

KİŞİSEL SAĞLIK VERİLERİNİN İŞLENMESİ VE VERİ MAHREMİYETİNİN SAĞLANMASI HAKKINDA YÖNETMELİK TASLAĞI

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1- (1) Bu Yönetmeliğin amacı, kişisel sağlık verilerinin mahremiyetini sağlamak, kişisel sağlık verilerinin işlenmesi ve bu verileri işleyecek gerçek ve tüzel kişilerin uyacakları esas ve usulleri belirlemektir.

Kapsam

MADDE 2- (1) Bu Yönetmelik;

- a) Kişisel sağlık verileri işlenen gerçek kişileri,
- b) Kişisel sağlık verilerini otomatik veya otomatik olmayan araçlarla kısmen veya tamamen işleyen Sağlık Bakanlığı ve bağlı kuruluşları ile sağlık ve sigorta hizmeti sunan diğer kamu ve özel kurum ve kuruluşlar ile kişileri,
- c) Sağlık hizmet sunucularına ait bilgi işlem sistemleri yazılım ve donanımı ile dosyalama sistemi gibi hizmetleri sunan gerçek ve tüzel kişileri,

kapsar.

Dayanak

MADDE 3- (1) Bu Yönetmelik, 663 sayılı Sağlık Bakanlığı ve Bağlı Kuruluşlarının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 8 inci maddesinin birinci fıkrasının (j) bendi ile 47 nci maddesine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4- (1) Bu Yönetmelikte geçen;

- a) Alıcı: Paylaşım açılacak verilerden yararlanan veri sorumlusu, veri işleyen ve üçüncü kişileri,
- b) Anonim hale getirme: Kişisel sağlık verilerinin belirli veya kimliği belirlenebilir bir gerçek kişiyle ilişkilendirilemeyecek hale getirilmesini,
- c) Bakanlık: Sağlık Bakanlığını,
- ç) Çocuk: Rıza açıklama yeteneğine sahip 18 yaş altındaki herhangi bir kişiyi,
- d) İlgili kişi: Kişisel sağlık verileri işlenen gerçek kişiyi,
- e) Kişisel sağlık verisi: İlgili kişinin kimlik ya da kimliğini belirlenebilir kılan verileri ile birlikte fiziksel, ruhsal ve sosyal durumuna ilişkin tüm verilerini,
- f) Otomatik olmayan: Kağıt tabanlı,
- g) Otomatik: Bilgisayar tabanlı,
- ğ) Rıza: İlgili kişilerin, yazılı veya elektronik ortamda kişisel sağlık verilerinin işlenmesine özgür iradesiyle verdiği ispatlanabilir kabul beyanını,
- h) Sır saklama yükümlülüğü bulunan kişi: Kişisel sağlık verilerinin işlenmesinde doğrudan veya dolaylı görev alan kişileri,
- ı) Üçüncü kişi: Veri sorumlusu, veri işleyen ve ilgili kişi haricinde verinin açıklandığı, paylaşıldığı yurt içi veya yurt dışı kamu ve özel kurum ve kuruluş ile kişiyi,
- i) Veri işleyen: Veri sorumlusunun verdiği yetkiye dayanarak, onun adına kişisel sağlık verilerini işleyen gerçek ve tüzel kişiyi,
- j) Veri kayıt sistemi: Kişisel sağlık verilerine ulaşımı kolaylaştıracak şekilde belirli kriterlerle yapılandırılmış her çeşit kayıt sistemini,
- k) Verilerin işlenmesi: Kişisel sağlık verilerinin otomatik veya otomatik olmayan araçlarla tamamen veya kısmen elde edilmesi, toplanması, kaydedilmesi, depolanması, muhafaza

edilmesi, paylaşılması, silinmesi, yok edilmesi, değiştirilmesi, yeniden düzenlenmesi, tehlike altındaki kişilere veya veri sorumlusuna açıklanması, yayımlanması, elde edilebilir hale getirilmesi, sınıflandırılması veya kullanılmasının engellenmesi gibi veriler üzerinde gerçekleştirilen her türlü işlemi,

İ) Veri sorumlusu: Mevzuatla tanımlanmış görevi kapsamında kişisel sağlık verilerinin amaca uygun işlenmesinde şartları ve araçları belirleyen, veri kayıt sisteminin kurulmasını ve/veya yönetimini sağlayan gerçek ve tüzel kişileri, ifade eder.

