YATAKLI TEDAVİ KURUMLARI TIBBÎ KAYIT VE ARŞİV HİZMETLERİ YÖNERGESİ

(Sağlık Bakanı'nın 06.11.2001 tarih ve 10588 sayılı olurları ile yürürlüğe girmiştir.)

BİRİNCİ BÖLÜM

Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

Madde 1 - Bu Yönergenin amacı, yataklı tedavi kurumlarına muayene, teşhis ve tedavi amacıyla gelen hastalara, yaralılara, acil ve adlî vak'alara ait kayıtların, düzenlenen ve kullanılan dokümanların toplanmasına ve bu dokümanların hastaların daha sonraki başvurularında veya araştırmacılar veyahut adlî makamlarca her istenildiğinde derhal hazır bulundurulması için merkezi tıbbî kayıt ve arşiv sistemi içinde tasnif ve muhafaza

edilmesine ilişkin usûl ve esasları belirlemektir.

Kapsam

Madde 2 - Bu Yönerge, Sağlık Bakanlığı'na bağlı yataklı tedavi kurumlarını ve bu kurumlardaki tıbbî kayıt ve arşiv hizmetlerini kapsar.

Dayanak

Madde 3 - Bu Yönerge, 13/1/1983 tarihli ve 17927 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Yataklı Tedavi Kurumları İşletme Yönetmeliği'nin 32 nci maddesine dayanılarak hazırlanmıştır.

Tanımlar

Madde 4 - Bu Yönerge'de geçen;

a) Hasta dosyası : Yataklı tedavi kurumlarına müracaat eden hastaların, muayene, teşhis ve tedavi evrakının muhafaza edildiği; A4 kağıdı boyutlarında,

kenarlarında **(EK-1)** ve **(EK-2)'**de düzenlenen forma uygun renkli şeritler bulunan

kartondan imal edilmiş ve iki kapaktan oluşan telli saklama aracını;

b) Vekil Dosya : Arşivden çıkarılan dosyaların dosya izleme fişiyle takip

edilmesi amacıyla, asıl dosyanın yerine geçici olarak konulan ve asıl dosya ile aynı

ebatlardaki, biri A4 kağıdı boyutunda diğeri büyük cebin üstünde dosya izleme fişinin

konulacağı şeffaf iki ayrı cebi olan, **(EK-3)'**deki forma uygun olarak düzenlenen; araştırma

için alınan ve diğer birimlere gönderilenlerin ayrı renkte olduğu plastik dosyayı;

ifade eder.

Organizasyon ve idare

Madde 5- Yataklı tedavi kurumlarında, idaresi ve organizasyonu aşağıdaki gibi

olan bir merkezi tıbbî arşiv kurulur.

TIBBî KAYIT VE ARŞİV HİZMETLERİ YÖNETİM VE

ORGANİZASYON ŞEMASI

Merkezî tıbbî arşive konulacak dosyalar

Madde 6 - Merkezi tıbbî arşivde bütün servislere ve ayrıca Yataklı Tedavi

Kurumları İşletme Yönetmeliği'nin 66 ncı maddesine göre yatırılan hastalara ait ve

polikliniklerde işi biten dosyalar, bir sıra ve düzen içerisinde muhafaza edilir.

İKİNCİ BÖLÜM

Merkezî Tıbbî Arşivin Bölümleri, Hasta Dosyasına Konulacak Belgeler

Merkezî tıbbî arşivin bölümleri

Madde 7 - Merkezi tıbbî arşiv, şu bölümlerden oluşur:

a) Hasta endeksi bölümü,

b) Eksik dosyalar bölümü,

c) Dosyalama bölümü,

d) Tıbbî sekreterlik bölümü,

e) Tıbbî istatistik ve kodlama bölümü.

Eğitim ve araştırma hastaneleri ile yatak sayısı 400 ve daha fazla olan genel ve

özel dal hastanelerinde adlî vakalara ait işlemlere ilişkin yazışmaların yürütülmesi ve

araştırmacıların talep ettiği araştırma ve inceleme dosyalarını çıkartmak üzere bir araştırma

ve haberleşme bölümü kurulur. Yatak sayısı 100'ün altındaki hastane arşivleri, bölümlere ayrılmaz.

Hasta endeksi bölümü

Madde 8 - Hasta endeksi bölümü; polikliniklere müracaat eden ve yatışı yapılan bütün hasta ve yaralıların dosyaları ile birlikte açılan endeks kartlarını **(Form-1)'**e uygun olarak alfabetik sıra içerisinde düzenlemek ve bilinmeyen hasta dosyası numaraları sorulduğunda, bunları temin etmekle yükümlüdür.

Eksik dosyalar bölümü

Madde 9 - Eksik dosyalar bölümü; yatan hastalar taburcu edildiğinde hasta kabul bölümünden liste karşılığı dosyaları günlük olarak teslim alıp analizlerini yaparak, eksik belgeleri tamamlar; epikrizlerini müdavi tabibe yazdırıp imzalatır; epikrizlerini

yazmakta ihmâli görülen tabiplerin isimlerini baştabipliğe resmî yazı ile bildirir.

Dosyalama bölümü

Madde 10 - Bu bölüm hasta dosyalarının, "renkli kod sistemine" göre sıralanması, gerektiğinde polikliniklerden gelen dosya istek fişi formuna uygun olarak verilmesi, verilen dosya yerine vekil dosya konulması, her gün bütün polikliniklerden saat 15.00'de liste karşılığı alınan dosyaları yerine kaldırma işlemini yürütür.

Dosyalama bölümü raporları ve M1'leri dosyalarına kaldırır. Yıpranmış olan dosyaların renk sistemine göre yenisini düzenler.

Dosyaların bulunmasında zaman kaybını azaltmak, tasnifini kolaylaştırmak ve yanlış yere kaldırılmasını önlemek amacıyla her harfe bir renk gelecek şekilde yüzlük bölümler halinde son iki rakama renk verilmeden dosyalama sistemi açıklama formuna **(EK-4)** uygun renkli dosyalama sistemi oluşturulur.

