1. **AMAÇ** Hastalara ait bilgilerin güvenliği, hastane diğer mail ve idari verilerin güvenliğinin sağlanması ve saklanması için alınacak tedbirlerin tarif edilmesidir.

2. **KAPSAM:** Bu talimat; hastanemizde bilgisayar kullanılan bilgilerin arşivlendiği, takip ve kontrol edildiği alanları, kullanıcıları, yöneticileri kapsar.

3. KISALTMALAR:
HBS : Hastane Bilgi Sistemi

4. TANIMLAR

5. SORUMLULAR:
insan Kaynakları Sorumlusu
Hasta Hakları ve Halkla ilişkiler Sorumlusu
Başhemşire
Branş Uzman Hekimi
Hasta Kabul Elemanı
Servis Hemşiresi
Santral Sorumlusu
Yatan Hasta Kabul Elemanı
Hasta Kabul Sorumlusu
Poliklinik Hemşireleri ve Sekreterleri
Ebe
Laboratuvar Teknikeri
Laboratuvar Sorumlu Teknikeri

6. FAALİYET AKIŞI:

6.1 Genel:

Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınmıştır.

Uygulama veya veri tabanı sunucularında donanım ve yazılıma ait problemler oluştuğunda, yetkili kişiler tarafından yerel veya uzak sistemden yeniden kesintisiz (veya makul kesinti süresi içerisinde) çalışma sağlanabilmektedi.r

Sistemin ne kadar süre ile ve ne kadar performans kaybını tolere edeceği dikkate alınacaktır. Bu durumu önleyici tedbirler alınacaktır.

Nevşehir Özel Kapadokya Hastanesi çalışanlarının, bilgi güvenliği ile ilgili acil bir durum oluştuğunda sorumlulukları dahilinde gerekli müdahaleyi yapabilmelerine yönelik standartlar şunlardır.

6.1.1 Acil Durum kapsamında değerlendirilen olaylar:

- **Seviye A:** Bilgi kaybı. Kurumsal değerli bilgilerin yetkisiz kişilerin eline geçmesi, bozulması, silinmesi.
- **Seviye B:** Servis kesintisi. Kurumsal servislerin kesintisi veya kesintisine yol açabilecek durumlar.
- **Seviye C:** Şüpheli durumlar. Yukarıda tanımlı ilk iki seviyedeki duruma sebebiyet verebileceğinden şüphe duyulan ancak gerçekliği ispatlanmamış durumlar.

6.1.2 Her bir seviyede tanımlı acil durumlarda karşılaşılabilecek riskler, bu riskin kuruma getireceği kayıplar ve bu riskler oluşmadan önce ve oluştuktan sonra hareket planları tanımlanacak ve dokümante edilecektir.

6.1.3 Acil durumlarda bilgi güvenliği yöneticisine erişilmeli, ulaşılamadığı durumlarda koordinayonu sağlamak üzere önceden tanımlanmış ilgili yöneticiye bilgi verilecek ve

zarar tespit edilerek süratle daha önceden tanımlanmış felaket kurtarma faaliyetleri yürütülecektir.

6.1.4 Bilgi İşlem Sorumlusu tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmeküzere Hastane Müdürlüğüne iletilecektir.

6.1.5 Olayın türü ve boyutuna göre emniyet veya diğer kurumlara başvurmak da gerekebilir. Bu özel olaylar (hırsızlık vb), başvurulacak kurumlar, başvuru şekli (telefon, dilekçe vb), başvuruyu yapacak kurum yetkilisi önceden belirlenmiş ve dokümante edilmiş olacaktır.

6.2 BİLGİ SİSTEMLERİNDE YEDEKLEME

Bilgi sistemlerinde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve olası bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigurasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesi gerekir. Sunucular ve veri depolama üniteleri yedekli olarak aynı veya uzak ortamlarda çalıştırılacaktır. Verinin de operasyonel ortamda online olarak aynı disk sisteminde farklı disk volümlerde ve DVD veya CD ortamında yedekleri alınacaktır. Taşınabilir ortamlar (Taşınabilir Disk, DVD veya CD) fiziksel olarak bilgi işlem odalarından faklı odalarda veya binalarda güvenli bir şekilde saklanır. Veriler offline ortamlarda süresiz olarak saklanır.