İKİNCİ BÖLÜM

Kişisel Sağlık Verilerinin İşlenmesi ve Paylaşım Esasları

Kişisel sağlık verilerinin işlenme esasları

MADDE 5–(1) Kişisel sağlık verileri, mevzuatla belirlenen görev alanına ve toplanma amacına uygun, sınırlı, ölçülü, doğru, tam, tutarlı ve güncel şekilde hukuka ve dürüstlük kurallarına uygun olarak işlenebilir.

(2) Kişisel sağlık verileri; koruyucu hekimlik, tıbbi teşhis, tedavi ve bakım veya rehabilitasyon hizmeti gibi kişiye özel ya da toplum sağlığı, sağlık politikalarının geliştirilmesi, sağlık hizmetlerinin yönetimi ve planlanması, finansmanı, sağlık sigortacılığı, bilimsel araştırma ve istatistik gibi toplumsal amaçlarla bu Yönetmelik hükümlerine uygun şekilde işlenebilir. Bu kapsamda işlenen veriler yalnızca anonim hale getirilerek yayımlanabilir.

(3) İkinci fıkrada belirtilen haller dışında kişisel sağlık verilerinin işlenebileceği durumlar şunlardır:

a) İlgili kişinin açık rızasının bulunması. İlgili kişinin rıza veremeyecek durumda olması durumunda yasal temsilcisinin; çocuklarda kendi rızasının yanı sıra ana ve babasının veya yasal temsilcisinin rızası alınır.

b) İlgili kişinin sağlık durumunun diğer kişileri veya toplum sağlığını tehdit etmesi halinde. Bu durumda Bakanlık veya bağlı kuruluş yetkilisi izniyle tehlike altındaki kişilerle ve ilgili kurumun yetkilileri ile paylaşım yapılır.

c) Bir hakkın tesisi, icrası veya korunması için paylaşımın kanunen zorunlu olması.

ç) Fiili imkansızlık nedeniyle rızasını açıklayamayacak durumda bulunan veya rızasına hukuki geçerlilik tanınmayan kişinin, kendisinin veya bir başkasının hayatı ya da beden bütünlüğünün korunması için zorunlu olması.

d) Kişisel sağlık verilerinin ilgili kişinin kendisi tarafından alenileştirilmiş olması.

(4) Kişisel sağlık verileri, veri sorumlusunun denetiminde ve bu konuda görevlendirilen kişilerce işlenir. Veri sorumlusu, veri işlenmesinin her aşamasının bu Yönetmelik hükümlerine uygun olmasını sağlar.

(5) Kişisel sağlık verilerini işlenmesinde görev alan herkes sır saklama yükümlülüğü altındadır.

(6) Ulusal ve/veya uluslararası bildirimi zorunlu bulaşıcı hastalıklar ilgili ulusal ve uluslararası mevzuata ve bu Yönetmelik hükümlerine uygun işlenir.

Veri paylaşım esasları

MADDE 6– (1) Kişisel sağlık verisini işlemek üzere isteyen kişi veya kuruluşlar, yazılı veya ispatlanabilir elektronik ortamda veri sorumlusuna veri paylaşım talebini bildirir. Veri sorumlusu talebi, mevzuatla tanımlanmış görevlerin ifa ve icrasına uygunluğu açısından değerlendirerek uygun görmesi halinde veri paylaşımını yapar. Veri paylaşım talebinde; kurum/kuruluş, kişi adı soyadı, iletişim bilgileri, veri işleme amacı ve hukuki dayanağı, istenilen verinin içeriği ve kapsamı belirtilir.

(2) Alıcı, paylaşım ile elde ettiği verileri 5 inci madde hükümlerine uygun şekilde işlemek ve bu verileri her kullanımında ilgili veri sorumlusunu kaynak göstermek zorundadır.

(3) Kişisel sağlık verilerinin uluslararası kuruluşlarla paylaşımına uluslararası hukuka uygun olarak Bakanlıkça izin verilebilir. Uluslararası kuruluşların, Avrupa Birliği veri koruması mevzuatına uygun seviyede bir korumayı garanti etmesi ve gerekli güvenlik önlemlerinin alındığını Bakanlığa yazılı olarak bildirmesi zorunludur.