Tıbbî sekreterlik bölümü

Madde 11 - Tabiplerin el yazısı ile yazılmış veya diktafonlara dikte edilmiş çıkış özeti, ameliyat notu gibi hasta ile ilgili çeşitli bilgilerin özel formlar üzerine daktilo edilmesi tıbbî sekreterlikçe yürütülür. Cumhuriyet savcılıklarından intikal eden müzekkerelerin takibinden ve cevaplandırılmasından bu bölüm sorumludur.

Hasta dosyasına konulacak belgeler

Madde 12 - Hasta dosyasında şu belgeler bulunmalıdır:

a) Hasta kabul kağıdı (Form 60),

b) Tıbbi müşahade ve muayene kağıdı (Form 62),

c) Derece kağıdı (Form 61),

d) Hasta tabelası (Form 51),

e) Röntgen istek kağıdı ve raporları (Form 64),

f) Laboratuvar istek kağıdı ve tetkik raporları (Form 65),

g) Ameliyat kağıdı (Form 63),

h) Hastanın muayene istek formu (Form 67),

i) Çıkış özeti (Form 67).

Hasta dosyaları **(Form-2)'**ye uygun olarak hastalık kodlama kartı doldurulmak

suretiyle dosyalama bölümüne gönderilir.

Tıbbî istatistik ve kodlama bölümü

Madde 13 - Tıbbî istatistik ve kodlama bölümünün görevleri şunlardır;

a) Dünya Sağlık Teşkilatınca yayınlanan "150 Başlıklı Liste"deki tanılara göre

999, ameliyatlara göre 99 başlığa göre sınıflandırılıp kodlaması yapılır. Kodlaması yapılan

dosyalar teşhis ve ameliyatlara göre ayrı ayrı karta geçirilerek kendi arasında sınıflanıp

endeks kutularına kaldırılır.

b) Tıbbî araştırmalarda dosyalar, vekil dosya ve zimmet karşılığı araştırmacıya

verilir.

c) Araştırma ve haberleşme bölümü kurulan hastanelerde araştırma ve inceleme

dosyaları bu bölüm tarafından çıkartılır.

d) Hasta ve yaralılara uygulanan tedavi usûlleri ve bu konudaki çalışmaların

verimini tespit etmek ve ileriye dönük planlama yapabilmek için yatan ve ameliyat olan

hastalara ait bilgiler bu bölüm tarafından uluslararası esaslara göre tasnif edilir ve

kodlaması yapılır.

e) (Form-56) ile bildirimi zorunlu hastalıklar, verem (tüberküloz), zehirlenme,

AİDS, kadın ve ana ölümleri, kanser vakalarına ilişkin bilgileri sağlık müdürlüklerine

bildirir.

Servis sekreterleri

Madde 14 - Servis sekreterleri şu görevleri yerine getirir:

a) Yatış kağıdını kontrol eder, hastanın adı, soyadı, baba adı, dosya numarası,

doğum tarihi, medeni durumu, cinsiyeti, işi ve adresi, teşhisi, yatıran tabibin isim kaşesi ve

imzası eksikse tamamlanmasını sağlar.

b) Hastanın yatmasından taburcu olmasına kadar kullanılan bütün formlar ile

biyopsi, EKG, sitopatoloji, röntgen, anestezi gibi raporları hasta dosyasına koyar ve bunun

takibini yapar.

c) Hasta taburcu olurken, resmî hastaların raporlarının ilgili tabipçe yazılmasını

sağlar; taburcu notunu kontrol eder ve hasta dosyasını hasta kabul bölümüne gönderilmeden

önce 12 nci maddedeki sıralamaya göre düzenler.

Adli vak'alara ilişkin kayıtların muhafazası

Madde 15 - Adli vak'alara ilişkin tüm tahlil, tetkik sonuçları ile her türlü kayıt, dökümanlar ve hasta dosyalarının en az yirmi yıl süreyle yataklı tedavi kurumunun arşivinde muhafazası zorunludur.

ÜÇÜNCÜ BÖLÜM

Son Hükümler

Hüküm öngörülmeyen haller

Madde 16 - Bu Yönerge'de hüküm öngörülmeyen ve açıklık getirilmeyen hususlarda, 16/5/1988 tarihli ve 19816 sayılı Resmî Gazete'de yayımlanarak yürürlüğe giren Devlet Arşiv Hizmetleri Hakkında Yönetmelik hükümleri uygulanır.

Yürürlükten kaldırılan hükümler

Madde 17 - Yataklı Tedavi Kurumları Merkezi Tıbbî Arşiv Yönergesi

hükümleri yürürlükten kaldırılmıştır.

Yürürlük

Madde 18 - Bu Yönerge, Bakan Onayı ile yürürlüğe girer.

Yürütme

Madde 19 - Bu Yönerge hükümlerini Sağlık Bakanı yürütür.

Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arşiv Hizmetleri Yönergesinde Değişiklik Yapılmasına Dair Yönerge

06.06.2007 tarihli ve **5228** sayılı makam onayı ile yürürlüğe girmiştir.

MADDE 1- Bakanlık Makamının 06.11.2001 tarih ve 10588 sayılı olurlarıyla yürürlüğe giren Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arşiv Hizmetleri Yönergesinin Ek 1 inci maddesinin birinci fıkrası aşağıdaki şekilde değiştirilmiş, birinci fıkradan sonra gelmek üzere aşağıdaki fıkralar eklenmiştir.

"(6.6.2007-5228 sayılı onayla değişik) Kurumlarda kağıt üzerinde tutulan, kurum dışına çıkmayan ve hukuken ıslak imza gerektirmeyen poliklinik defterleri, laboratuar defterleri, yatan hasta takip kartları, anamnez formları, tedavi takip kartları gibi sağlık kayıtları ve belgeleri, lüzumu halinde istenilen içerik ve formatta çıktıları alınacak şekilde olmak şartıyla, elektronik imza uygulamaları yaygınlaşana kadar, Ek-5 de belirlenen standart ve kurallar çerçevesinde gerekli yedekleme ve güvenlik önlemleri alınarak yapılandırılan kurumlar sadece elektronik ortamda tutabilir, iş ve işlemler bu ortamda gerçekleştirilebilir."

