BYS'NİN AMAÇ VE KAPSAMI

Sağlık tesisimiz teşhis tedavi hizmetlerinde; yasal mevzuat şartların karşılanmasından, hizmet sunumunda hasta ihtiyaç ve beklentilerine cevap verecek şekilde gerçekleşmesinden sorumludur. Hasta kayıtları, tanı ve tedavi bilgileri radyoloji görüntüleri, laboratuvar sonuçları, ameliyat bilgileri, ücretlendirmeler gibi tüm bilgiler HBYS ortamında kaydedilmekte ve veri tabanında saklanmaktadır.

Bu amaçla kurumumuz;

- Faaliyetlerimizin ticari, mali ve diğer iç ve dış baskılardan ve etkilerden uzak tutulmasını,
- Hasta ve hak sahiplerine ait gizli bilgilerin ve tescilli hakların korunmasını,
- Teşhis ve tedavi sonuçlarının uygun şartlarda muhafaza edilmesini ve iletilmesini,
- Yeterlilik, tarafsızlık, karar verme ve çalışmalarda güveni azaltacak herhangi bir faaliyette bulunmamayı,
- Sağlık hizmeti sunarken beklenen kalite seviyesinin sağlanmasını,
- Vereceğimiz hizmetin belirlenen standartlar çerçevesinde gerçekleştirilmesini,
- Söz konusu bilgileri hasta onayı dışında ya da yasal bir yükümlülük altında bulunmadığı sürece herhangi bir üçüncü şahıs, kurum ve kuruluş ile paylaşmamayı taahhüt eder. Kurum olarak gizliliğin önemli olduğuna inanırız. Bu politika hastanemizde sunulan tüm sağlık hizmetleri için geçerlidir.

Hastanemiz Hasta Hakları, güvenlik, veri bütünlüğü, erişim ve uygulama ile ilgili gizlilik ilkelerine bağlıdır.

Topladığımız bilgiler ve onları nasıl kullandığımız:

- Sağladığınız bilgiler; hastanemize teşhis ve tedavi için başvurduğunda hastalarımızdan kişisel bilgiler (ad, soyad, hastalık bilgileriniz, T.C Kimlik numarası, adres, telefon bilgileri, vb.) istenmektedir.
- Hastanemiz yalnızca, Hasta Bilgi Güvenliği Politikası ve/veya belirli hizmetlere ilişkin gizlilik uyarısında açıklanan amaçlarla kişisel bilgileri kullanır.

Bilgi güvenliğini sağlamak amacıyla Bilgi Güvenliği gizlilik sözleşmesi tüm personele imzalatılmaktadır.

BİLGİ GÜVENLİĞİ:

- Verileri yetkisiz erişime, yetkisiz şekilde değiştirilmelerine, açıklanmalarına veya imha edilmelerine karşı korumak için uygun önlemleri alırız.
- Hastanın özlük bilgileri ve kurum bilgileri sadece poliklinik sekreterleri tarafından değiştirilebilir.
  - Hastalarla ilgili her türlü kaydın kim tarafından, hangi tarihte girildiği, ulaşma, değiştirme bilgisi hastane bilgi işlem programı log kayıtları altında tutulmaktadır.
  - Hastaların klinik kayıtlarına yalnızca konu ile ilgili yetkilendirilmiş kişinin giriş yaptığı hastane bilgi işlem programında "Güvenlik Sistemi" adı altında izlenebilmektedir.
- Veri tabanı üzerinde Hasta kayıt logları, Hasta Hizmet logları, Hasta Fatura Logları, Hasta Poliklinik logları, Tanımlama Logları, Hasta Dosya logları, Veri tabanı oturum logları, Sağlık kurulu kayıt logları kayıt altına alınmaktadır.
- Kullanıcıların ara yüze bağlanmak için kullandıkları şifreler, şifreli biçimde veri tabanında saklanmaktadır. Veri tabanı sistem logları gerektiğinde hastane yönetimi tarafından izlenmektedir.
- Kullanıcılar veri tabanına yapılacak müdahale (yama, güncelleme vb.) öncesinde otomasyon sistemi üzerinden bilgilendirilmektedir.
- Hastaneye destek hizmeti veren firmanın dış ortamdan iç ortama hangi durumlarda erişim yapacağı hakkında hastane tarafından onaylanmış gizlilik sözleşmesi mevcut olup dış ortamdan iç ortama erişimler kayıt altına alınmaktadır.
- Her kullanıcının veri tabanında hangi bilgilere erişebileceği bilgi işlem biriminde sorumlular tarafından belirlenmektedir. Ayrıca bu kişilerin hangi yetkilere sahip olduğu HBYS üzerinden takip edilebilmekte ve rapor edilebilmektedir.

