**1.AMAÇ:**

Bu güvenlik politikası, etkin ve yerleşmiş bilgi teknolojileri güvenlik süreçleri ve prosedürleri aracılığıyla sağlık hizmetlerinden faydalanan vatandaşa ait bilgilerin ya da kurumsal hizmetlerin icra edilmesi esnasında edinilen bilgi ve kaynakların güvenliğini, bütünlüğünü ve kullanılabilirliğini sağlamayı amaçlamaktadır.

**2.KAPSAM:**

Kurumumuz, hizmet verdiği vatandaşların kayıt altına aldığı her türlü bilgisini, kendisine emanet edilmiş bir değer olduğu vizyonuyla korumakla mükellef olduğunun bilinciyle hareket etmektedir. Bu suretle gerçekleştirilen faaliyetlerin ifasını verilen hizmetlerin etkin, güvenilir ve kesintisiz bir şekilde yürütülmesi; edinilen bilgilerin bütünlüğünün, tutarlılığının, güvenilirliğinin sağlanması için uygun bilgi sistemleri ortamının tesis edilmesi, bu bilgi sistemlerinin kullanılmasından kaynaklanacak risklerin kontrol edilmesi ve tüm bu hususlarda gerekli tedbirlerin alınması usul ve esasları üzerine kurmuştur.

**3.HEDEFLER:**

3.1. Bilgi güvenliği standartlarının gerekliliklerini yerine getirmek,
3.2. Bilgi güvenliği ile ilgili tüm yasal mevzuata uyum sağlamak,
3.3. Bilgi varlıklarına yönelik riskleri tespit etmek ve sistematik bir şekilde riskleri yönetmek,
3.4. BGYS'yi sürekli gözden geçirmek ve iyileştirmek,
3.5. Bilgi güvenliği farkındalığını artırmak için teknik ve davranışsal yetkinlikleri geliştirecek şekilde eğitimler gerçekleştirmek.

**4.YÖNETİMSEL SÜREÇLER:**

4.1. Üst Yönetim Bilgi Güvenliği Taahhüdü
BGYS'nin tüm süreçleri için gerekli yönetimsel destek ve kaynaklar sağlanır.

4.2. Bilgi Güvenliği Faaliyetlerinin Nasıl Yürütüleceği
Kurum bilgi güvenliği faaliyetlerinin etkin olarak yürütülmesi maksadıyla yaygın olarak kabul gören bilgi güvenliği standartları, ilgili yasa, mevzuat ve yönetmeliklerin gerektirdiği şartlara yönetim tarafından uyulacak, ilgili taraflarca uyulması sağlanacaktır. İç bağlamda belirtilen unsurlar, ilgili standart, mevzuat ve yönetmeliklerin getirdiği sorumluluklara uymakla yükümlüdür.

4.3. Kurum Bilgi Güvenliği Organizasyonunun Oluşturulması
Bilgi yönetimine ilişkin faaliyetlerin yürütülmesi ve koordinasyonuna yönelik sorumlular belirlenerek görevlendirmeleri yapılmış ve sorumlulukları tanımlıdır.

4.3.1.Başhekim Yardımcısı:
Bilgi yönetimine ilişkin süreçlerin güvenli bir şekilde yürütülmesi ve koordinasyonuyla ilgili tüm konulardan sorumludur. Genel işleyişle ilgili sorunların tespiti ve çözüme ulaştırılması, yeni uygulamaların yürürlüğe konması vb. konularda ilgili kişileri organize ederek süreci takip eder. Sonuçları Başhekime raporlar.

4.3.2.Müdür Yardımcısı:
Genel işleyişle ilgili sorunların tespiti ve çözüme ulaştırılması, yeni uygulamaların yürürlüğe konması vb. konularda Bilgi işlem Birim Sorumlusu ile koordineli çalışarak sürecin takibini yapar.