"**(6.6.2007-5228 sayılı onayla eklenen)** Sağlık kurumlarımızda kullanılmakta olan tüm

bilgi sistemlerinde gerek veritabanından gerekse kullanılan uygulama yazılımları arayüzlerinden

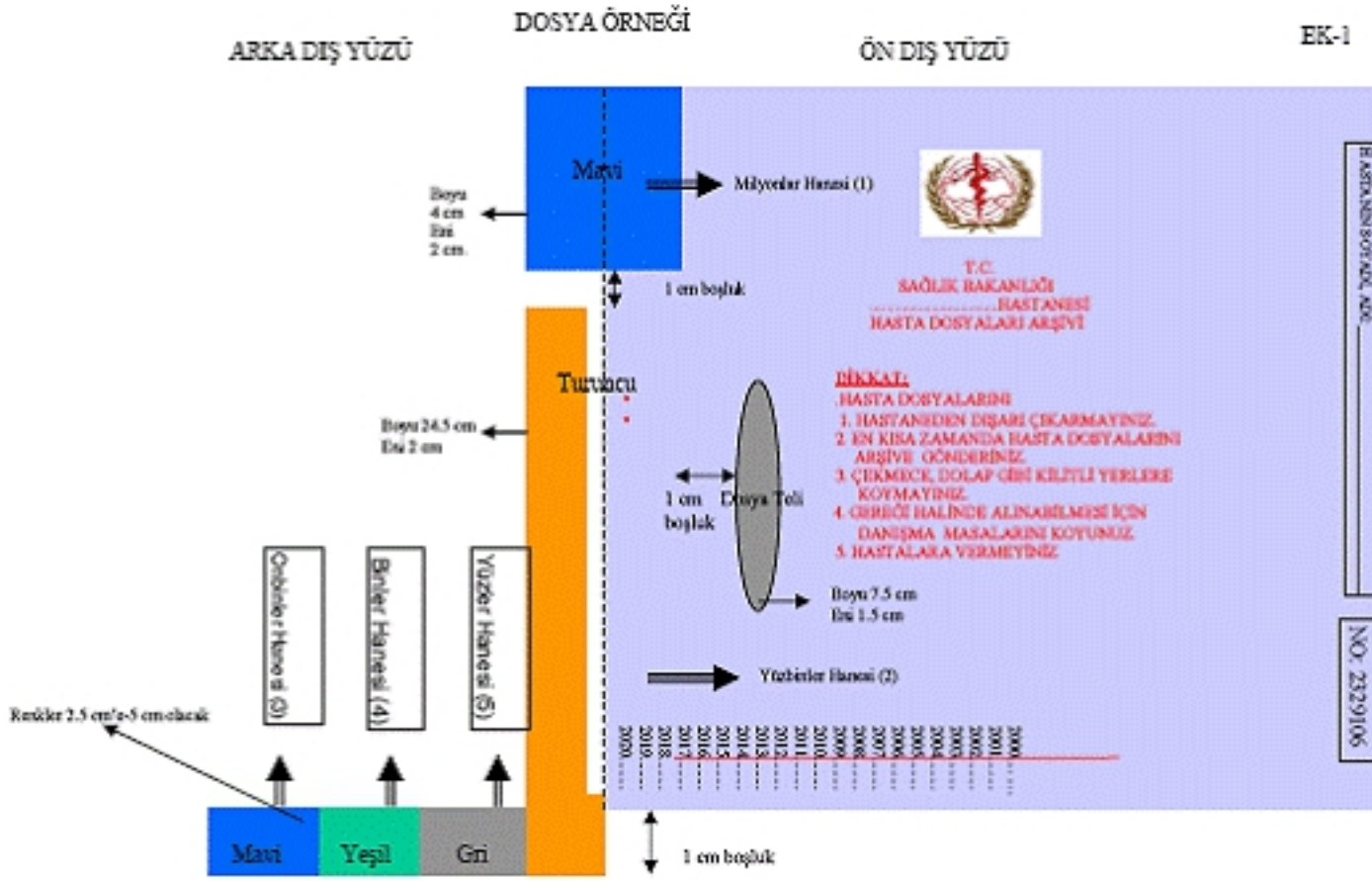
(Hastane Bilgi Sistemleri, Aile Hekimliği Bilgi sistemleri, Birinci Basamak Sağlık Kurumları Bilgi sistemleri vb.) geçmiş kayıtlardaki kapanmış, onaylanmış ve sonuçlandırılmış işlemlere ait verilerde değiştirme, silme ve ekleme yapılamaz. Son kullanıcılara sadece okuma ve raporlama yetkisi verilir."

"**(6.6.2007-5228 sayılı onayla eklenen)** Herhangi bir nedenden (teknik, programatik, mevzuat vb.) kaynaklanan zorunlu haller söz konusu olduğu takdirde bunun için gerekli değiştirme, silme ve ekleme yapma yetkisi, ilgili sağlık kurumunun en üst amirine aittir. Bu değişikliklere ait detaylı
loglar
mutlaka tutulmalıdır."

