ROMATEM Fizik Tedavi Ve Rehabilitasyon Dal Hastanesi Bilgi Güvenliği Eğitimi

Bilgi güvenliği, bilgilerin izinsiz kullanımından, izinsiz ifşa edilmesinden, izinsiz yok edilmesinden, izinsiz değiştirilmesinden, bilgilere hasar verilmesinden koruma, veya bilgilere yapılacak olan izinsiz erişimleri engelleme işlemi. Bilgi güvenliği, bilgisayar güvenliği ve bilgi sigortası terimleri, sık olarak birbirinin yerine kullanılmaktadır. Bu alanlar birbirleri ile alakalıdırlar ve mahremiyetin, bütünlüğün ve bilginin ulaşılabilirliğinin korunması hususunda ortak hedefleri paylaşırlar..

Türk Standartları Enstitüsü TSE tarafından Türkçeye çevrilerek yayınlanan TS ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemi Standardı, bilgi güvenliğini üç başlık altında inceler:

Gizlilik: Bilgilerin yetkisiz erişime karşı korunması
Bütünlük: Bilgilerin eksiksiz, tam, tutarlı ve doğru olması
Kullanılabilirlik: Bilgilere yetkililerce ihtiyaç duyulduğunda erişilebilir olması

BİLGİ YÖNETİMİNE İLİŞKİN FAALİYETLERİN YÜRÜTÜLMESİ VE KOORDİNASYONUNA YÖNELİK SORUMLULAR VE SORUMLULUKLAR

Hastane Bilgi Yönetimi Sistemini kullanan tüm çalışanlar: HBYS sistemini kullanan tüm çalışanlar hastanedeki mevcut tüm bilgisayarlardan kendilerine verilmiş ve görevleri ile yetkilendirilmiş kullanıcı kodu ve şifresi ile yaptığı tüm işlemlerden sorumludur.(Veri girişi, değiştirmesi, silmesi vb.)

Bilgi İşlem Sorumlusu:

- Hastaneye ait bilgisayar sisteminin verimli ve amaca uygun çalışmasını sağlamak.
- Bilgisayar sistemleri ile ilgili her türlü donanım ve yazılım problemlerinin çözümü, yedeklerinin alınmasını ve bilgilerin arşivlenmesi işlemlerini yürütmek.
- Sistemlerin arızalanması durumunda ön inceleme ve bakımını yaparak, gerekli servis hizmetlerinin verilmesini sağlamak.
- Bilgisayar sistemlerinin periyodik bakımlarında ve onarımlarında sözleşmeli firma elemanlarını ve çalışmalarını denetlemek, gerekli gördüğü hallerde yazılı-sözlü bilgi vermek.
- Her gün mesai başlangıcında bilgisayar sistemleri ve donanımlarının açılmasını, iş bitiminde ise kapatılmasını sağlamak.
- Faaliyetler çerçevesinde, ihtiyaç duyulan yazılım sistemleri konusunda personele destek vermek; meydana gelen küçük teknik arızaları geciktirmeden gidermek veya giderilmesini sağlamak.
- Hastaneye ait elektronik postasına gelen bilgi ve talepleri ilgili birimlere iletmek.
- Bilgisayar donanımlarında meydana gelen aksaklıkların giderilmesi için Mesul Müdürüne bilgi vermek.
- Konusuyla ilgili olarak Mesul Müdürü tarafından verilen diğer işleri yerine getirmek.

KİŞİSEL SAĞLIK KAYITLARIN GÜVENLİĞİ

Kullanıcılar, hasta ile ilgili bilgileri girilir, muayene ve reçete girildikten sonra hasta kaydı kapanır. Tekrar kullanıcılar bilgileri değiştiremez. Kişisel bilgiler kişinin kendisi veya mahkeme tarafından istenildiği takdirde verilir.