BYS'Yİ OLUŞTURAN ALT SİSTEMLER (SBYS, LBYS, PACS, WEB, E-POSTA, DOSYA SUNUCU, VARSA DİĞER BİLGİ YÖNETİM ALT SİSTEMLERİ GİBİ)

- Hizmetin daha hızlı ve standartlara uygun kayıt ortamında verilebilmesi için Hastane Bilgi Yönetim Sistemi (HBYS) kullanılmaktadır. HBYS hizmeti 4734 sayılı kanun doğrultusunda satın alınmakta olup, 24 saat kesintisiz hizmet sunulmaktadır.
- HBYS nin hizmeti devam ettirebilmesi amacıyla firma tarafından laboratuvar tetkik işlemleri için LIS, radyoloji tetkik işlemleri için PACS bilgi yönetim alt sistemleri kullanılmaktadır.

SBYS İŞLETİMİ VE DEĞİŞİKLİK YÖNETİM SÜREÇLERİ:

- Hastane bilgi yönetim sistemi kullanıcılarına her yıl hizmet içi eğitim dahilinde bilgi güvenliğine yönelik farkındalık eğitimleri düzenlenmektedir. Bu eğitimlerle kullanıcılara sistem üzerinden kendilerine tanımlanan yetkileri dahilinde işlem yapabilecekleri, birim/bölüm değişikliği ya da farklı bir bilgi ulaşımına ihtiyaç

duyulması durumu ortaya çıktığında hastane yöneticisi onayı dahilinde yetki genişletilmesi yapılabileceği aktarılmaktadır.

- Kullanıcılar tarafından yapılan iş ve işlemlerde mevzuat değişikliği, il sağlık müdürlüğünce gelen yazı gereği veya hastane içi işleyişte yapılan değişikliğe istinaden HBYS üzerinde geliştirme talepleri bilgi işlem birimine gerekçesi ile iletilir.
- Bilgi işlem birim personeli ve talep eden personel tarafından talep içeriğine uygun olarak çalışma gerçekleştirilir. Bu çalışma neticesinde istenilen değişiklik sağlanabilir ya da firmaya bilgi işlem birimince konu hakkında çağrı açılarak talebin firma tarafından gerçekleştirilmesi istenir.
- Firma tarafından oluşturulması beklenen değişiklikler bilgi işlem birimince firma ile hastane bilgi işlem birimi arasında kullanılan sistem üzerinden takip edilir.
- İstenen taleplere yönelik ya da firmaya bakanlık tarafından bildirimi yapılan değişiklikler için firma tarafından yapılan güncel versiyonlar öncelikle proxy yapı dışında tutulan sunucular üzerine yüklenerek test edilir. Sonrasında kullanıcılara bilgilendirme yapılarak güncel versiyon yüklemesi yapılır.