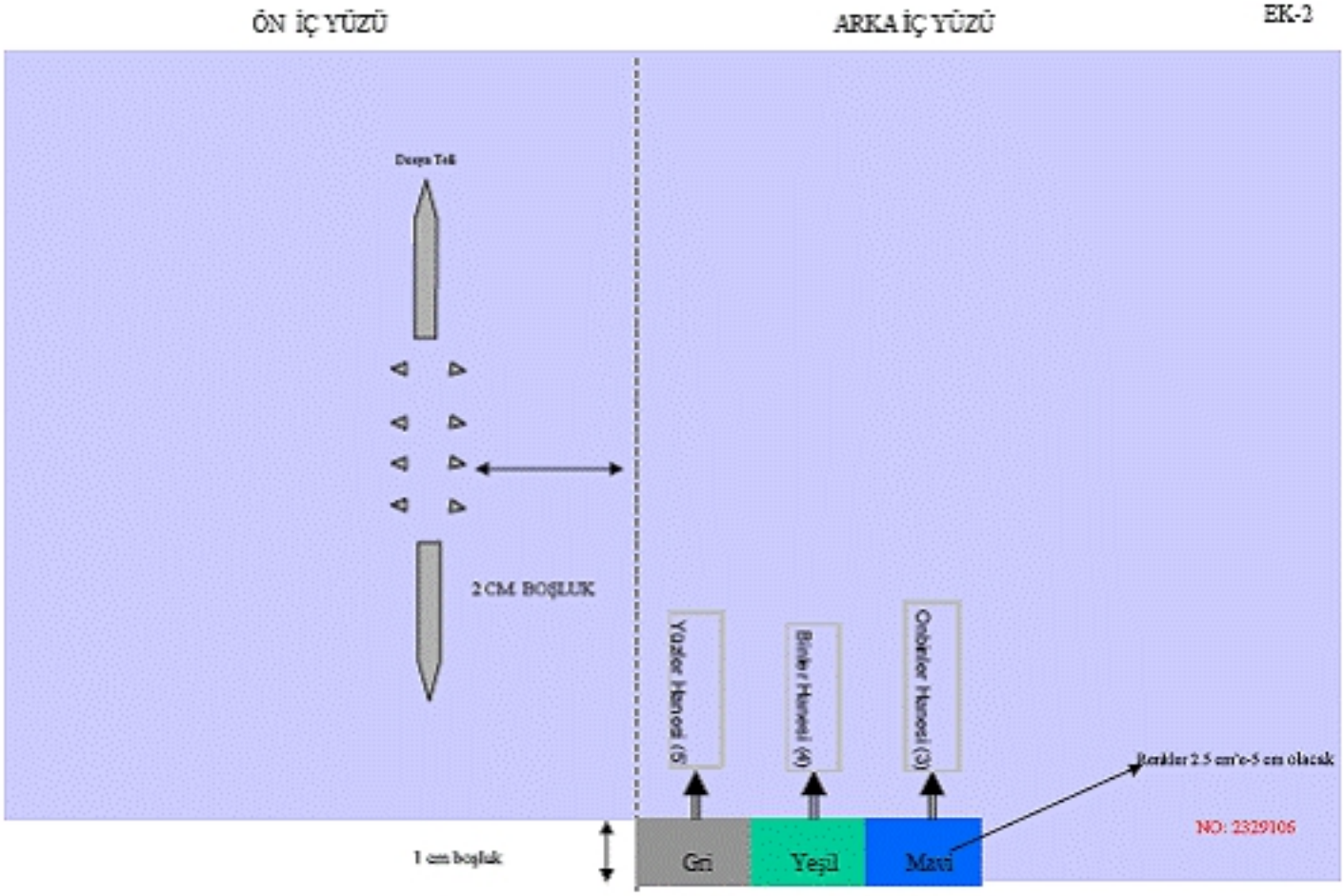
MADDE 2- Aynı Yönerge'ye ek'teki Ek-5 eklenmiştir.

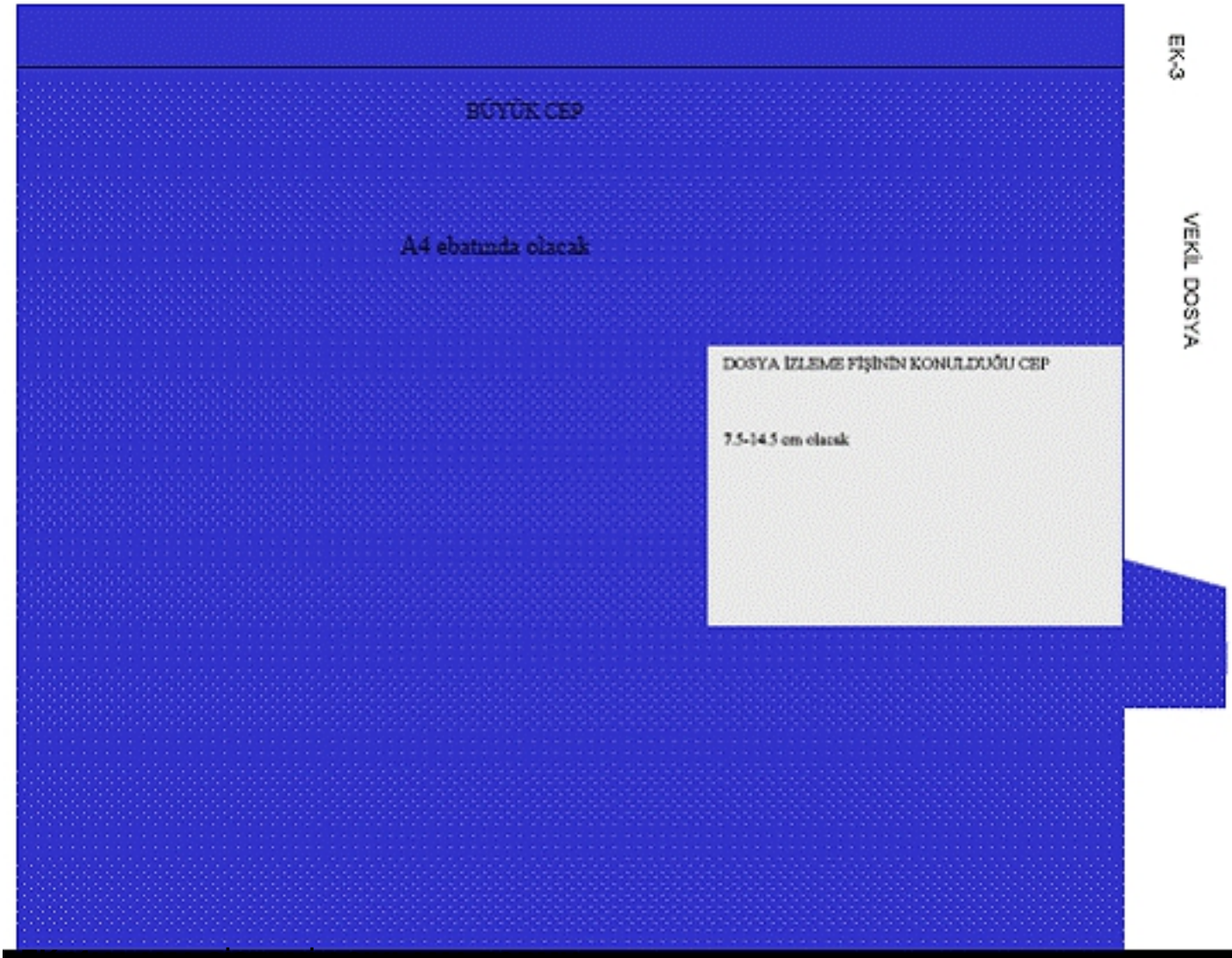
MADDE 3- Bu Yönerge Bakan onayını müteakiben yürürlüğe girer.