6.2.1 Kurumsal kritik verilerin saklandığı bölümler ile sistem kesintisinin kritik olduğu sistemlerin bir varlık envanteri çıkartılmalı ve yedekleme ihtiyacı bakımından sınıflandırılarak dokümante edilecektir.

6.2.2 Düzenli yedeklemesi yapılacak varlık envanteri üzerinde hangi sistemlerde ne tür uygulamaların çalıştığı ve yedeği alınacak dizin, dosya Bilgi sistemlerinde değişiklik yapmaya yetkili personel ve yetki seviyeleri dokümante edilecektir.

6.2.3 Yedekleme konusu bilgi güvenliği süreçleri içinde çok önemli bir yer tutmaktadır. Bu konuyla ilgili sorumluluklar tanımlanmalı ve atamalar yapılacaktır.

6.2.4 Yedekleri alınacak sistem, dosya ve veriler dikkatle belirlenmeli ve yedeği alınacak sistemleri belirleyen bir yedekleme listesi oluşturulacaktır.

6.2.5 Yedek ünite üzerinde gereksiz yer tutmamak üzere, kritiklik düzeyi düşük olan veya sürekli büyüyen izleme dosyaları yedekleme listesine dahil edilecektir.

6.2.6 Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilmeli ve güncellenecektir.

6.2.7 Yeni sistem ve uygulamalar devreye alındığında, yedekleme listeleri güncellenecektir.

6.2.8 Yedekleme işlemi için yeterli sayı ve kapasitede yedek üniteler seçilip, temin edilecektir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilecektir.

6.2.9 Yedekleme ortamlarının düzenli olarak test edilecek ve ortam ısısı kontrol altında bulundurulacak, acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanacaktır.

6.2.1O Geri yükleme prosedürlerinin düzenli olarak kontrol ve test edilerek etkinliklerinin doğrulanması ve operasyonel prosedürlerin öngördüğü süreler dahilinde tamamlanabileceğinden emin olunacaktır.

6.2.11 Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanacaktır.

6.2.12 Yedekleme Standardı ile doğru ve eksiksiz yedek kayıt kopyalarının bir felaket anında etkilenmeyecek bir ortamda bulundurulması ve kritik bilgiler için en az üç nesil yedekleme bilgisinin tutulması gerekir.

Veri Yedekleme Standardı; yedekleme sıklığı, kapsamı, gün içinde ne zaman yapılacağı, ne koşullarda ve hangi aşamalarla yedeklerin yükleneceği ve yükleme sırasında sorunlar çıkarsa nasıl geri dönüleceği, yedekleme ortamlarının ne şekilde işaretleneceği, yedekleme testlerinin ne şekilde yapılacağı ve bunun gibi konulara açıklık getirecek şekilde hazırlanmalı ve işlerliği periyodik olarak gözden geçirilmelidir.

7. VERİ TABANI GÜVENLİĞİ

Kritik verilere her türlü erişim işlemleri (okuma, değiştirme, silme, ekleme) loglanmalıdır. Log kayıtlarına idarenin izni olmadan kesinlikle hiçbir şekilde erişim yapılamamalıdır. Taşınabilir Disk, DVD veya CD ortamlarında tutulan log kayıtları en az 5 (beş) yıl süre ile güvenli ortamlarda saklanmalıdır. Veritabanı sunucularının güvenliği hakkında daha detaylı bilgi ve uyulması gereken kurallar şunlardır.