4.3.3.Bilgi İşlem Birim Sorumlusu:
Bilgi yönetimine ilişkin tüm süreçlerin takibi, geliştirilmesi ,karşılaşılan donanımsal ve yazılımsal problemlerin çözülmesi , yeni uygulamaların hayata geçirilmesi vb. konularda firma personelini koordine ederek çalışır. Süreçle ilgili Müdür Yardımcısına bilgi verir.

4.3.4.Firma Sorumlu Personeli:
Bilgi yönetim sistemi ile ilgili yazılımsal ve donanımsal olarak karşılaşılan sorunların , gerektiğinde yazılım firması merkeziyle irtibata geçerek çözülmesini sağlar. Süreçlerle ilgili Bilgi işlem Birim Sorumlusu ile koordineli olarak çalışır.

4.4. Bilgi Güvenliği Eğitim Programlarının Yapılması
Kurum genelinde tüm personeli kapsayacak şekilde, sürekli güvenlik bilincinin, kurumsal güvenlik kültürünün oluşturulmasına ve korunmasına yardımcı olacak bilgi güvenliği eğitimi yıllık eğitim programında yer almaktadır.

**5.ELEKTRONİK POSTA GÜVENLİĞİ:**

Kurumumuzda görev yapan personel tarafından görevleri gereği yürütülen kurumsal iş ve işlemlerde, *@saglik.gov.tr uzantılı kurumsal veya tüzel e-Posta hesabı kullanılır. Kurumsal iş ve işlemler, kişilerin özel işleri için (Gmail, Hotmail gibi) internet hizmet sağlayıcılarından alınan hesaplar üzerinden yürütülmez.

**6.SOSYAL MÜHENDİSLİK VE SOSYAL MEDYA GÜVENLİĞİ:**

6.1.Sosyal mühendislik, normalde insanların tanımadıkları birisi için yapmayacakları şeyleri yapmalarını sağlama sanatı olarak tanımlanır. Başka bir tanım ise insanoğlunun zaaflarını kullanarak istenilen bilgiyi, veriyi elde etme sanatıdır.

6.2.Sosyal mühendislik yapan kötü niyetli kişiler, sosyal medya ve analiz yöntemlerini kullanarak hedef kişiler hakkında bilgi toplarlar. Sonrasında sosyal mühendislik tekniklerini kullanarak insanların zaaflarından faydalanıp istedikleri bilgilere ulaşmak için çalışma yaparlar.

**6.3.Sosyal mühendislik saldırılarından korunmak için kişisel olarak dikkat edilmesi gereken hususlar şu şekildedir:**

6.3.1. Taşıdığınız ve işlediğiniz verilerin öneminin bilincinde olunuz.
6.3.2. Bilgilerin kötü niyetli kişilerin eline geçmesi halinde oluşacak zararları düşünerek hareket ediniz.
6.3.3. Arkadaşlarınızla, çevrenizle paylaştığınız kayıtları seçerken dikkat ediniz.
6.3.4. Özellikle telefonda, e-Posta veya sohbet yoluyla yapılan haberleşmelerde parola gibi özel bilgilerinizi kesinlikle paylaşmayınız.
6.3.5. Parola kişiye özel bilgidir. Sistem yöneticiniz dâhil telefonda veya e-Posta ile parolanızı hiç kimseyle kesinlikle paylaşmayınız.
6.3.6. Oluşturulan dosyaya erişecek kişiler ve haklarını, "bilmesi gereken" prensibine göre belirleyiniz ve erişim kontrol tedbirleri uygulayınız.
6.3.7. Verdiğiniz erişim haklarını belirli dönemlerde kontrol ediniz.
6.3.8. Çöpe atılan kâğıtlara dikkat ediniz. Kişisel veri içeren ya da kuruma ait bilgilerin yer aldığı kâğıtları, kâğıt kırpma makinesinde imha ediniz.
6.3.9. Çok acele bilgi istendiği zaman istenen bilginin niteliğine göre teyit mekanizması kullanınız.
6.3.10. Bilgisayarınızı yabancı bir kişiye kullandırmayınız. Bu kişiler tarafından bilgisayarınıza takılacak olan USB depolama aygıtları ya da harici disklerden bilgisayarınıza zararlı yazılım bulaştırabilir.
6.3.11. Hediye olarak verilen USB depolama aygıtlarını kullanmadan önce mutlaka virüs taramasından geçiriniz.
6.3.12. Kişisel sağlık kayıtlarının (tüm tetkik sonuçları, hasta dosyaları, barkodlar, gözlem formları vb.) özel nitelikli kişisel veri kategorisinde olduğu ve 6698 sayılı kanun ile özel koruma uygulanması gerektiği her zaman dikkate alınmalıdır.
6.3.13. Telefon ile hasta hakkında bilgi almak isteyen kişilere, hastanın kişisel bilgileri ile ilgili açıklama yapılmamalıdır.
6.3.14 Hasta dosyaları, hastanın tedavi sürecine dâhil olan sağlık profesyonelleri/ çalışanları dışında kimseyle paylaşılmaz. Kolay ulaşılır yerlere konulmaz.
6.3.15. Sağlık Bilgi Yönetim Sistemi (SBYS) programlarında kullanılan parolalar kimseyle paylaşılmaz.