BİLGİ SİSTEM DONANIM VE ALTYAPI, YÖNETİM VE TALEP SÜREÇLERİ:

- Kurumda kullanılan donanım araç ve gereçleri bilgi işlem birimi tarafından gözden geçirilerek yapılan işe uygun olarak birimlere dağıtılmasında hastane yönetimine önerilerde bulunur.
- Tüm birimlerde bulunan bilgisayar donanım ve yazılımlarının güncel envanteri bilgi işlem birimince güncellenerek muhafaza edilir. Bu envanterde Bulunduğu bölüm, Marka, Model, Seri no, Demirbaş numarası, Donanım ve yazılım adı, İşletim sistemi, Ek aksamlar, Alınma tarihi ve Varsa garanti süresi gibi bilgiler yer alır.
- Kurumda bilgi işlem network altyapısı gigabit portlara sahip anahtarlama cihazları ile sağlanır. Anahtarlama cihazları birbirine yedekli fiber kablolarla bağlanırken, bilgisayar ve dicom cihazlarla gigabit Ethernet ara yüzü ile kablolu olarak haberleşir.
- Kurumda mobil cihazların ağa erişimleri için kablosuz ağ altyapısı bulunur ve cihazların ağa yetkilendirildikleri kadar erişimine izin veren yazılım ve donanımlar kullanılır.
- Ağa bağlı bulunan bütün kritik cihazlar kesintisiz güç kaynakları ile (oline ups) beslenir ve kesintisiz hizmet vermeleri sağlanır.
- Ortak alanlarda kullanılan ağ yazıcıları şifreli/kartlı erişim sistemiyle çalışır ve yetkisiz kişilerin yazdırılan dokümana erişimi engellenir.
- Bilgi sistem yönetimi kapsamında yazılımsal ya da donanımsal talepler tüm hastane kullanıcıları tarafından yapılabilir. Donanımsal ihtiyaçlarda ise demirbaş olan malzeme istemlerinde "MC.FR.08 İHTİYAÇ LİSTESİ FORMU" ile ilgili ambar biriminde talepte bulunulur, istenen malzeme depoda var ise talep eden birime depodan çıkışı yapılarak kişiye zimmet oluşturulur. Tüketim malzemesi istemlerinde ise ilgili depodan tüm malzemeler bilgi işlem birimine çıkışı yapıldığından bu malzemelerin dağıtımı bilgi işlem birimi tarafından yapılır. Tüketim malzeme talebi HBYS üzerinden kayıt açılarak gerçekleşir ve bilgi işlem birim personeli tarafından kullanımda olan malzeme kontrolü yapılarak değişiklik sağlanır.
- Kullanıcılar tarafından yazılımsal talepler HBYS üzerinden kayıt altına alınarak iletilir. Gelen taleplerin değerlendirilmesinden sonra bilgi işlem birim personeli ve kullanıcı ile ön çalışma yapılır, talep bu çalışma ile karşılanır ya da firmaya iletilerek talebe yönelik çalışma istenir.

ERİŞİM VE YETKİ KONTROLÜ:

- Erişim kontrolünün amacı, bilgi ve bilgi işleme tesislerine yapılacak olan erişimlerin kısıtlanması, sadece yetki verilen kişilerin kontrollü ve kayıt altına alınarak bilgiye erişmesine imkân verecek bir sistemin tesis edilmesidir. Erişim kontrolü ile ilgili hususlar, BY.PR.01 Bilgi Yönetim Sistemi Prosedüründe ayrıntılı olarak açıklanmıştır.

BİLGİ SINIFLANDIRMA/GİZLİLİK DERECELERİNİN VERİLMESİ:

- Kurum bilgi varlıkları, içerdikleri verilerin hassasiyeti, kurum için taşıdıkları önem ve yasal zorunluluklar dikkate alınarak uygun bir şekilde sınıflandırılır/gizlilik derecesi verilir.
- Bilgi varlıklarına (resmi yazılar dâhil) verilecek gizlilik dereceleri için 13/05/1964 tarihli ve 6/3048 sayılı Bakanlar Kurulu kararı ile yürürlüğe giren "Gizlilik Dereceli Evrak ve Gerecin Güvenliği Hakkındaki Esaslar" dikkate alınır. Buna göre;
- İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda kişi güvenliği veya milli güvenlik açısından saygınlık ve çıkarlarımıza hayati derecede zararlar verebilecek, yabancı bir devlet için faydalar temin edebilecek ve güvenlik bakımından olağanüstü sonuçlar doğurabilecek bilgiler "çok gizli",
- İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda, kişi güvenliği veya milli güvenlik açısından, saygınlık ve çıkarlarımıza büyük zarar verebilecek, yabancı bir devlet için faydalar temin edebilecek özellikler taşıyan bilgiler "gizli",