- Veritabanı sistemleri envanteri ve bu envanterden sorumlu personel tanımlanmalı ve dokümante edilmelidir.
- Veritabanı işletim kuralları belirlenmeli ve dokümante edilmelidir.
- Veritabanı sistem logları tutulmalı ve izlenmelidir.
- Veritabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli alınması kontrol altında tutulmalıdır.
- Yedekleme planları dokümante edilmelidir.
- Veritabanı erişim politikaları "Kimlik doğrulama ve Yetkilendirme" politikaları çerçevesinde oluşturulmalıdır.
- Hatadan arındırma, bilgileri yedekten dönme kuralları "Acil Durum Yönetimi" politikalarına uygun olarak oluşturulmalı ve dokümante edilmelidir.
- Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.
- Veritabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmaları yetkili bir personel gözetiminde yapılmalıdır.
- Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulmalı ve sonrasında ilgili uygulama kontrolleri gerçekleştirilmelidir.
- Bilgi saklama ortamlarının kurum dışına çıkarılması için yetkilendirme yapılması ve bu durumun izleme takip amacıyla kaydedilmesi gerekir.
- Sistem dokümantasyonu güvenli şekilde saklanmalıdır.
- İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için kurulacak temaslar belirlenmelidir.
- Veritabanı serverda sadece ssh açık olmalı ftp, telnet, remote vb. bağlantılara kapalı olmalıdır.
- Veritabanı servera veritabanı yöneticisi dışında hiçbir kullanıcı ssh bağlantı yapma yetkisi olmamalıdır.
- Application serverlardan veritabanına rlogin vb. şekilde erişememelidir.
- Veritabanı serverların şifresi sorumlu kişiler dışında bir zarfa yazılıp bantlanıp imzalanıp üst düzey yöneticisinin kasasında saklanmalıdır. Çok kritik bilgilere erişim için çift şifreleme mekanizması olmalıdır. Bu durumda en az iki kullanıcı bir şifreyi tamamlayacak olup birbirlerinin şifrelerini bilmeyeceklerdir.
- Arayüzden gelen kullanıcılar bir tabloda saklanmalı bu tablodaki kullanıcı adı ve şifreleri şifrelenmiş olmadır.

- Veritabanında güvenliği önemli veriler mutlaka şifrelenmelidir. Bu sayede verileri taşınsa bile orjinallerine erişilmemesi sağlanır.
- Veritabanı servera root olarak hiçbir kullanıcı bağlanmamalı. Bağlanması gereken kişilere kendi adında belli yetkilerle kullanıcı oluşturulmalıdır. Bu kullanıcıların yaptıkları işlemler loglanmalıdır. Root şifresi sadece sistem yöneticisinde olmalıdır.
- Veritabanında Veritabanı yöneticisi dışında SYSDBA,DBA yetkili kullanıcı olmamalıdır.
- Veritabanında bulunan farklı Schemaların kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenmelidir.
- Veritabanına internetten direkt bağlantı kesinlikle engellenmelidir.
- Veritabanı server a Sistem yöneticisi, Veritabanı Yöneticisi ve application server dışında hiçbir kullanıcı erişememelidir, ip bazında kısıtlana yapılmalıdır.
- Veritabanı servera kod geliştiren kullanıcı dışında hiçbir kullanıcı bağlanıp sorgu yapamamalıdır. istekler arayüzden sağlanmalıdır.(Kullanıcılara tablolardan select yapamamalılar).
- Veritabanına giden veri trafiği şifrelenmelidir. (Networku dinleyen verilere ulaşamamalıdır.)
- Bütün şifreler düzenli aralıklarla değiştirilmelidir. Detaylı bilgi için şifreleme politikasına bakılmalıdır.

8. ŞİFRELEME

Şifreleme, bilgisayar güvenliği için önemli bir özelliktir. Kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir şifre, ağ güvenliğini tümüyle riske atabilir. Güçlü bir şifreleme oluşturulması, oluşturulan şifrenin korunması ve bu şifrenin değiştirilme sıklığı hakkındaki standartlar ve uyulması gereken kurallar şunlardır.

a. Genel Bilgiler

- Bütün sistem seviyeli şifreler (örnek, root, administrator, enable, vs) en az üç ayda bir değiştirilmelidir.
- Bütün kullanıcı seviyeli şifreler (örnek, e-posta, web, masaüstü bilgisayar vs.) en az altı ayda bir değiştirilmelidir. Tavsiye edilen değiştirme süresi her dört ayda birdir.
- Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.
- Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.
- SNMP kullanıldığı durumlarda varsayılan olarak gelen "public", "system" ve "private" gibi community string'lere farklı değerler atanmalıdır.
- Kullanıcı, şifresini başkası ile paylaşmaması, kağıtlara yada elektronik ortamlara yazmaması konusunda eğitilmelidir.
- Kurum çalışanı olmayan harici kişiler için açılan kullanıcı hesaplarının şifreleri de kolayca kırılamayacak güçlü bir şifreye sahip olmalıdır.
- Bütün kullanıcı ve sistem seviyeli şifrelemeler aşağıdaki ana noktalara uymalıdır.

