



T.C.
SAĞLIK BAKANLIĞI
Sağlık Bilgi Sistemleri Genel Müdürlüğü

7/25464
GK 111

SAĞLIK BİLGİ SİSTEMLERİ GENEL MÜDÜRLÜĞÜ
- STANDART VE AKREDİTASYON DAİRESİ
BAŞKANLIĞI
06/01/2022 11:59 - E-75730711-610-2
00156187292

Sayı : 75730711-610
Konu : Yazılı Soru Önergesi Cevabı

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

İlgi : 26.02.2020 tarihli ve 43452547-120.07-E.624067 sayılı yazısı.

Eskişehir Milletvekili Sayın Metin Nurullah SAZAK tarafından verilen “Tıbbi kayıt ve arşivleme sistemi ile kişisel verilerin güvenliğine ilişkin” 7/25464 sıra sayılı yazılı soru önergesinin cevabı ilişikte sunulmaktadır.

Arz ederim.

Dr. Fahrettin KOCA
Bakan

Ek: Soru Önergesi Cevabı

Eskişehir Milletvekili Sayın Metin Nurullah SAZAK tarafından verilen “Tıbbi kayıt ve arşivleme sistemi ile kişisel verilerin güvenliğine ilişkin” 7/25464 sıra sayılı yazılı soru önergesinin cevabıdır:

SORU 1: Ülkemizde tıbbi kayıt arşivleme sistemi nerede ve hangi kurum tarafından sağlanmaktadır? Bu sisteme erişim izni kimlerde vardır ve nasıl alınmaktadır?

CEVAP 1: Elektronik ortamda işlenen kayıtlar, sağlık hizmetinin sunumunun yapıldığı sağlık tesisleri ve Sağlık Bakanlığı (Sağlık Bilgi Sistemleri Genel Müdürlüğü) olmak üzere temel olarak iki kademede saklanmaktadır.

Sağlık tesislerinde Sağlık Bilgi Yönetim Sistemleri (SBYS) üzerinde saklanan tıbbi kayıtlara sağlık hizmetinin sunumunda görev yapan sağlık profesyonelleri (tabip, eczacı, hemşire, ebe, laborant, sağlık teknisyeni vb.) tarafından erişim sağlanmaktadır. Erişim izinleri verilirken Kişisel Sağlık Verileri Hakkında Yönetmeliğin “sağlık personelinin verilere erişimi” başlıklı 6’ncı maddesinde belirtilen esaslar uyarınca hareket edilmektedir. Bu kapsamda hasta mahremiyetine azami dikkat gösterilmekte ve ilgili personele, bilmesi gereken prensibi uyarınca, sadece ihtiyaç duyacağı kadar bilginin gösterilmesi sağlanmaktadır. Erişim izinleri (kimin, hangi bilgiye, hangi yetki ile erişeceği) hastane yönetimleri tarafından oluşturulan komiteler tarafından belirlenmekte ve hastane yönetiminin onayı ile uygulanmaktadır.

Bakanlık tarafından tutulan verilerin saklandığı sistem “merkezi sağlık veri sistemi” olarak adlandırılır. Tüm sağlık hizmet sunucularında SBYS’ler üzerinde saklanan veriler Bakanlık tarafından belirlenen standartlara uygun olarak merkezi sağlık veri sistemine aktarılır. Aktarılan veriler, merkezi sağlık veri sisteminde kimliksizleştirilmiş olarak saklanır. Bakanlık birimlerinin merkezi sağlık veri sisteminde saklanan verilere erişimi ile ilgili hususlar Kişisel Sağlık Verileri Hakkında Yönetmeliğin “Bakanlık birimlerinin verilere erişimi” başlıklı 7’nci maddesinde açıklanmıştır.

Bunların dışında her vatandaş kişisel e-Nabız hesabı oluşturarak merkezi sağlık veri sisteminde tutulan verilere erişim sağlayabilir.

SORU 2: Tahlil, tetkik tanı gibi kişisel sağlık verilerinin başkaları tarafından görülmesini önleyecek ne gibi tedbirler alınmaktadır? Kötü amaçlı bir bilgi edinme tespit edildiğinde yaptırım uygulanmakta mıdır?

CEVAP-2: Tüm SBYS yazılımları rol tabanlı erişim yetkilendirme mekanizmalarına sahip olup hastanelerde görev yapan personel, önceden tanımlı rollere atanmakta; erişim yetkileri ise ekran ve rapor bazında söz konusu rollere tanımlanmaktadır. Doktor, hemşire gibi ana roller, birçok alt kırılımlarla detaylandırılmaktadır.

SORU-3: Hastane içi bilgisayar veri tabanındaki mevcut hasta bilgilerine yetkisi olmayan kişilerin erişmesi nasıl engellenmekte? Bilgisayar veri sisteminin güvenliği nasıl sağlanmaktadır?

CEVAP-3: HBYS yazılımları üç katmanlı mimaride çalışmaktadır. Kullanıcılar SBYS uygulama sunucusuna erişim yapmakta, veriler ise Veri Tabanı Yönetim Sistemi (VTYS) olarak adlandırılan bir başka sunucuda tutulmaktadır. Kullanıcılar, uygulama sunucusu ve VTYS sunucusu arasındaki veri trafiği güvenlik duvarı yazılımları vasıtası ile denetlenmekte; kullanıcıların sadece uygulama sunucusuna erişimine, VTYS sunucusuna ise sadece uygulama sunucusundan erişime izin verilmektedir. Bu mimaride kullanıcılar hiçbir şekilde VTYS sunucusuna erişememektedir. VTYS sunucusunun (uygulama sunucusu hariç) dış ağ ile tüm iletişimi kapatılmaktadır.