BİLGİ GÜVENLİĞİ İHLAL OLAYLARI

Kurumun bilgilerinin gizliliğini, bütünlüğünü veya kullanılabilirliğini herhangi bir biçimde etkileme potansiyeline sahip herhangi bir olaydır. Hastanemizde aşağıdaki hususlardan kaynaklanacak ihlaller Bilgi Güvenliği İhlali Olarak kabul edilmiştir.

- Kullanılan bilgi varlıklarının çalınması, kaybolması ya da kırılması
- Bilginin Gizlilik, Bütünlük, Erişilebilirlik beklentilerindeki ihlaller
- İnsan hatalarından kaynaklanan ihlaller
- Bakanlık tarafından yayımlanmış Bilgi Güvenliği Yönergesi, Politikalar ve Prosedürlere göre iş ve işlemlerin yürütülmemesi
- Fiziksel Güvenlik düzenlemelerinin ihlali
- Kontrolsüz sistem değişiklikleri
- Yazılım ya da donanım arızaları
- Erişim ihlalleri (yetkisiz erişim), yetkisiz bilgi kullanımına izin veren uygun olmayan erişim denetimleri Siber saldırılar (Virüs, izinsiz giriş, Truva atı, casus yazılım vb. bulgular için, sistem sunucu servis problemleri için)
- Gizli bilginin yetkisiz kişilerce ifşa edilmesi

Yukarıda sayılan kurallardan bir ya da birkaçının ihlali ve tespiti durumunda, güvenlik ihlaline yol açan kullanıcı hakkında **ÖZEL ROMATEM FİZİK TEDAVİ VE REHABİLİTASYON DAL HASTANESİ** tarafından işlem başlatılacaktır. Ciddi ihlaller kullanıcının dava edilmesine yol açacaktır.

VERİ KAYBI / İFŞASI

Gizli bilgilerin e-posta aracılığı ile iletimi, ağ üzerinden iletilen bilgilerin yetkisiz ya da yanlış alıcıya iletimi, internet üzerinden güvenli olmayan kanallar aracılığıyla veri iletimi, ortak kullanım yazıcılarından alınan çıktıların sahiplenilmemesi ya da güvenliğine önem verilmemesi, masa üstü ya da ortak alanlarda basılı kopyaların denetimsiz bırakılması vb. durumlarda tüm çalışanlar verilerin güvenliğini ve bütünlüğünü korumanın önemini göz

önünde bulundurarak bilinçli hareket etmeli, ihlal durumlarını rapor etmesi gerekir

BİLGİ SIZDIRMA (DATA LEAKAGE)

Kurumun bilişim teknolojileri ile kullandığı, işlediği ya da ürettiği verilerin bilinçli ya da bilinçsiz bir şekilde kurum dışına taşınarak, belirlenmiş "bilgi güvenliği" politikalarının ihlali durumunda ilgili çalışan veya kullanıcı sorumludur.

TAAHHÜTNAME

Taahhütname Hastane ile çalışan arasında gizlilik esaslarının belirlenmesi amacı ile tanzim edilmiştir.

Gizlilik sözleşmesi gerekli tüm personele imzalatılmaktadır. Aksi davranışlar içerisinde bulunanlar hakkında gerekli yasal işlemler yapılacaktır.

. Kurum teşhis ve tedavi hizmetlerinde, yasal mevzuat şartlarının yerine getirilmesinden, hizmet sunumunun hasta ve yakının ihtiyaç ve beklentilerine karşılanmasından ve memnuniyetin sağlanmasından, çalışanına uygun çalışma koşulları, donanım ve ekipman sağlamaktan sorumludur. Kurum hasta hakları, güvenlik, veri bütünlüğü, erişim, uygulama ve çalışan hakları ile ilgili olarak gizlilik ilkesine bağlı kalacağını taahüd eder.