MADDE 4- Bu Yönerge hükümlerini Sağlık Bakanı yürütür.


DOSYA ÖRNEĞİ
EK-1
ARKA DIŞ YÜZÜ
ÖN DIŞ YÜZÜ
Mavi
Milyemler Hanesi (1)
Boyu 4 cm Eni 2 cm
1 cm boşluk
T.C.
SAĞLIK BAKANLIĞI
.....HASTANESİ
HASTA DOSYALARI ARŞİVİ
Turuncu
Boyu 24.5 cm Eni 2 cm
DİKKAT:
HASTA DOSYALARINI
1. HASTANEDEN DIŞARI ÇIKARMAYINIZ.
2. EN KISA ZAMANDA HASTA DOSYALARINI ARŞİVE GÖNDERİNİZ.
3. ÇEKMECE, DOLAP GİBİ KİLİTLİ YERLERE KOYMAYINIZ.
4. GEREĞİ HALİNDE ALINABİLMESİ İÇİN DANIŞMA MASALARINI KOYUNUZ.
5. HASTALARA VERMEYİNİZ.
1 cm boşluk
Dosya Teli
Boyu 7.5 cm Eni 1.5 cm
Onbirler Hanesi (3)
Birler Hanesi (4)
Yüzler Hanesi (5)
Yüzbinler Hanesi (2)
Renkler 2.5 cm'e-5 cm olacak
Mavi
Yeşil
Gri
1 cm boşluk
NO: 2329106

EK-2


ÖN İÇ YÜZÜ
ARKA İÇ YÜZÜ
Dosya Teli
2 CM. BOŞLUK
Yazılar Hanesi (5)
Birimler Hanesi (4)
Onlıklar Hanesi (3)
Renkler 2.5 cm'e-5 cm olacak
NO: 2329105
1 cm boşluk
Gri
Yeşil
Mavi



[illegible] dosya örneğine uygun olarak, Yazılık [illegible] dosya numarasının okunma şekli;

[illegible] uygulanmasına ait [illegible] dosya tel ve güvenlik bandı için paslanmaz çelik

FORM 1

DOSYA NO:	SOYADI:	ADI:	BABA ADI:	ANNE ADI:
.....	....	....	.....	.....
DOĞUM TARİHİ: ... /... /.....			BÖLÜM:.....	
ADRES:.....				
NOT: 1 - Her hastanın bir tane dosyası olmalıdır. 2 - Kimlik bilgilerini yazarken, bölgesel şivelere dikkat ediniz. 3 - Bütün bilgiler eksiksiz, hatasız daktilo ile büyük harf olarak yazılmalıdır. 4 - Çift isimleri parantez içine alınız. 5 - Bu kartı en kısa zamanda hasta endeksine gönderiniz.				

FORM 2

DOSYA NO	YAŞ	CİNS	SONUÇ	K.G.	C.T.	AÇIKLAMA	BAŞKA TANI VE AMELİYATLAR	DOKTORU

HASTALIK ENDEKSİ :

EK-5 (6.6.2007-5228 sayılı onayla eklenen)

5.1. KRİZ / ACİL DURUM YÖNETİMİ

Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınmalıdır. Örneğin, uygulama veya veri tabanı sunucularında donanım ve yazılıma ait problemler oluştuğunda, yerel veya uzak sistemden yeniden kesintisiz (veya makul kesinti süresi içerisinde) çalışma sağlanabilmelidir. Kümeleme (cluster) veya uzaktan kopyalama (remote replication) çözümleri hayata geçirilmelidir. Hastaneler, sistemlerini tasarlarken ne kadar süre ile ve ne kadar performans kaybını
tolere
edeceklerini göz önüne almalıdırlar. Kurum çalışanlarının, bilgi güvenliği ile ilgili acil bir durum oluştuğunda sorumlulukları
dahilinde
gerekli müdahaleyi yapabilmelerine yönelik standartlar şunlardır.

5.1.1. Acil durum sorumluları atanmalı ve yetki ve sorumlulukları belirlenmeli ve dokü mante
edilmelidir.

5.1.2. Acil durumlarda kurum içi işbirliği gereksinimleri tanımlanmalıdır.

5.1.3. Acil durumlarda sistem log'ları incelenmek üzere saklanmalıdır.

5.1.4. Güvenlik açıkları ve ihlallerinin rapor edilmesi için kurumsal bir mekanizma oluşturulmalıdır.

5.1.5. Yaşanan acil durumlar sonrası politikalar ve süreçler yeniden incelenerek ihtiyaçlar doğrultusunda revize edilmelidir.