Kullanıcılar ile uygulama sunucusu arasındaki tüm iletişim şifreli olarak gerçekleştirilmektedir. Bu sayede ağı dinleyen bir üçüncü kişinin verileri ele geçirme/dinleme ihtimali ortadan kalkmaktadır.

SORU-4: Bu konuda hastane yönetiminin görev ve sorumlulukları nelerdir?

CEVAP-4: Bilgi güvenliğinin sağlanması için her kademedeki üst yöneticinin görevleri Bilgi Güvenliği Politikaları Yönergesinin 5'nci maddesinin (2) nci fıkrasında açıklanmıştır. Buna göre "Bilgi Güvenliği Yönetim Sisteminin (BGYS) tesis edilmesi ve etkin bir şekilde işletilmesi için, üst yönetim desteği ve katılımı zorunludur. Bakanlık merkez teşkilatı, bağlı kuruluşlar ve il sağlık müdürlüklerinin üst yöneticileri, bu Yönergenin dördüncü bölümünde belirtilen bilgi güvenliği organizasyonunun kurulmasından ve kendilerine bağlı en uç noktalara kadar bilgi güvenliği ile ilgili tedbirlerin alınmasını sağlamaktan birinci derecede sorumludur".

Hastane yönetimlerinin hastanenin genel işleyişi, gözetim ve denetim ile ilgili görev ve sorumlulukları ilgili mevzuatta (Yataklı Tedavi Kurumları İşletme Yönetmeliği vb.) açıklanmıştır.

Bu mevzuatta tanımlanan genel görev ve sorumluluklara ilave olarak, hastane yönetimlerinin kendi tesislerinde "bilgi güvenliğinin sağlanması" için almaları gereken tedbirler İl Sağlık Müdürlükleri tarafından yayımlanan "İl Sağlık Müdürlüğü BGYS Politikası" dokümanlarında yer almaktadır.

SORU-5: Hasta mahremiyeti ve bilgilerin gizli tutulması konusunda denetim nasıl sağlanmaktadır?

CEVAP-5: Sağlık Bilgi Yönetim Sistemi (SBYS) yazılımları ile ilgili teknik denetimler, Sağlık Bilgi Sistemleri Genel Müdürlüğü tarafından kurulmuş olan "Kayıt Tescil Sistemi (KTS)" esasları çerçevesinde yürütülmektedir. KTS kapsamında belirlenen kriterleri sağlamayan yazılım ve ürünlerin kullanımına kısıtlama getirilmektedir.

Bilgi güvenliği denetimleri Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesinin "**Bilgi Güvenliği Denetimi**" başlıklı 13'üncü maddesinde belirtilen esaslar doğrultusunda yürütülmektedir. Bu kapsamda;

• SBSGM tarafından sektörel SOME vasıtasıyla, önceden makam onayı almak ve ilgili birimlere bilgi vermek şartıyla, Bakanlık merkez ve taşra teşkilatı ile bağlı kuruluşlara bağlı birimlerde sızma ve sosyal mühendislik testleri gerçekleştirilmektedir.

• Bakanlık bağlı kuruluşlar ile taşra teşkilatları kendi kurumsal SOME'leri vasıtasıyla, önceden makam onayı almak ve ilgili birimlere bilgi vermek şartıyla, kendi bağlı birimlerde sızma ve sosyal mühendislik testleri yapmakta veya yaptırmaktadır.

Sağlık hizmeti sunumu yapılan sağlık tesislerinin kalite denetimleri, Bakanlığımız Sağlıkta Kalite, Akreditasyon ve Çalışan Hakları Dairesi Başkanlığı tarafından yapılmaktadır. Söz konusu denetimler içerisinde yer alan **“Bilgi Yönetim Sistemi Denetimleri”** ile “hasta ya da çalışanlara ait tıbbi ve kişisel bilgilerin, doğru ve güvenli şekilde kayıt altına alınması ve depolanması; ihtiyaç duyulan doğru bilginin, bilgi mahremiyeti ve güvenliği gözetilerek, doğru zamanda, doğru kişiye ulaştırılması” için alınmış olan tedbirler, kalite denetçileri tarafından yerinde denetlenmektedir.

Bunun dışında Bakanlığımız Teftiş Kurulu Başkanlığınca; Başkanlık görev, yetki ve sorumluklarının açıklandığı “Sağlık Bakanlığı Denetim Hizmetleri Başkanlığı Yönetmeliği”nin “Bilgi Teknolojileri Denetimi” başlıklı 52’nci maddesi uyarınca denetlenen birimlerin elektronik bilgi sistemlerinin sürekliliğinin ve güvenilirliğinin değerlendirilmesi yapılmaktadır.

SORU-6: Yönetmeliğin ilgili maddelerin hayata geçirilmesi kısmında yaşanan sıkıntılar nelerdir?

CEVAP-6: Bilindiği üzere güvenliğin sağlanması büyük oranda kısıtlamaların/yasakların konulması ile mümkün olabilmektedir. Sistemler üzerine eklenen her bir ilave kural ve kısıtlama, teknik olarak hangi tedbir alınır ise alınsın, uygulamanın performansını olumsuz yönde etkileyebilmektedir.

Bu noktada, “güvenliğin sağlanması”, “hizmetin zamanında ve etkili olarak verilebilmesi” ve bunları yaparken de “mevcut mevzuattan kaynaklanan yükümlülöklere uyulması” için kabul edilebilir bir denge sağlanabilmesi gerekmektedir.

Konuya gösterilen ilgiye teşekkür ederim.