Rızaya bağlı olarak veri işlenmesi

MADDE 7- (1) Eğitim ve bilimsel araştırmalar kapsamında kişisel sağlık verilerinin işlenebilmesi için ilgili kişinin ayrıntılı olarak bilgilendirilip rızasının alınması zorunludur.

(2) Rızaya bağlı olarak kişisel sağlık verilerinin işlenmesinde ilgili kişi ile aşağıdaki bilgiler paylaşılır:

- a) Veri işleyen kurum/kuruluş veya kişiye ait bilgiler,
- b) Veri işlemenin amacı,
- c) Cevap verme zorunluluğunun bulunmadığı.

(3) Rızaya bağlı olarak kişisel sağlık verisi işlenmesinin kurumsal yönünün bulunması durumunda ilgili kurumun da onayı alınır.

(4) İlgili kişi, rızasını her zaman geri alma hakkına sahiptir. Ancak rızanın geri alınması, geri almadan önceki dönemde gerçekleştirilen işlemleri etkilemez.

İlgili kişinin bilgi isteme, erişim ve düzeltme hakkı

MADDE 8 - (1) İlgili kişi;

- a) Kendi kişisel sağlık verilerini isteme hakkına sahiptir ve veri sorumlusu bu bilgileri vermekle yükümlüdür.
- b) Kendi kişisel sağlık verilerinin işlenmesi hususunda bilgi isteme hakkına sahiptir. Bu talep üzerine veri sorumlusu, açık ve anlaşılabilir şekilde veri işleyene ait bilgileri, verinin işlenme amacını, içerik ve kapsamı ile verinin paylaşımına ilişkin bilgileri verir.
- c) Kendi kişisel sağlık verilerine erişim hakkına sahiptir.
- ç) İsteddiği zaman kendisiyle ilgili verilerin bulunduğu veri sorumlusundan gerçekleştirilmiş veya gerçekleştirilmekte olan işlemlerle ilgili kayıtlarının düzeltilmesini, dondurulmasını, silinmesini ya da güncellenmesini yazılı veya elektronik ortamda isteme hakkına sahiptir. Bilginin teyidinden sonra gerekli işlem yapılır. Ancak kamu sağlığı ve güvenliğini ilgilendiren hallerde veriler silinemez.

(2) Bu maddenin uygulanmasına dair uyuşmazlıklar Bakanlıkça ilgili mevzuata göre oluşturulan hasta hakları kurullarında çözümlenir.

ÜÇÜNCÜ BÖLÜM

Veri Toplama Organizasyonu ve Sistem Standartları

Veri toplama organizasyonu

MADDE 9 - (1) Bakanlık ve bağlı kuruluşları, mevzuatla kendilerine verilen görevleri etkin ve hızlı biçimde yerine getirebilmek için sağlık verisi işleyen bütün kişi ve kuruluşlardan kişisel sağlık verilerini bu Yönetmelik hükümlerine uygun olarak her türlü vasıta ile toplamaya, işlemeye ve paylaşmaya yetkilidir.

(2) Ülke genelinde e-sağlık ve diğer veri toplama sistemlerinin planlanması, kurulması, yürütülmesi, geliştirilmesi ve denetlenmesinden sorumlu organizasyon Bakanlıktır.

(3) İl Sağlık Müdürü, ilindeki sistemin yürütülmesi ve denetlenmesi için gerekli organizasyonel yapının kurulması ve işletilmesinden sorumludur. Bu sorumluluğu yerine getirmek üzere kendi ilinde yeterli sayıda koordinatörü görevlendirerek bu koordinatörleri Bakanlığa bildirir. Koordinatörler kendi sorumluluklarında olan; sağlık hizmeti sunan kamu ve özel sağlık kurum ve kuruluşlarında, sağlık hizmeti sunumunda bir aksamaya sebebiyet vermeksizin Bakanlıkça belirlenen teknik, idari ve mali kriterlere uygun verilerin toplanmasını, Bakanlık veri merkezine güvenli bir şekilde gönderilmesini sağlar.