5.1.6. Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulmalı ve bu bildirim süreçleri tanımlanmış olmalıdır.

5.1.7. Acil Durum kapsamında değerlendirilen olaylar aşağıda farklı seviyelerde tanımlanmıştır:

- **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.

5.1.8. Herbir seviyede tanımlı acil durumlarda karşılaşılabilecek riskler, bu riskin kuruma getireceği kayıplar ve bu riskler oluşmadan önce ve oluştuktan sonra hareket planları tanımlanmalı ve dokümante edilmelidir.

5.1.9. Acil durumlarda bilgi güvenliği yöneticisine erişilmeli, ulaşılamadığı durumlarda koordinasyonu sağlamak üzere önceden tanımlanmış ilgili yöneticiye bilgi verilmeli ve zararın tespit edilerek süratle daha önceden tanımlanmış felaket kurtarma faaliyetleri yürütülmelidir.

5.1.10. Bilgi güvenliği yöneticisi tarafından gerekli görülen durumlarda konu hukuksal zeminde incelenmek üzere ilgili makamlara iletilmelidir.

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

edilmiş olmalıdır.

5.2. 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 çalışmalıdır. Verinin de operasyonel ortamda online olarak aynı disk sisteminde farklı disk volümlerde ve offline olarak Manyetik kartuş, DVD veya CD ortamında yedekleri alınmalıdır. Taşınabilir ortamlar (Manyetik kartuş, DVD veya CD) fiziksel olarak bilgi işlem odalarından faklı odalarda veya binalarda güvenli bir şekilde saklanmalıdır. Veriler offline ortamlarda süresiz olarak saklanmalıdır. Buna yönelik standartlar şunlardır.

5.2.1. Kurumsal kritik verilerin saklandığı sistemler ile sistem kesintisinin kritik olduğu sistemlerin bir varlık envanteri çıkartılmalı ve yedekleme ihtiyacı bakımından sınıflandırılarak dokümante edilmelidir.

5.2.2. 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

edilmelidir.

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

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

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

5.2.6. Yedeklenecek bilgiler değişiklik gösterebileceğinden yedekleme listesi periyodik olarak gözden geçirilmeli ve güncellenmelidir.

5.2.7. Yeni sistem ve uygulamalar devreye alındığında, yedekleme listeleri güncellenmelidir.

5.2.8. Yedekleme işlemi için yeterli sayı ve kapasitede yedek üniteler seçilmeli ve temin edilmelidir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilmelidir.

5.2.9. Yedekleme ortamlarının mümkünse düzenli olarak test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmalıdır.

5.2.10. Geri yükleme prosedürlerinin düzenli olarak kontrol ve test edilerek etkinliklerinin doğrulanması ve operasyonel prosedürlerin öngördüğü süreler

dahilinde
tamamlanabileceğinden emin olunması gerekir.

5.2.11. Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanmalıdır.

5.2.12. 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.

5.2.13. 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.

5.3. VERİ TABANI GÜVENLİĞİ

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

5.3.1. Veritabanı sistemleri envanteri ve bu envanterden sorumlu personel tanımlanmalı ve dokümante edilmelidir.

5.3.2. Veritabanı işletim kuralları belirlenmeli ve dokümante edilmelidir.

5.3.3. Veritabanı sistem logları tutulmalı ve izlenmelidir.

5.3.4. Veritabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli alınması kontrol altında tutulmalıdır.

5.3.5. Yedekleme planları dokümante edilmelidir.

5.3.6. Veritabanı erişim politikaları "Kimlik doğrulama ve Yetkilendirme" politikaları çerçevesinde oluşturulmalıdır.

5.3.7. Hatadan arındırma, bilgileri yedekten dönme kuralları "Acil Durum Yönetimi" politikalarına uygun olarak oluşturulmalı ve dokümante edilmelidir.

5.3.8. Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.

5.3.9. Veritabanı sistemlerinde oluşacak problemlere yönelik bakım, onarım çalışmaları yetkili bir personel gözetiminde yapılmalıdır.

5.3.10. Yama ve güncelleme çalışmaları yapılmadan önce bildirimde bulunulmalı ve sonrasında ilgili uygulama kontrolleri gerçekleştirilmelidir.

5.3.11. Bilgi saklama ortamlarının kurum dışına çıkarılması için yetkilendirme yapılması ve bu durumun izleme takip amacıyla kaydedilmesi gerekir.

5.3.12. Sistem dokümantasyonu güvenli şekilde saklanmalıdır.

5.3.13. İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için kurulacak temaslar belirlenmelidir.

5.3.14. Veritabanı serverda sadece ssh açık olmalı ftp, telnet, remote vb. bağlantılara kapalı olmalıdır.

5.3.15. Veritabanı servera veritabanı yöneticisi dışında hiçbir kullanıcı ssh bağlantı yapma yetkisi olmamalıdır.

5.3.16. Application serverlardan veritabanına rlogin vb. şekilde erişememelidir.

5.3.17. 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.

5.3.18. Arayüzden gelen kullanıcılar bir tabloda saklanmalı bu tablodaki kullanıcı adı ve şifreleri şifrelenmiş olmadır.

5.3.19. Veritabanında güvenliği önemli veriler mutlaka şifrelenmelidir. Bu sayede verileri taşınsa bile orjinallerine erişilmemesi sağlanır.

5.3.20. 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.

5.3.21. Veritabanında Veritabanı yöneticisi dışında SYSDBA,DBA yetkili kullanıcı olmamalıdır.

5.3.22. Veritabanında bulunan farklı Schemaların kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenmelidir.

5.3.23. Veritabanına internetten direkt bağlantı kesinlikle engellenmelidir.

5.3.24. Veritabanı server a Sistem yöneticisi, Veritabanı Yöneticisi ve application server dışında hiçbir kullanıcı erişememelidir, ip bazında kısıtlana yapılmalıdır.