- İzinsiz ve yetkisiz açıklanması, kullanılması, işlenmesi ya da paylaşılması durumunda, kişi güvenliği veya milli güvenlik açısından saygınlık ve menfaatlere zarar verebilecek, yabancı bir devlet için faydalar temin edebilecek bilgiler "özel",
- İçerdiği bilgi itibarıyla ÇOK GİZLİ, GİZLİ veya ÖZEL gizlilik dereceleriyle korunması gerekmeyen, ancak bilmesi gerekenler dışındaki kişiler tarafından bilinmesi durumunda gerçek ve tüzel kişilerin itibarını sarsacak bilgiler "hizmete özel" olarak sınıflandırılır.
- Çok gizli gizlilik dereceli evrak ve dokümanlar, Kurumun en üst düzey yöneticisi tarafından belirlenen ve yazılı olarak görevlendirilen kişi veya kişilertarafından hazırlanır ve özel usullere göre dağıtımı yapılır. Bu tip evrak ve dokümanlar korumalı odalarda, kasa, çelik masa veya diğer tipte çelik dolaplar içinde muhafaza edilir.
- Gizli, özel ve hizmete özel evrakların gizlilik derecesi, yazıyı hazırlayan makam tarafından tayin edilir. Gizli ve özel evraklar kilitli çelik dolaplarda, hizmete özel evraklar ise masa gözlerinde kilitli olmak şartıyla muhafaza edilir.
- Yukarıda sıralanan gizlilik derecelerinden hiçbirisi ile sınıflandırılmayan ve özel bir koruma gerektirmeyen evrak ve dokümanlar, "tasnif dışı" olarak kabul edilir.
- Tasnif dışı bir gizlilik derecesi olmayıp, evrakın yukarıda sıralanan gizlilik derecelerinden hiç biri ile sınıflandırılmamış olduğunu belirtir. Tasnif dışı belgeler için herhangi bir erişim kısıtlaması yoktur.
- Resmi yazı şeklinde hazırlanan ve uygun bir gizlilik derecesi ile sınıflandırılan belgelerin, elektronik ortamda hazırlanması ve dağıtılması ile ilgili hususlar için Sağlık Bakanlığı Elektronik Belge Yönetim Sistemi Yönergesinde belirtilen kurallar uygulanır.

FİZİKSEL VE ÇEVRESEL GÜVENLİK YÖNETİMİ:

Güvenli Alanlar:

- Fiziksel ve çevresel güvenlik tedbirlerinin belirlenmesi ve uygulamaya alınmasının ön koşulu hassas veya kritik bilgi ve bilgi işleme tesislerini barındıran güvenli alanların tespit edilmesi ve bu alanların güvenlik sınırlarının tanımlanmasıdır.
- Güvenlik sınırları belirlenirken kademeli bir yaklaşım kullanılır. Gerekiyorsa iç içe güvenli alanlar oluşturularak daha hassas ve kritik bilgilerin işlendiği alanlara erişim için birden fazla fiziksel sınırdan geçilmesi zorunlu hale getirilir.
- Güvenlik sınırları belirlenirken kişilerin kontrolsüz olarak giriş çıkış yapabilecekleri herhangi bir boşluk bulunmamasına dikkat edilir. Bu tür boşlukların kapatılması/korunması için ilave tedbirler alınır.
- Güvenli alanlar sadece yetkili personele erişim izni verilmesini temin etmek için uygun giriş kontrolleri ile korunur.
- Göreceli olarak daha az hassas varlıkların yer aldığı dış güvenlik sınırında alınan güvenlik tedbirleri ile kritik varlıkların yer aldığı iç güvenlik sınırlarındaki tedbirler farklılaştırılır.
- Sunucu odaları, güvenlik kontrol merkezleri, arşiv odaları vb. hassas bilgilerin işlendiği veya saklandığı alanlar kolayca ulaşılamayacak yerlere kurulur. Bu alanlara erişim uygun yöntemler kullanılarak sınırlandırılır.
- Giriş/çıkış yapılan yerler ve ortak kullanım alanları güvenlik kameraları ile kayıt altına alınır.