b. Genel Şifre Oluşturma Kuralları

Şifreler değişik amaçlar için kullanılmaktadır. Bunlardan bazıları: Kullanıcı şifreleri, web erişim şifreleri, e-posta erişim şifreleri, ekran koruma şifreleri, yönlendirici erişim şifreleri vs.). Bütün kullanıcılar güçlü bir şifre seçimi hakkında özen göstermelidir.

(1) Zayıf şifreler aşağıda belirtilen karakteristiklere sahiptir.

- Şifreler sekizden daha az karaktere sahiptirler.
- Şifreler sözlükte bulunan bir kelimeye sahiptir.

Şifreler aşağıdak i gibi ortak değere sahiptir.

Ailesinin, arkadaşının, sahip olduğu bir hayvanın veya bir sanatçının ismine sahiptir.
- Bilgisayar terminolojisi ve isimleri, komutlar, siteler, şirketler, donanım veya yazılım gibi.
- "Sağlık", "istanbul" , "ankara" gibi isimler.
- Doğum tarihi veya adres ve telefon numaraları gibi kişisel bilgiler.
- Aaabbb, qwerty,zyxwuts, 123321 vs. Gibi sıralı harf veya rakamlar.
- Yukardaki herhangi bir kelimenin geri yazılış şekli.
- Yukarıdaki herhangi bir kelimenin rakamla takip edilmesi (örnek ,gizli1, gizli2).

(2) Güçlü şifreler aşağıdaki karakteristiklere sahiptir.
- Küçük ve büyük karakterlere sahiptir (örnek, a-z, A-Z)
- Hem dijit hemde noktalama karakterleri ve ayrıca harflere sahiptir. (0-9, !@#$%"&*()_+ı~-=\'{}[]:";'<>?,./)
- En az sekiz adet alfanümerik karaktere sahiptir.
- Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.
- Aile isimleri gibi kişisel bilgilere ait olmamalıdır .
- Şifreler herhangi bir yere yazılmamalıdır veya elektronik ortamda tutulmamalıdır.
- Kolayca hatırlanabilen şifreler oluşturulmalıdır. örnek olarak; "olmaya devlet cihanda bir nefes sıhhat gibi" cümlesi "OdC1nSg!" veya türevleri şeklinde olabilir.

Not: Yukarıdaki herhangi bir örneği şifre olarak kullanmayınız.

(3) Şifre Koruma Standartları

Sağlık Bakanlığı bünyesinde kullanılan şifreleri hastane dışında herhangi bir şekilde kullanmayınız. (örnek, internet erişim şifreleri, bankacılık işlemlerinde veya diğer yerlerde). Değişik sistemler için farklı şifreleme kullanın. Örnek, Unix sistemler için farklı şifre, Windows sistemler için farklı şifre kullanınız.

Sağlık Bakanlık bünyesinde kullanılan şifreleri herhangi bir kimseyle paylaşmayınız. Bütün şifreler Sağlık Bakanlığına ait gizli bilgiler olarak düşünülmelidir.

(4) Aşağıdakiler yapılmayacakların listesidir:
- Herhangi bir kişiye telefonda şifre vermek.
- e-posta mesajlarında şifre belirtmek.
- üst yöneticinize şifreleri söylemek.
- Başkaları önünde şifreler hakkında konuşmak.
- Aile isimlerini şifre olarak kullanmak.
- Herhangi form üzerinde şifre belirtmek.
- Şifreleri aile bireyleri ile paylaşma k.
- Şifreleri işten uzakta olduğunuzzamanlarda iş arkadaşlarınıza bildirmek.

Herhangi bir kimse şifre isteğinde bulunursa bu dokümanı referans göstererek Bilgi İşlem birimi yetkilisini aramasını söyleyiniz.

