedbir olarak SBYS'lerde görüntüleme de dâhil olmak üzere tüm erişim loglarının tutulması için sistemin güncellenmesi gerekmektedir.

2- İlgi (a) Karar'da *"Özel nitelikli kişisel verilerin işlenme süreçlerinde yer alan çalışanlara yönelik olarak, verilere erişim yetkisine sahip kullanıcıların yetki kapsamlarının ve sürelerinin net olarak tanımlanması ve periyodik olarak yetki kontrollerinin gerçekleştirilmesi"* gerektiği belirtilmiştir. İlgi (b) Karar'da hastanedeki tüm poliklinik hasta kayıt personeli ve doktorların tüm hastaların dosyalarını görme yetkisine sahip olmasının veri işlemenin amaçla bağlantılı, sınırlı ve ölçülü olmasına aykırı olduğu, kimin hangi veriyi görüntülediği noktada log kaydı tutulmadığı için herhangi bir kontrolün de mümkün olmadığı değerlendirilmiş, bu bakımdan hastanedeki tüm doktor ve hasta kayıt personelinin tüm hasta kayıtlarına erişmesi yerine, hastaların muayene ve tedavisi ile ilgili olarak çalışan personelin ve doktorların söz konusu verilere erişmesinin uygun olabileceği, veri sorumlusunun kimlerin hasta verilerini görüntüleyebileceğine dair yetki matrisini oluşturmak suretiyle olası hukuka aykırı veri işlemelerin önüne geçilebileceği bu kapsamda doktorların sadece kendisinde kayıtlı hastalara hizmet vermedikleri, planlı veya aniden gelişen durumlarda başka hastalara da hizmet verdikleri, sağlık hizmetlerinin yoğun ekip çalışması gerektirmesi ve aciliyet arz eden durumların da dikkate alınabileceğinin değerlendirildiği belirtilmiştir.

Bu doğrultuda hastanedeki tüm doktor ve hasta kayıt personelinin tüm hasta kayıtlarına erişmesi yerine yalnızca hastaların muayene ve tedavisi ile ilgili olarak çalışan personelin ve doktorların söz konusu verilere erişmesine dair yetki matrisinin net bir şekilde ortaya konulması gerekmektedir.

Üniversiteler Mah. 6001. Cad. No: 9 06800 Bilkent, Ankara Bilgi için: Av. Bilgenur KARA
Telefon No: 0 (312) 471 83 50
e-Posta: bilgenur.kara@saglik.gov.tr İnternet Adresi: https://sbsgm.saglik.gov.tr
Kep Adresi: sb@hs01.kep.tr

T.C.
SAĞLIK BAKANLIĞI
Sağlık Bilgi Sistemleri Genel Müdürlüğü

3- İlgi (b) Karar'da SBYS üzerinden çıktı alma noktasında sadece belirli personele yetki verilmesinin güvenlik risklerini azaltacağı göz önünde bulundurulduğunda, hasta kayıt örneklerinin alınması konusunda belirli birtakım prosedürlerin ve yetkili personelin belirlenmesinin önemi belirtilmiştir.

Bu kapsamda SBYS üzerinden hasta kayıt örneklerinin alınması konusunda belirli bir prosedür oluşturularak yetkili personelin belirlenmesi gerekmektedir.

Bilgilerini ve gereğini arz/rica ederim.

Dr. Mustafa Mahir ÜLGÜ
Bakan a.
Sağlık Bilgi Sistemleri Genel Müdürü V.

Ek:
1- İlgi (a) Karar (2 Sayfa)
2- İlgi (c) Kanun (18 Sayfa)
3- İlgi (ç) Kılavuz (225 Sayfa)

Dağıtım:
Gereği:
81 İl Valiliğine (İl Sağlık Müdürlükleri)
KTS'de Kayıtlı SBYS Üreticilerine

Bilgi:
Halk Sağlığı Genel Müdürlüğüne
Kamu Hastaneleri Genel Müdürlüğüne
Sağlık Hizmetleri Genel Müdürlüğüne

Üniversiteler Mah. 6001. Cad. No: 9 06800 Bilkent, Ankara
Telefon No: 0 (312) 471 83 50
e-Posta: bilgenur.kara@saglik.gov.tr İnternet Adresi: https://sbsgm.saglik.gov.tr
Kep Adresi: sb@hs01.kep.tr
Bilgi için: Av. Bilgenur KARA