Ekipman Güvenliği:

- Hassas bilgiler içeren bilgi, belge ve evraklar masa üzerlerinde ya da kolayca ulaşılabilir yerlerde açıkta bulundurulmaz. Bu gibi bilgi ve belgeler kilitli dolap, çelik kasa ya da arşiv odası gibi fiziki koruması olan güvenli alanlarda muhafaza edilir.
- Yetkisiz kişilerin erişiminin engellenmesi için bilgisayar başından ayrılma durumunda ekran kilitlemesi yapılır. Otomatik ekran kilitlemesi devreye alınır.
- Sistemlerde kullanılan parola, telefon numarası ve T.C. kimlik numarası gibi bilgiler ekran üstlerinde veya masa üstünde bulundurulmaz.
- Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler imha edilir.
- Faks makinelerine gelen yazılar sürekli kontrol edilir ve makinede yazı bırakılmaması için tedbir alınır.
- Her türlü bilgiler, parolalar, anahtarlar ve bilginin sunulduğu sistemler, sunucular, kişisel bilgisayarlar ve benzeri cihazlar yetkisiz kişilerin erişebileceği bir şekilde parola korumasız ve fiziki olarak güvensiz bir şekilde gözetimsiz bırakılmaz.
- Fotokopi ve diğer çoğaltma teknolojilerinin (tarayıcı, sayısal kamera vb.) yetkisiz kullanımını önlemek için uygun idari ve teknik tedbirler alınır.

VARLIK YÖNETİMİ:

- "BY.YD.06 BİLGİ YÖNETİMİ RİSK ANALİZİ" nde "riske konu olan varlık bilgilerinin tanımlanması", "riske konu olan varlık ile ilgili tehdit ve zafiyetler", "risk tanımı ve detayları, risk değerleme (ilk dönem)", "risk iyileştirme planı (ilk dönem)", "bir sonraki dönem risk gözden geçirme ve yeniden değerleme" başlıklarıyla riskler belirlenerek,

değerlendirmesi, iyileştirilmesi ve gözden geçirilme süreçleri kayıt altına alınmaktadır. Risklere yönelik iyileştirmelerin gerçekleşme durumları ise 6 ayda 1 yapılan gözden geçirmeler ile takip edilmekte ve kayıt altına alınmaktadır.

İLETİŞİM GÜVENLİĞİ:

Ağ Güvenliği:

- Daha güvenli bir iletişim ortamı sağlamak maksadıyla ilimizdeki hastaneler ve Sağlık Müdürlüğü geniş alan ağı bağlantıları ve internet erişimleri SBA üzerinden sağlanır. Ağa bağlı sağlık tesislerinin internet erişimleri il toplama noktasında bulunan internet bağlantısı üzerinden gerçekleştirilir. Bu noktada sınır güvenliği için tesis edilmiş olan güvenlik duvarının yönetimi, İl Sağlık Müdürlüğünce görevlendirilen personel tarafından yapılır.
- Kablolama Güvenliği:
- Güç ve iletişim kabloları (ağ kabloları, güç kaynağı kabloları, telefon kabloları, vb.)
- binalar arası geçişte yeraltında, bina içlerinde kablo kanalları veya tavalar içerisinden geçirilir.
- Karışmanın (interference) olmaması için güç ve iletişim kabloları fiziksel olarak ayrılır.
- Hatalı bağlantıların olmaması için ekipman, kablolar ve prizler görülebilecek bir şekilde etiketlenir ya da işaretlenir.
- Dağıtım panelleri ve kenar anahtarların konulduğu kabinler yetkisiz erişime karşı kilitli olarak bulundurulur.
- Bahse konu kabinlerin de kesintisiz güç kaynağı ve jeneratör altyapısından faydalanması sağlanır.