Uygulamalardaki "şifre hatırlama" özelliklerini seçmeyiniz. (örnek, Outlook, Internet Explorer vs.)

Tekrar etmek gerekirse, şifreleri herhangi bir yere yazmayınız ve herhangi bir ortamda elektronik olarak saklamayınız.

Şifreler an az altı ayda bir değiştirilmelidir (sistemlerin şifreleri ise en az üç ayda bir değiştirilmelidir). Tavsiye edilen aralık ise 3 ayda birdir.

Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıya şifresini değiştirmesi talep edilecektir.

9. 11 Uygulama Geliştirme Standartları

11.1 Uygulama geliştiricileri programlarında aşağıdaki güvenlik özelliklerinin sağlandığından emin olmalıdırlar.

11.2 Bireylerin (grupların değil) kimlik doğrulaması (authentication) işlemini destekleyebilmelidir.

11.3 Şifreleri text olarak veya kolay anlaşılabilir formda saklamamalıdır.

11.4 Kural yönetim sistemini desteklemelidir. (Örnek; bir kullanıcı diğer bir kimsesin şifresini bilmeden fonksiyonlarına devam edebilmesi.)

11.5 Mümkün olduğu kadar TACACS+ , RADIUS ve/veya X.509/LDAP güvenlik protokollerini desteklemelidir.

1O. **12 Uzaktan Erişen Kullanıcılar için Şifre Kullanımı**

Kurumun bilgisayar ağına uzaktan erişim tek yönlü şifreleme algoritması veya güçlü bir passphrase ile yapılacaktır.

12.1 Passphrase

Bir passphrase standart şifrelerden daha uzun karakter dizisine sahiptir (genellikle 4'ten 16'ya kadar karaktere sahiptir), dijital imzaların (bir mesajı gönderen kişinin gerçekten o kişi olduğunu kanıtlayan kodlanmış bir imza), mesajların kodlanması veya çözülmesinde kullanılır.

Passphrase'ler şifreler gibi değildir. Passphrase şifrelerden daha uzundur, dolayısı ile daha güvenlidir.

Passphrase'ler tipik olarak birçok kelimeden ibarettir. Bundan dolayı passphrase'ler "sözlük" saldırılarına karşı daha güvenlidir.

İyi bir passphrase büyük ve küçük harf ve rakamlardan oluşan kombinasyona sahiptir.

örnek bir passphrase:

"*?#>*@1012inciCaddekiTrafik*&#!#BuSabah"

Şifrelem . için gE:ÇE:rli olan bütün kurallar passphrase'ler için de geçerlidir.

11. SUNUCU GUVENLIGI

Sunucuların güvenliğinin sağlanması için uyulması gereken kurallar ve standartlar şunlardır.

a. Genel Bilgiler

(1) Sahip Olma ve Sorumluluklar

Kurum bünyesindeki bütün dahili sunucuların yönetiminden sistem yöneticileri sorumludur.

Sunucu konfigurasyonları sadece bu grup tarafından yapılacaktır.

12.1.1.1.Bütün sunucular ilgili kurumun yönetim sistemine kayıt olmalıdır. En az aşağıdaki bilgileri içermelidir:

- Sunucuların yeri ve sorumlu kişi.
- - Donanım ve işletim Sistemi.
- - Ana görevi ve üzerinde çalışan uygulamalar.
- - İşletim Sistemi versiyonları ve yamalar.
- Bütün bilgiler tek bir merkezde güncel olarak tutulmalıdır.