(4) Tüzel kişiliğe sahip sağlık hizmeti sunan kuruluşlarda yöneticiler ile bireysel olarak sağlık hizmeti sunan gerçek kişiler bizzat kendileri, sağlık tesisinde Bakanlığın belirlemiş olduğu standartlara uygun elektronik kayıt sistemlerinin kurulmasından ve işletilmesinden, sistemlerindeki kayıtların yedeklilik, güvenlik ve mahremiyetinin sağlanmasından, kaydedilen verilerin günlük olarak Bakanlık veri merkezine gönderilmesinden sorumludur. Bu gerekliliklerin yerine getirilmesi amacıyla tüzel kişiliğe sahip kuruluşlarda bir veri sorumlusu görevlendirilir ve Bakanlığa bildirilir. Bireysel olarak sağlık hizmeti sunan kişilerin kendisi aynı zamanda veri sorumlusudur.

Sistem standartları

MADDE 10- (1) Bakanlık, ülke genelinde sağlık bilgi sistemleri ile hizmet sunucularına, hizmetlere, hizmet sunum sürecinde kullanılan araç, gereç, tıbbi malzeme ve ilaçlara, olaylara ait veriler dahil gerekli görülen tüm alanlara dair kodlama ve sınıflandırma sistemi standartlarını bir Tebliğ ile belirler ve ilan eder, bu standartlara uygunluğu denetler.

DÖRDÜNCÜ BÖLÜM

Kişisel Sağlık Verilerinin Korunması, Müeyyide ve Son Hükümler

Verilerin korunması

MADDE 11 – (1) Veri sorumlusu ve alıcı, kişisel sağlık verilerinin ihlaline karşı ve ihlali halinde gerekli hukuki, teknik ve idari önlemleri alır.

(2) Veri sorumlusu ve alıcı kişisel sağlık verilerinin ihlali halinde gecikmeden, ihlal edilen veri kategorileri, veri konusu kişi sayısı, ihlalin sonuçları ve alınan önlemler hakkında bilgilendirilir, veri korumada görevli personelle, bilgi işlem sorumluları ile iletişime geçilir. Kişisel veri ihlali halinde veri sorumlusu bilgilendirildikten sonra ilgili kişiye bilgi verilir.

(3) Veri sorumlusu ve alıcı, mevzuatla tanımlanmış görevleri çerçevesinde istatistiksel ve bilimsel amaçlarla ileride işlenmek üzere saklanacak kişisel sağlık verilerinin güvenliği ve korunması için uygun güvenlik önlemlerinin alınmasına yönelik bu Yönetmelik hükümlerine uygun politikalar geliştirmek ve Bakanlık tarafından uygun görülen standartlara uygunluğu sağlamakla yükümlüdür.

(4) Alıcının, veri sorumlusunun veri tabanının tamamına doğrudan erişimine izin verilmez. Talep edilen verinin aktarımı sağlanır veya CD, DVD, sabit disk, taşınabilir bellek gibi elektronik veya manyetik kayıt ortamında şifrelenerek alıcıya gönderilir.

(5) Veri kaybının önlenmesi bakımından yedekleme sistemleri kurulması zorunludur. Yazılımlar kullanıcı tanımlanması ve yetkilendirme dahilinde kullanılmak zorundadır. Kullanıcı tanımlama ve yetkilendirme, her defasında belgelendirme suretiyle yapılır. Veri işleyenler ancak üstlendikleri görevlerinin gerektirdiği ölçüde sistemdeki verilere ulaşabilir.

Müeyyide

MADDE 12-(1) Bu Yönetmelikle korunan verileri, kendisine veya başkasına yarar sağlamak veya başkasına zarar vermek amacıyla hukuka aykırı olarak işleyenler hakkında genel hükümlere göre işlem yapılır.

(2) Bu Yönetmelik gereklerini yerine getirmeyen kamu görevlileri için bağlı oldukları disiplin amirliğine bildirim yapılır ve varsa yetkileri iptal edilir. Özel hukuk kişileri için yetkilerinin alınması ile birlikte ilgili kuruluş hakkında ilgili mevzuatına göre idari işlem yapılır.

Yürürlük

MADDE 13 - (1) Bu Yönetmeliğin 11 nci maddesinin üçüncü fıkrası 01/12/2015 tarihinde; diğer maddeleri yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 14- (1) Bu Yönetmelik hükümlerini Sağlık Bakanı yürütür.