BİLGİ GÜVENLİĞİ İHLAL OLAYI YÖNETİMİ:

- Hastanemiz kapsam dâhilinde, bilgi ve bilgi sistemlerini etkileyen güvenlik olaylarının tanımlanması, olayların nasıl ele alındığı ve / veya alınması gerektiğini, ihlal olaylarının sorumlularının belirlenmesi, olayların raporlanması ve işlenmesi için rehberlik sağlanması ve tüm çalışanlar tarafından bilgi güvenliği ihlal olaylarının rapor edilmesi; güvenlik ihlallerinin sonuçlarının hafifletilmesi ve gelecekteki güvenlik ihlallerinin azaltılmasına yönelik uygulamalar "BY.PR.09 Bilgi Güvenliği İhlali Yönetimi Prosedürü" doğrultusunda yapılmaktadır.

İŞ SÜREKLİLİĞİ YÖNETİMİ:

- Hasta kayıt işlemleri, başvuru yapan hastaların kimliklerini ibraz etmeleri koşulu ile yapılır.
- Başvuruda bulunan hastaların T.C Kimlik No'ları, iletişim bilgileri manuel olarak kayıt altına alınmak suretiyle yapılır.
- Kayıt esnasında MHRS randevusu olmayan başvurular için başvuru saatleri göz önüne alınarak sıra numarası verilir.
- Poliklinik hizmeti boyunca yapılan işlemlerden önce hastaların kimliklerini ibraz etmeleri zorunludur.
- Hastaların T.C. Kimlik No ları, ad ve soyadları manuel olarak kayıt altına alınır.
- Yapılan hizmetler, bilgileri alınan hastalar için diş numaraları ile birlikte manuel olarak kayıt altına alınır.
- Yapılan hizmetler boyunca kullanılan steril malzemelerin paket barkodları her hasta için saklanır.
- Hastalara düzenlenen reçeteler kağıt reçete olarak düzenlenir, doktor kaşe/imza ve sistem çalışmamakta kaşesi uygulanarak hastaya verilir.
- Sistem kesintisi giderildikten sonra, tüm başvular hasta kayıt personelleri tarafından oluşturulur.
- Kontrolü yapılan başvuruların, hizmetleri, reçeteleri ve kullanılan malzemeleri SBYS sistemine işlenir.

YEDEKLEME:

- Yedekleme, günde 4 defa merkez lokasyonda (Kırklareli Eğitim ve Araştırma Hastanesi) sistemin yoğun olmadığı zamanlarda yapılır.
- Hastanemizde web tabanlı HBYS kullanıldığından dolayı kurum bünyesinde fiziki olarak yedek tutulmamaktadır. Web tabanlı uygulama öncesinde alınan yedeklerin kayıtlarına hastanemizden ve güncel tutulan web üzerindeki yedeklerin kayıtlarına da istenildiği zaman Kırklareli Eğitim ve Araştırma Hastanesi bünyesindeki bilgi işlem biriminden ulaşılabilinmektedir.
- Yedekleme dosyaları HBYS'nin çalıştığı sunucu haricindeki bir ortama alınır.
- Yedekleme; harici bellek, taşınabilir kayıt ortamları veya ağ üzerinde çalışan yedek sunucu gibi bir ortamda saklanır.
- Devlet hastanelerinde kullanılan SBYS/HBYS yazılımları aşağıda belirtildiği şekilde yedeklenmektedir. Yedekleme Kırklareli Eğitim ve Araştırma Hastanesi'nde bulunan harici bilgisayarlara yapılmaktadır.
- Kullanılan Veri Tabanı Yönetim Sistemi: Açık Kaynak Kodlu MySQL Community Edition 8.0
- Veritabı İçin İşletim Sistemi: Oracle Linux Redhat 7 Enterprise Editions
- Uygulama Yazılımı İçin İşletim Sistemi: Microsoft Server 2016
- SBYS/HBYS yazılımları günlük 4 defa, haftalık (7 defa) ve aylık olarak anlık otomatik yedeklenir.