(2) Genel Konfigurasyon Kuralları

- İşletim sistemi konfigurasyonları Bilgi İşlem Biriminin talimatlarına göre yapılacaktır.
- Kullanılmayan servisler ve uygulamalar kapatılacaktır.
- Eğer mümkünse servislere erişimler için log tutulacak (örnek; TCP Wrapper) ve erişim kontrol metotlarıyle koruma sağlanacaktır.
- Sunucu üzerinde çalışan işletim sistemlerinin, hizmet sunucu yazılımlarının ve anti-virüs vb. koruma amaçlı yazılımların sürekli güncellenmesi sağlanmalıdır. Mümkünse, yama ve anti virüs güncellemeleri otomatik olarak yazılımlar tarafından yapılmalı, ancak değişiklik yönetimi kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanmalıdır.
- Uygulama erişimleri için standart güvenlik prensiplerini çalıştırın, gereksiz servisleri açmayın.
- Sistem yöneticileri gerekli olmadığı durumlar dışında "Administ rator" ve "root" gibi genel kullanıcı hesapları kullanmamalı, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmalıdır. Genel yönetici hesapları yeniden adlandırılmalıdır. Gerekli olduğunda önce kendi hesapları ile log-on olup, daha sonra genel yönetici hesaplarına geçiş yapmalıdırlar.
- Ayrıcalıklı bağlantılar teknik olarak mümkünse güvenli kanal (SSH veya IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
- Sunucular fiziksel olarak erişim kontrollü sistem odalarında bulunmalıdırlar.

(3) Gözlemleme

- Kritik sistemlerde oluşan bütün güvenlikle ilgili olaylar loglanmalıdır ve aşağıdaki şekilde saklanmalıdır:
- Bütün güvenlikle ilgili loglar minimum 1 hafta saklanmalıdır ve online olarak erişilmelidir.
- Günlük tape backupları en az 1 ay saklanmalıdır.
- Logların haftalık tape backupı en az 1 ay tutulmalıdır.
- Aylık full backuplar en az 6 ay tutulmalıdır.
- Güvenlikle ilgili loglar sorumlu kişi tarafından değerlendirilecek ve gerekli tedbirleri alacaktır. Güvenlikli ilgili olaylar aşağıdaki gibi olabilir fakat bunlarla sınırlı değildir.
    - Port tarama atakları
    - Yetkisiz kişilerin ayrıcalıklı hesaplara erişmeye çalışması.
    - Sunucuda meydana gelen mevcut uygulama ile alakalı olmayan anormal olaylar.

(4) Uygunluk

- Denetimler yetkili organizasyonlar tarafından Bakanlık bünyesinde belli aralıklarda yapılacaktır.
- Denetimler Bilgi İşlem grubu tarafından yönetilecektir.
- Denetimler organizasyonun işleyişine zarar vermemesi için maksimum gayret österilecektir.

(5) işletim

- Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir.
- Sunucuların yazılım ve donanım bakımları üretici tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılmalıdır.

- Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve kayıt edilmelidir.

12. KİMLİK DOĞRULAMA VE YETKİLENDİRME

Bilgi sistemlerinde Kimlik Doğrulama ve Yetkilendirme, konusunda alınması gereken önlemler, uyulması gereken kurallar ve standartlar şunlardır.

- Kurum sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecek ve dokümante edilecektir.
- Kurum sistemlerine erişmesi gereken kurum dışı ve extranet kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanacak ve dokümante edilecektir.
- Bakanlık bünyesinde kullanılan ve merkezi olarak erişilen tüm uygulama yazılımları, paket programlar, veritabanları, işletim sistemleri ve log-on olarak erişilen tüm sistemler üzerindeki kullanıcı rolleri ve yetkiler belirlenmeli, dokümante edilmeli ve denetim altında tutulmalıdır.
- Tüm kurumsal sistemler üzerindeki kullanım hakları (kullanıcıların kendi sistemlerine yönelik olarak birbirlerine verdikleri haklar dahil) periyodik olarak gözden geçirilmeli ve gereksinimler ve gerekli minimum yetkinin verilmesi prensibi doğrultusunda revize edilmelidir.
- Erişim ve yetki seviyelerinin sürekli güncelliği temin edilmelidir.
- Kullanıcılar kurum adına kullanımları için tahsis edilmiş sistemlerin güvenliğinden sorumludurlar.
- Sistemlere başarılı ve başarısız erişim logları düzenli olarak tutulmalı, tekrarlanan başarısız log-on girişimleri incelenmelidir.
- Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.
- Sistemlere log-on olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve yetki ihlalleri kontrol edilmelidir.
- Kullanıcılara erişim haklarını yazılı olarak beyan edilmeli ve erişim haklarını ihlal eden kullanıcılar için ilgili politika maddesi uygulanmalıdır.
- Kullanıcı hareketlerini izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.
- Sistemler üzerindeki tüm roller, rollere sahip kullanıcılar, ve rollerin sistem kaynakları üzerindeki yetkileri, uygun araçlar kullanılarak belirli aralıklarla listelenmelidir. Bu listeler yetki matrisleri ile karşılaştırılmalıdır. Eğer uyumsuzluk var ise nedenleri araştırılmalı, ve dokümanlar veya yetkiler düzeltilerek uyumlu hale getirilmelidir.