**6.4. Kişisel Sosyal Medya Güvenliği:**

6.4.1. Sosyal medya hesaplarına giriş için kullanılan parolalar ile kurum içinde kullanılan parolalar farklı seçilir.
6.4.2. Kurum içi bilgiler sosyal medya ortamlarında paylaşılmaz.
6.4.3. Kuruma ait gizli bilgiler, resmi yazılar, çeşitli gelişmeler sosyal medya ortamında yayımlanamaz.
6.4.4. Eğitimlerde sosyal medya güvenliği ile ilgili hususlara yer verilir.

**7.ERİŞİM KONTROL POLİTİKASI:**

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.

**8.BİLGİ SINIFLANDIRMA/GİZLİLİK DERECELERİNİN VERİLMESİ:**

8.1. Kurum bilgi varlıkları, içerdikleri verilerin hassasiyeti, kurum için taşıdıkları önem ve yasal zorunluluklar dikkate alınarak uygun bir şekilde sınıflandırılır/gizlilik derecesi verilir.
8.2. 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;
8.3. 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",

8.4. 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",

8.5. 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",

8.6. 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.

8.7. 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.

8.8. 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.

8.9. 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.

8.10. 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.

**9.FİZİKSEL VE ÇEVRESEL GÜVENLİK:**

9.1.Güvenli Alanlar:

9.1.1. 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.

9.1.2. 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.

9.1.3. Güvenlik sınırları belirlenirken kişilerin kontrolsüz olarak giriş çıkış yapabilecekleri herhangi bir boşluk bulunmamasına dikkat edilir. Bu tür boşlukların kapatılması/korunması için ilave tedbirler alınır.

9.1.4. Güvenli alanlar sadece yetkili personele erişim izni verilmesini temin etmek için uygun giriş kontrolleri ile korunur.

9.1.5. Göreceli olarak daha az hassas varlıkların yer aldığı dış güvenlik sınırında alınan güvenlik tedbirleri ile kritik varlıkların yer aldığı iç güvenlik sınırlarındaki tedbirler farklılaştırılır.

9.1.6. 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.

9.1.7. Giriş/çıkış yapılan yerler ve ortak kullanım alanları güvenlik kameraları ile kayıt altına alınır.

9.2.Ekipman Güvenliği:

9.2.1. 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.

9.2.2. Yetkisiz kişilerin erişiminin engellenmesi için bilgisayar başından ayrılma durumunda ekran kilitlemesi yapılır. Otomatik ekran kilitlemesi devreye alınır.

9.2.3. Sistemlerde kullanılan parola, telefon numarası ve T.C. kimlik numarası gibi bilgiler ekran üstlerinde veya masa üstünde bulundurulmaz.

9.2.4. Kullanım ömrü sona eren, artık ihtiyaç duyulmadığına karar verilen bilgiler imha edilir.

9.2.5. Faks makinelerine gelen yazılar sürekli kontrol edilir ve makinede yazı bırakılmaması için tedbir alınır.

9.2.6. 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.