5.3.25. Veritabanı servera kod geliştiren kullanıcı dışında hiçbir kullanıcı bağlanıp sorgu yapamamalıdır. İstekler arayüzden sağlanmalıdır.(Kullanıcılara tablolardan select yapamamalılar)

5.3.26. Veritabanına giden veri trafiği şifrelenmelidir. (Networku dinleyen verilere ulaşamamalıdır.)

5.3.27. Bütün şifreler düzenli aralıklarla değiştirilmelidir. Detaylı bilgi için şifreleme politikasına bakılmalıdır.

5.4. 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.

5.4.1. Genel Bilgiler

5.4.1.1. Bütün sistem seviyeli şifreler (örnek, root, administrator, enable, vs) en az üç ayda bir değiştirilmelidir.

5.4.1.2. 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.

5.4.1.3. Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.

5.4.1.4. Şifreler e-posta iletilerine veya herhangi bir elektronik forma eklenmemelidir.

5.4.1.5. SNMP kullanıldığı durumlarda varsayılan olarak gelen "public", "system
" ve "
private
"

gibi

community

string'lere

farklı

değerler atanmalıdır.

5.4.1.6. Kullanıcı, şifresini başkası ile paylaşmaması, kağıtlara yada elektronik ortamlara yazmaması konusunda eğitilmelidir.

5.4.1.7. 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.

5.4.2. □□□□□□□ 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.

 Zayıf şifreler aşağıda belirtilen karakteristiklere sahiptir.

· Şifreler sekizden daha az karaktere sahiptirler.

· Şifreler sözlükte bulunan bir kelimeye sahiptir.

· Şifreler aşağıdaki gibi ortak değere sahiptir.

o Ailesinin, arkadaşının, sahip olduğu bir hayvanın veya bir sanatçının ismine sahiptir.

o Bilgisayar terminolojisi ve isimleri, komutlar, siteler, şirketler, donanım veya yazılım gibi.

o "Sağlık", "istanbul", "ankara" gibi isimler.

o Doğum tarihi veya adres ve telefon numaraları gibi kişisel bilgiler.

o Aaabbb, qwerty,zyxwuts, 123321 vs. Gibi sıralı harf veya rakamlar.

o Yukardaki herhangi bir kelimenin geri yazılış şekli.

o Yukarıdaki herhangi bir kelimenin rakamla takip edilmesi (örnek ,gizli1, gizli2).

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, !@#$%^&*()_+|~-=`{}[]:";'<> ?,./)

- 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.

5.4.3. □□□□□□□Şifre Koruma Standartları

Sağlık Bakanlığı bünyesinde kullanılan şifreleri kurum 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.

Bakanlık bünyesinde kullanılan şifreleri herhangi bir kimseyle paylaşmayınız. Bütün şifreler

Bakanlığa ait gizli bilgiler olarak düşünülmelidir.

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 paylaşmak.
- Şifreleri işten uzakta olduğunuz zamanlarda iş arkadaşlarınıza bildirmek.

Herhangi bir kimse şifre isteğinde bulunursa bu dökümanı 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.

5.4.4. □□□□□□□ Uygulama Geliştirme Standartları

5.4.4.1. Uygulama geliştiricileri programlarında aşağıdaki güvenlik özelliklerinin sağla ndığından
emin olmalıdırlar.

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

5.4.4.3. Şifreleri text olarak veya kolay anlaşılabilir formda saklamamalıdır.

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

5.4.4.5. Mümkün olduğu kadar TACACS+ , RADIUS ve/veya X.509/LDAP güvenlik

protokollerini desteklemelidir.

5.4.5. Uzaktan Erişen Kullanıcılar için Şifre Kullanımı

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

5.4.6. 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"

Şifreleme için geçerli olan bütün kurallar passphrase'ler için de geçerlidir.

5.5. SUNUCU GÜVENLİĞİ

Sunucuların güvenliğinin sağlanması için uyulması gereken kurallar ve standartlar şunlardır.

5.5.1 Genel Bilgiler

5.5.1.1 Sahip Olma ve Sorumluluklar

Kurum bünyesindeki bütün dahili sunucuların yönetiminden sistem yöneticileri sorumludur.

Sunucu konfigurasyonları sadece bu grup tarafından yapılacaktır.

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

- Sunucuların yeri ve sorumlu kişi.

- Donanım ve İşletim Sistemi.

- Ana görevi ve üzerinde çalışan uygulamalar.

- İşletim Sistemi versiyonları ve yamalar.

5.1.1.2. Bütün bilgiler tek bir merkezde güncel olarak tutulmalıdır.

Genel Konfigurasyon Kuralları

5.1.2.1. İşletim sistemi konfigurasyonları Bilgi İşlem Biriminin talimatlarına göre yapılacaktır.

5.1.2.2. Kullanılmayan servisler ve uygulamalar kapatılacaktır.

5.1.2.3. Eğer mümkünse servislere erişimler için log tutulacak (örnek; TCP Wrapper) ve erişim kontrol metotlarıyle koruma sağlanacaktır.

5.1.2.4. 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.

5.1.2.5. Uygulama erişimleri için standart güvenlik prensiplerini çalıştırın, gereksiz servisleri açmayın.

5.1.2.6. Sistem yöneticileri gerekli olmadığı durumlar dışında "Administrator" 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.

5.1.2.7. Ayrıcalıklı bağlantılar teknik olarak mümkünse güvenli kanal (SSH veya IPSe
c
VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.

5.1.2.8. Sunucular fiziksel olarak erişim kontrollü sistem odalarında bulunmalıdırlar.

5.5.2. Gözlemleme

5.5.2.1. Kritik sistemlerde oluşan bütün güvenlikle ilgili olaylar loglanmalıdır ve aşağıdaki şekilde saklanmalıdır:

o 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.

5.5.2.2. 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.