13. KİŞİSEL SAĞLIK KAYITLARININ GÜVENLİĞİ

Kişisel sağlık kaydı kapsamına, hasta ile ilgili sözlü bilgi, yazılı bilgi, tıbbı müdahaleler, ön tanı, teşhisler, grafik imajları, fatura gibi konular girmektedir.
Kişisel sağlık kayıtlarının güvenliğinin sağlanması amacıyla; Sağlık Bakanlığına tarafından istenilen hasta sağlık bilgisinin mahremiyeti hususunda uyulması gereken temel kurallar şunlardır.

a. Genel Kurallar

Bütün kişisel ve kurumsal bilgilerin (klinik, idari, mali vb.) güvenliğinin sağlanması için aşağıda belirtilen hususlara dikkat edilmelidir.

- Veri güvenliği konusunda üç temel prensibin göz önüne alınması gerekmektedir. Bunlar; gizlik, bütünlük ve erişilebilirliktir.
- Kurumda kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi tanımlanmalıdır. Rol bazlı yetkilendirme yapılmalıdır ve yetkisiz kişilerin hastanın sağlık kayıtlarına erişmesi mümkün olmamalıdır.
- Sağlık kayıt bilgileri hastaya aittir. Yetkilendirilmiş çalışanlar ancak kendisine kayıtlı olan hastaların sağlık kayıtlarına erişebilmelidirler. Ancak hastanın yazılı onayı ile diğer sağlık çalışanları bu veriye erişebilirler.
- Hasta taburcu olmuş ise hiçbir kurum çalışanı hastanın sağlık kayıtlarına erişemez.
- Hastanın rızası olmadan hiçbir çalışan sözle de olsa hasta sağlık bilgilerini hastanın yakınları dışında üçüncü şahıslara ve kurumlara iletemez.
- Hasta sağlık bilgileri ticari amaçlı olarak da üçüncü şahıslara iletilemez. Hastanın kullandığı ilaçlar, diyet programları vs. buna dahildir.
- Hasta dosyasının bir kopyası hastaya teslim edilmelidir. İlgili mevzuat hükümleri saklı kalmak kaydıyla hiç bir hasta kaydı, elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilmemelidir.
- Hastanın dosyasının izlenmemesi için gerekli tedbirler alınmalıdır. [Hasta dosyalarının gelişigüzel ortada bırakılmaması, bilgisayar ekranının başkalarınca okunabilecek şekilde bırakılmaması gibi]
- Telefon ile konuşurken hasta ile ilgili mahrem bilgilerin üçüncü şahısların eline geçmemesine azami özen göstermelidir.
- Bütün hasta sağlık kayıtları fiziksel olarak korunmuş mekanlarda saklanmalıdır.
- Elektronik hasta kayıtlarına internet ortamından erişim mümkün olmamalıdır.
- Hasta sağlık bilgileri bilginin üretildiği kurum tarafından veya Bakanlığımızın Bilgi Yönetim sistemleri tarafından araştırma, istatistik ve Karar Destek Sistemleri için kullanılabilir. Bu durumda hasta sağlık bilgisi hasta tanımlayıcısı ile ilişkilendirilemez.

14. Sistem Güvenliği

a. Veriye erişirken dört temel prensibin gerçekleştirilmesi gerekmektedir. Bunlar; İzlenebilirlik, kimlik sınama, güvenirlik ve inkar edilememedir.

b. Sağlık kurumları bünyesinde hasta tanımlayıcı olarak TC Kimlik numarası baz alınacaktır. Veri tabanlarında hiçbir zaman hastalık tanısı ile TC kimlik numarası eşleşmeyecek, TC kimlik numarasından tek yönlü algoritma ile türetilmiş özel bir tanımlayıcı numara kullanılacaktır.

c. Bilgi sistemlerinde güvenlik veriye erişim bazında olacaktır. Bunun için bu sistemin özellikle yazılım ve veritabanı erişim katmanlarında özel uygulamalar oluşturulacaktır.

d. Veriye erişecek kişiler aşağıdaki şekilde tanımlanmıştır:

Bu amaçla; BIL.TL.02 Bilgi İşlem Yetkilendirme Talimatı hazırlanmıştır .