9.2.7. Fotokopi ve diğer çoğaltma teknolojilerinin (tarayıcı, sayısal kamera vb.) yetkisiz kullanımını önlemek için uygun idari ve teknik tedbirler alınır.

**10.VARLIK YÖNETİMİ:**

BGYS kapsamında varlık envanterine esas olan varlık kategorileri aşağıdaki gibidir.

10.1. İş Süreçleri: Kurumsal bilgi varlıklarının kullanıldığı, çeşitli vasıtalarla hassas bilgilerin yoğun olarak işlendiği iş süreçleri (hasta kabul, heyet işlemleri, tıbbi kayıt arşiv vb.).

10.2. Kurumsal Bilgi Varlıkları: Elektronik veya kâğıt ortamda tutulan hasta kayıtları, personel kayıt ve dosyaları, kurumsal evraklar, bilgisayarlarda saklanan ve kurum için değeri olan veriler, raporlar, listeler, çizimler, veri tabanları, veri tabanı yedekleri, faturalar, sözleşmeler, teklifler, telifler, lisanslar vb.

10.3. Yazılımlar: İşletim sistemleri, ofis uygulamaları, HBYS yazılımları, laboratuvar yazılımları, tıbbi görüntüleme yazılımları, kurumsal yazılımlar vb.

10.4. Fiziksel varlıklar: Sunucular, masaüstü bilgisayarlar, taşınabilir bilgisayarlar, depolama birimleri, yedekleme birimleri (kasetler, hard diskler vb.), aktif cihazlar (anahtarlama cihazı, güvenlik duvarı, yönlendirici, ağ erişim cihazı, anahtar, modem, erişim noktası vb), fakslar, fotokopiler, yazıcılar, santraller, telefonlar, evrak imha cihazları, ağa bağlı olarak çalışan veya ağa bağlanma arayüzleri olan tıbbi cihazlar vb.

10.5. İnsan Kaynakları: Çalışanlar

10.6. Altyapı: Yapısal ve elektrik kablolama altyapısı, UPS, jeneratör, iklimlendirme, giriş/çıkış kontrol sistemleri, kamera sistemleri, yangın, duman uyarı sistemleri, yangın söndürme sistemleri, destek teçhizatı vb.

10.7. Mekânlar: Yönetim ve hizmet odaları, sunucu odaları, arşiv odaları, tıbbi kayıt saklama odaları vb.

Bilgi güvenliği yetkilisince, görevlendirilen ekip ile birlikte kurumun iş süreçleri analiz edilir. Başta taşınır mal sorumluları olmak üzere, teşkilatta yer alan diğer birimlerin birim sorumluları ile birlikte çalışılmak suretiyle, bilgi varlıklarının envanteri belirlenir.

Envanter belirleme işlemi bir kez yapılan ve tamamlanan bir iş değildir. Hazırlanan envanterin yazılı hale getirilmesi, farklı kaynaklardan (Çekirdek Kaynak Yönetim Sistemi/ÇKYS, Malzeme Kaynak Yönetim Sistemi/SBYS vb.) doğruluğunun kontrol edilmesi ve sürekli olarak güncel tutulması gerekir. Envanter tespit süreci, bir döngü şeklinde, periyodik olarak yapılması gereken bir faaliyettir.

**11.HABERLEŞME GÜVENLİĞİ:**

11.1. 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.

11.2. Kablolama Güvenliği:

11.2.1. Güç ve iletişim kabloları (ağ kabloları, güç kaynağı kabloları, telefon kabloları, vb.)

11.2.2. binalar arası geçişte yeraltında, bina içlerinde kablo kanalları veya tavalar içerisinden geçirilir.

11.2.3. Karışmanın (interference) olmaması için güç ve iletişim kabloları fiziksel olarak ayrılır.

11.2.4. Hatalı bağlantıların olmaması için ekipman, kablolar ve prizler görülebilecek bir şekilde etiketlenir ya da işaretlenir.