5.5.3. Uygunluk

5.5.3.1. Denetimler yetkili organizasyonlar tarafından Bakanlık bünyesinde belli aralıklarda yapılacaktır.

5.5.3.2. Denetimler Bilgi İşlem grubu tarafından yönetilecektir.

5.5.3.3. Denetimler organizasyonun işleyişine zarar vermemesi için maksimum gayret gösterilecektir.

5.5.4.□□□□□ İşletim

5.5.4.1. Sunucular elektrik ve ağ altyapısı ile sıcaklık ve nem değerleri düzenlenmiş ortamlarda işletilmelidir.

5.5.4.2. Sunucuların yazılım ve donanım bakımları üretici tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılmalıdır.

5.5.4.3. Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çık ışlar

erişim
kontrollü olmalı ve kayıt edilmelidir.

5.6. KİMLİK DOĞRULAMA VE YETKİLENDİRME

□

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

□

5.6.1. Kurum sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere, hangi kimlik doğrulama yöntemi ile erişeceği belirlenecek ve dokümante edilecektir.

5.6.2. Kurum sistemlerine erişmesi gereken kurum dışı ve extranet kullanıcılarına yönelik ilgili profiller ve kimlik doğrulama yöntemleri tanımlanacak ve dokümante edilecektir.

5.6.3. 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.

5.6.4. 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.

5.6.5. Erişim ve yetki seviyelerinin sürekli güncelliği temin edilmelidir.

5.6.6. Kullanıcılar kurum adına kullanımları için tahsis edilmiş sistemlerin güvenliğinden sorumludurlar.

5.6.7. Sistemlere başarılı ve başarısız erişim logları düzenli olarak tutulmalı,

tekrarlanan başarısız log-on girişimleri incelenmelidir.

5.6.8. Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.

5.6.9. Sistemlere log-on olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve yetki ihlalleri kontrol edilmelidir.

5.6.10. Kullanıcılara erişim haklarını yazılı olarak beyan edilmeli ve erişim haklarını ihlal eden kullanıcılar için ilgili politika maddesi uygulanmalıdır.

5.6.11. Kullanıcı hareketlerini izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.

5.6.12. 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.

5.7. 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; Bakanlığımıza bağlı bütün kurum ve kuruluşlarda (merkez ve taşra teşkilatları, hastaneler, sağlık ocakları, aile hekimleri vs.) hasta sağlık bilgisinin mahremiyeti hususunda uyulması gereken temel kurallar şunlardır.

5.7.1. Genel Kurallar

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

5.7.1.1. Veri güvenliği konusunda üç temel prensibin göz önüne alınması gerekmektedir. Bunlar; gizlik, bütünlük ve erişilebilirliktir.

5.7.1.2. Kurumda kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi tanımlanmalıdır. Rol bazlı yetkilendirme yapılmalıdır ve yetkisiz kişilerin hastanın sağlık kayıtlarına erişmesi mümkün olmamalıdır.

5.7.1.3. 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.

5.7.1.4. Hasta taburcu olmuş ise hiçbir kurum çalışanı hastanın sağlık kayıtlarına erişemez.

5.7.1.5. Hastanın rızası olmadan hiçbir çalışan sözle de olsa hasta sağlık bilgilerini hastanın yakınları dışında üçüncü şahıslara ve kurumlara iletemez.

5.7.1.6. Hasta sağlık bilgileri ticari amaçlı olarak da üçüncü şahıslara iletilemez. Hastanın kullandığı ilaçlar, diyet programları vs. buna dahildir.

5.7.1.7. 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.

5.7.1.8. Hastanın dosyasının izlenmemesi için gerekli tedbirler alınmalıdır. [Hasta dosyalarının gelişigüzel ortada bırakılmaması, bilgisayar ekranının başkalarınca okunabilecek şekilde bırakılmaması gibi]

5.7.1.9. Telefon ile konuşurken hasta ile ilgili mahrem bilgilerin üçüncü şahısların eline geçmemesine azami özen göstermelidir.

5.7.1.10. Bütün hasta sağlık sağlık kayıtları fiziksel olarak korunmuş mekanlarda saklanmalıdır.

5.7.1.11. Elektronik hasta kayıtlarına internet ortamından erişim mümkün olmamalıdır.

5.7.1.12. 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.

5.7.2. □□□□ Sistem Güvenliği

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

5.7.2.2. 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.

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

Veriye erişecek kişiler aşağıdaki şekilde tanımlanmıştır:

- Hasta kendi verisine online olarak hiçbir zaman erişmemelidir.

- Bir Aile hekimi ancak kendisine kayıtlı olan hastaların elektronik sağlık kayıtlarına erişebilmelidir.

- 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.

5.7.2.4. Sistem yöneticilerine de bir güvenlik katmanı konulacaktır. Bunun için veritabanı yazılımının gelişmiş güvenlik yönetimi özellikleri kullanılacaktır.

5.7.2.5. Gerektiğinde saat ve/veya gün bazında belirlenen bir sure için bazı kullanıcı ve istemci makinelerin sisteme oturum açmalarına kısıtlama getirilebilmelidir.

5.7.2.6. Aynı kullanıcı kodu ile aynı anda birden fazla oturum açılmasına izin verilmemelidir.

5.7.2.7. 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.

5.7.2.8. 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.

5.7.2.9. 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.

5.7.2.10. 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.

5.7.2.11. 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.

5.7.2.12. Sistem yöneticilerinin kimlik tanımlama ve doğrulaması için X.509v3 uyumlu sayısal sertifikalar kullanılmalıdır. Sayısal sertifikaların güvenli depolaması için akıllı kartlar veya usb token cihazları kullanılmalıdır.

5.7.2.13. Sertifika tabanlı kimlik doğrulama yapılmadığı halde password ve hash tabanlı kimlik doğrulama yapılacaktır. Sistemlere erişim için tek yönlü şifreleme algoritmaları kullanılacaktır.

Kurum içerisinde veya Kurum ile başka ağlar arasındaki tüm haberleşme şifreli yapılmalıdır. Bütün iletişim VPN ve Açık Anahtar Alt Yapısı (PKI) teknolojilerini kullanmalıdır.