ÇALIŞANLARIN; Hasta, yakını ve iş birliği yapılan firmalara ilişkin gizlilik esasları

- Hasta ve hak sahiplerine ait gizli bilgilerin ve tescilli hakların korunmasından,
- Teşhis ve tedavi sonuçlarının uygun şartlarda muhafaza edilmesi ve iletilmesinden,
- Yeterlilik, tarafsızlık, karar verme ve çalışmalarda güveni azaltacak herhangi bir faaliyette bulunmamayı,
- Verilen hizmetin belirlenen kurallar çerçevesinde gerçekleştirilmesini,
- Söz konusu bilgilerin hasta onayı dışında ya da yasal bir yükümlülük altında bulunmadığı sürece herhangi bir üçüncü şahıs, kurum ya da kuruluş ile paylaşılmamasını,
- Hasta ve yakınından alınan kişisel bilgilerin (ad, soyad, T.C. No, adres, telefon ve hastalık bilgileri v.s.) kurum içinde ya da dışında üçüncü şahısların ve kurum kuruluşların bulunduğu ortamlarda paylaşmayacağını,

ÇALIŞANLARIN; E-posta ve internet kullanımına ilişkin gizlilik esasları

- Kurumun e-posta sisteminin kullanılarak suistimale açık alıcıya ve kullanıcıya zarar verecek nitelikli e-postalar için kullanılmayacağından,
- Kurum e-posta adresi ile internet ortamında bulunan özel içerikli web sitelerine üye olunmamasından,
- Alınan zincir mesajların ya da spamların açılmayarak direk silinmesinden,
- Bu e-posta ile uygun olmayan içerikte (ırkçılık, siyasi propaganda, pornografik görüntü v.s.) mailler gönderilmemesinden ya da alınmamasından,
- E-posta adreslerine düşen tüm maillerin günde iki kez olmak üzere kontrollünden,
- Bu maillerin kontrol edilmemesi halinde oluşabilecek aksaklıklardan,
- İnternet üzerinden kurum tarafından onaylanmamış yazılım indirilmemesinden genel ahlak anlayışına aykırı ve kanunlara aykırı web sitelerine giriş yapılmamasından,

ÇALIŞANLARIN; Şifre kullanımında gizlilik esasları

- Tüm kullanıcılar gerek medisis gerekse E-posta şifrelerinin ikinci üçüncü şahıslarla paylaşılmamasından,
- Diğer bir kullanıcının şifresi üzerinden işlem yapılmamasından,
- Şifrelerin çalışma alanlarında yazılı halde bulundurulmamasından,

ÇALIŞANLARIN; Kurumun genel işleyişine ilişkin gizlilik esasları

- Kurum içinde oluşan herhangi bir durumun asla diğer şahıslarla paylaşılmamasından,
- Kurum hakkında fikir beyan ederken resmi konuşma dilinin dışına çıkılmamasından,
- Kalite Yönetim Sistemi gereğince kullanılan her türlü doküman ve işletilen sistemin diğer kurumlar ile paylaşılmamasından,
- Hastaya ait bilgi ve belgeler 3. Şahıslarla kesinlikle paylaşılamaz, arşive giden ve muhafaza edilen evraklar bilgi güvenliği hasta mahremiyeti doğrultusunda kesinlikle paylaşılamaz,

ÇALIŞANLARIN; Kullanıcı bilgisayarlarındaki bilgi güvenliği esasları

- Tüm kullanıcılar kullandığı bilgisayarların içindeki dosyalardan,
- Kurum bilgisayarlarına kişisel bilgilerini asla kopyalamamaktan,
- Cep telefonu, flash bellek vb. kişisel depolama cihazlarını kullandıkları bilgisayarlara takmamaktan,
- Bilgisayardaki firmaya ait bilgileri kendi depolama cihazlarına kaydetmemekten,
- Kişisel depolama cihazı bağladıktan sonra oluşabilecek virüs, donanım arızası ve veri kayıplarından Sorumludur ve gereğini yerine getireceğini taahüd eder.