11.2.5. Dağıtım panelleri ve kenar anahtarların konulduğu kabinler yetkisiz erişime karşı kilitli olarak bulundurulur.

11.2.6. Bahse konu kabinlerin de kesintisiz güç kaynağı ve jeneratör altyapısından faydalanması sağlanır.

**12.YEDEKLEME POLİTİKASI:**

12.1. Verilerin yedeklenmesi iş sürekliliğinin en temel prensipleri arasında yer alır. Donanım arızaları, yazılım hataları, kullanıcıdan kaynaklanan sorunlar ya da doğal tehditler gibi nedenlerle veri kayıpları yaşanabilir. Başarılı bir yedekleme işlemi ve yedeklenen verinin ihtiyaç anında veri kaybı olmadan kurtarılabilmesi veri yedekleme sistemlerinin en temel iki bileşenidir.

12.2. Yedekleme, günde 4 defa yapılır( yedekleme işlemi için sistemin yoğun olmadığı zamanlar seçilir)

12.3. Yedekleme dosyaları HBYS'nin çalıştığı sunucu haricindeki bir ortama alınır.

12.4. Yedekleme; harici bellek, taşınabilir kayıt ortamları veya ağ üzerinde çalışan yedek sunucu gibi bir ortamda saklanır.

12.5. Alınan yedekleme ortamı, fiziksel olarak HBYS'nin üzerinde çalıştığı alanlardan farklı bir alanda/ farklı binada saklanır.

12.6. Veriler offline ortamlarda süresiz olarak hastane yönetimi tarafından saklanır.

12.7. Yedeklemeler aracılığı ile yılda bir kez veri kurtarma testi uygulanır.

12.8. Yedeklemeden geri dönüşüm sağlanıp sağlanmadığı ve veri kaybının olup olmadığı kontrol edilir.

**13.KÖTÜCÜL YAZILIMLARDAN KORUMA:**

13.1. Sunuculara yapılan erişimlerin raporlanması, mesai saati dışındaki erişimlerin işaretlenmesi gibi detaylar gözlenir. Kullanıcılara olması gerekenden fazla yetki tanımlanmaz.
13.2. BIOS 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.
13.3. Sunucu işletim sistemleri, güvenlik açıklarına karşı güncel tutulur.
13.4. Virüs vb. zararlı yazılımlardan korunmak ve kurumsal bilgilerin kurum dışına sızmasını engellemek amacıyla gerekiyorsa USB bellek gibi taşınabilir cihazların kullanımı engellenir.
13.5. Geliştirme ve test ortamları esas çalışma ortamından ayrılır. Yapılması planlanan işlemler öncelikle test ortamında denenir.
13.6. Sunucularda yapılan işlemlerin iz kayıtlarına erişmek için olay günlükleri (event logs) tutulur.
13.7. Tüm bilgisayarlar lisanslı anti-virüs yazılımı ile korunur. Anti-virüs yazılımının virüs veritabanı güncel tutulur.
13.8. Sunucu ve sistem güvenliğini sağlayabilmek için lisanslı yazılımlar kullanılır.
13.9. İç erişim güvenliği için her bilgisayarda masaüstü erişim şifreleri ve HBYS kullanıcı kodu ve şifreleri kullanılır.

**14.KRİPTOGRAFİK POLİTİKALAR:**

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

**15.KİŞİSEL BİLGİLERİN MAHREMİYETİ VE KORUNMASI:**

15.1. 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.
15.2. Kişisel verilerin işlenmesine ilişkin süreçlerde 6698 sayılı kanunda yer alan usul ve esaslara uygunluk sağlanmalıdır.
15.3. 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.
15.4. Hastalarla ilgili her türlü kaydın kim tarafından, hangi tarihte girildiği, ulaşma, değiştirme bilgisi hastane bilgi işlem programı log kayıtları altında tutulmaktadır.

**16.TEDARİKÇİ İLİŞKİLERİ:**

16.1. 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.
16.2. 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.
16.3. 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.
16.4. Tedarik hizmeti alınan SBYS firmasının kurum içerisinde çalışan personeliyle gizlilik sözleşmesi imzalanır.
16.5. 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.