- Hastanedeki yetkilendirilmiş sağlık çalışanları ise, ancak hastanın giriş tarihinden, taburcu olana kadar geçen zaman içerisinde ve ancak hasta kendisi ile ilgili sağlık kayıtlarının erişimine yazılı olarak onay vermiş ise hastanın elektronik sağlık kayıtlarına erişebilirler. Ve bu da "geçici bir süreliğine"olacaktır.
- Sistem yöneticilerine de bir güvenlik katmanı konulacaktır. Bunun için veritabanı yazılımının gelişmiş güvenlik yönetim i özellikleri kullanılacaktır.

- Gerektiğinde saat ve/veya gün bazında belirlenen bir sure için bazı kullanıcı ve istemci makinelerin sisteme oturum açmalarına kısıtlama getirilebilmelidir.
- Aynı kullanıcı kodu ile aynı anda birden fazla oturum açılmasına izin verilmemelidir.
- Eğer hasta, herhangi bir sağlık çalışanının elektronik sağlık kayıtlarına erişmesini istemiyorsa, sağlık çalışanı ilgili dosyayı okuma hakkına kavuşamamalıdır. Fakat sağlık çalışanı muayene sonuçlarını hastanın veri tabanına aktarabilmelidir. Bu diğer doktorlar tarafından yazılan kayıtlara erişilmemesi için kullanılan metottur.
- Sadece yetkisi olan kullanıcılar için veri girişi ve/veya verinin elde edilmesi için erişim izni verilmelidir. Birçok kullanıcının veri tabanında sadece belirli bir veri setine erişim yetkisinin denetlenebilmesini sağlamak için çok katmanlı denetim mekanizmaları olmalıdır.
- Veri tabanında tutulacak verilerin tutarlılığı tam ve kesin bir şekilde sağlanmalıdır. Bunu sağlamak için en azından, veri onay (validation), çapraz sorgulama (cross-checking) ve mükerrer kayıt önleme gibi ölçütler uygulanmalıdır.
- Yönetimsel analizler yapmak için veri tabanındaki veriler bir yerden başka bir yere aktarılırken, kayıtlarda bulunan kişisel kimlik tanımlayıcıları kayıtlardan çıkartılmalı ve analizler hasta ile hastalık bilgilerini eşleştirmeden yapılmalıdır.
- Kullanıcı aktiviteleri (yapılan tüm işlemler ve erişimler) izlenebilmelidir. Veri tabanı üzerinde yapılan şüpheli işler denetlenebilmelidir. Sistemin hem etkin bir şekilde yönetilmesi, hem de yetkisiz erişimlerin engellenmesi ve izlenmesi anlamında gelişmiş bir kontrol mekanizması olmalıdır. Sistem, hangi kullanıcının sistemin hangi kısmına ne zaman ve nereden eriştiğine dair (zaman damgası-date stamp, işlem, kullanılan istemci bilgisayar tanımı gibi bilgileri de içeren) kayıt tutmalıdır.
- Sistem yöneticilerinin kimlik tanımlama ve doğrulaması için X.509v3 uyumlu sayısal sertifikalar kullanılmalıdır. Sayısal sertifikaların güvenli depolaması için akıllı kartlar veya usb teken cihazları kullanılmalıdır.
- Sertifika tabanlı kimlik doğrulama yapılmadığı halde password ve hash tabanlı kimlik doğrulama yapılacaktır. Sistemlere erişim için tek yönlü şifreleme algoritmaları kullanılacaktır.

Hastane içerisinde veya hastane ile başka ağlar arasındaki tüm haberleşme şifreli yapılmalıdır.

Bütün iletişim VPN ve Açık Anahtar Alt Yapısı (PKI) teknolojilerini kullanmalıdır.