- Yedekleme işlemi Linux sistemi üzerine kurulan program ile alınarak sunucu ile koordineli çalışan yazılım ile otomatik harici bir bilgisayara alınır.
- Yedeklenen veriler DVD veya Blu-ray diske son kullanıcı kontrolünde alınır, tutanak karşılığında hastane idaresine teslim edilir.
- Herhangi bir olağanüstü durumda anlık yedek geri dönüşü ile sistemin sürekliliğini sağlamak mümkündür.
- Veri kaybı en alt düzeye indirgenmiştir.
- Alınan yedekleme ortamı, fiziksel olarak HBYS'nin üzerinde çalıştığı alanlardan farklı bir alanda/ farklı binada saklanır.
- Veriler offline ortamlarda süresiz olarak Kırklareli Eğitim ve Araştırma Hastanesi tarafından saklanır.
- Hastanemize ait her türlü belge, resim, video ya da ses dosyaları kullandıkları bilgisayar haricinde Raid10 seviyesinde 4 adet fiziksel hard diski bulunan ortak depolama cihazında (Qnap cihazı) yedeklenir. Alınan yedeklerin yılda iki kez geri dönüş testi yapılarak imza altına alınmaktadır.
- Yedeklemeden geri dönüşüm sağlanıp sağlanmadığı ve veri kaybının olup olmadığı kontrol edilir. Kırklareli Eğitim ve Araştırma Hastanesi tarafından BY.FR.07 HBYS YEDEKTEN VERİ KURTARMA TESTİ KAYIT FORMU ile kayıt altına alınır. Hastanemiz ile ortak sunucu üzerinden çalışıldığından kayıt formunun bir örneği tarafımıza gönderilir.
- Gerektiğinde iyileştirme çalışmaları başlatılır.

BİLGİ TEKNOLOJİLERİ İMHA YÖNETİMİ (BİLGİSAYAR, DİSK, SUNUCU VB)YÖNETİM SÜREÇLERİ:

- Kurumda verilerin depolandığı cihazlarda teknik ve fiziki nedenlerle kullanılmasında yarar görülmeyerek hizmet dışı bırakılması gerektiği sonucuna varılması halinde; veri depolama ünitesi bulunan ilgili cihazın Marka, Model Seri No/Sicil No gibi bilgileri kayıt edilerek, Kayıttan Düşme Teklif ve Onay Tutanağı ile tespit edilen taşınırların veri depolama üniteleri HEK komisyonda bulunan üyelerin gözetiminde imha edilir ve imha işlemleri kayıt altına alınır.

KÖTÜCÜL YAZILIMLARDAN KORUMA:

- Sunuculara yapılan erişimlerin raporlanması, mesai saati dışındaki erişimlerin işaretlenmesi gibi detaylar gözlenir. Kullanıcılara olması gerekenden fazla yetki tanımlanmaz.
- IOS güncellemeleri takip edilir. Sunucuların BIOS ayarlarının girişi parola ile korunur. Sunucuların varsayılan olarak CD-ROM, DVD-ROM veya flash disk gibi harici kaynaklardan başlatılması engellenir.
- Sunucu işletim sistemleri, güvenlik açıklarına karşı güncel tutulur.
- Virüs vb. zararlı yazılımlardan korunmak ve kurumsal bilgilerin kurum dışına sızmasını engellemek amacıyla gerekiyorsa USB bellek gibi taşınabilir cihazların kullanımı engellenir.
- Geliştirme ve test ortamları esas çalışma ortamından ayrılır. Yapılması planlanan işlemler öncelikle test ortamında denenir.
- Sunucularda yapılan işlemlerin iz kayıtlarına erişmek için olay günlükleri (event logs) tutulur.
- Tüm bilgisayarlar lisanslı anti-virüs yazılımı ile korunur. Anti-virüs yazılımının virüs veri tabanı güncel tutulur.
- Sunucu ve sistem güvenliğini sağlayabilmek için lisanslı yazılımlar kullanılır.
- İç erişim güvenliği için her bilgisayarda masaüstü erişim şifreleri ve HBYS kullanıcı kodu ve şifreleri kullanılır.

KRİPTOGRAFİK POLİTİKALAR:

- Kurumumuzda tüm resmi yazışmalar Elektronik Belge Yönetim Sistemi üzerinden yapılmaktadır. İmza yetkisi olan yöneticilerimiz, sayısal sertifika (e-imza) kullanarak evrak imzalamaktadır.
- Hekimlerimiz reçetelerini e-imza kullanarak imzalamaktadır.
- Kullanıcıların ara yüze bağlanmak için kullandıkları şifreler, şifreli biçimde veri tabanında saklanmaktadır. Veri tabanı sistem logları gerektiğinde hastane yönetimi tarafından izlenmektedir.

KİŞİSEL VERİLERİN KORUNMASI:

- Kurumumuz çalışanları ve vatandaşlar tarafından tespit edilen Sağlık Bakanlığı ile ilgili her türlü bilgi güvenliği ihlal olayı https://bilgiguvenligi.saglik.gov.tr/ adresinde yer alan merkezi ihlal bildirim sistemine girilir.
- Kişisel verilerin işlenmesine ilişkin süreçlerde 6698 sayılı kanunda yer alan usul ve esaslara uygunluk sağlanmalıdır.
- Veri tabanı üzerinde Hasta kayıt logları, Hasta Hizmet logları, Hasta Fatura Logları, Hasta Poliklinik logları, Tanımlama Logları, Hasta Dosya logları, Veri tabanı oturum logları, Sağlık kurulu kayıt logları kayıt altına alınmaktadır.
- Hastalarla ilgili her türlü kaydın kim tarafından, hangi tarihte girildiği, ulaşma, değiştirme bilgisi hastane bilgi işlem programı log kayıtları altında tutulmaktadır.

TEDARİKÇİ İLİŞKİLERİ:

- Sağlık kuruluşlarında kullanılacak tüm SBYS yazılımlarının Bakanlık tarafından yayımlanan sağlık bilişimi standartlarına ve veri gönderim servislerine uyumlu olmaları gerekmektedir. SBYS üreticisi firma, Bakanlık tarafından talep edilen geliştirmeleri ve güncellemeleri belirtilen süreler içerisinde sistemlerine yansıtmakla mükelleftir.
- SBYS yazılım üreticileri, Bakanlık Kayıt Tescil Sistemine (KTS) kayıt olarak akredite olurlar. Hizmet alınan firmanın KTS'ye kayıtlı olması şartı aranmaktadır. KTS'ye kayıt olan SBYS yazılım üreticileri Bakanlık tarafından yayımlanan sağlık bilişimi standartlarına uygunluk açısından denetlenir.
- Hastaneye destek hizmeti veren firmanın dış ortamdan iç ortama hangi durumlarda erişim yapacağı hakkında hastane tarafından onaylanmış gizlilik sözleşmesi mevcut olup dış ortamdan iç ortama erişimler kayıt altına alınmaktadır.
- Tedarik hizmeti alınan SBYS firmasının kurum içerisinde çalışan personeliyle gizlilik sözleşmesi imzalanır.
- Herhangi bir sebeple mevcut SBYS yazılımının kullanımına son verilirse, verilerin tamamı (orijinal veri tabanı formatında) ve VEM görüntüleri kolay ve sorunsuz okunabilir bir medya ortamında, 3 (üç) kopya halinde sağlık kuruluşuna teslim edilmek zorundadır.