1. AMAÇ

Fakültemizde görev yapan ve başvuruda bulunan kişilere ait bilgilerin güvenliğinin sağlanması, verilerin doğru olarak toplanması, depolanması ve kullanılmasına ilişkin uygulamalarımızı ve güvenlik önlemlerimizi dâhili olarak gözden geçirmek, kişisel verileri depoladığımız sistemleri yetkisiz erişime karşı korumak için fiziksel güvenlik önlemlerini almak ve bunun devamlılığını sağlamak, hastalara ait bilgilerin mahremiyeti konusunda uyulması gereken kuralları tanımlamaktır.

2. KAPSAM

Tüm Fakültede bulunan, görev yapan kişileri kapsar.

3. TANIMLAR

3.1. HBYS: Hastane Bilgi Yönetimi Sistemi

4. SORUMLULAR

Başta üst yönetim olmak üzere, bilgi işlem sorumluları, ilgili firmalar ve tüm çalışanlar sorumludur.

5. FAALİYET AKIŞI

5.1. Bilgi Güvenliğinin Sağlanması

5.1.1. Fakültemizde tüm hasta bilgilerinin girişi HBYS' de tanımlanan alanlara yapılmaktadır. Bu alanlardan girişi zorunlu olanlar bulunmaktadır. (TC Kimlik No, Telefon, Adres, vb.) Hasta bilgilerinin güvenliği için tüm kullanıcılar için her kademede yetkilendirme yapılır ve kontrol edilir. Kullanıcılara yetkileri hakkında eğitimler düzenlenir ve imza altına alınır. Yerilen yetkilendirmelerle ilgili yetkilendirme mesajı kullanıcılara iletilir.

5.1.2. Sunucu üzerindeki her türlü yazılım, işletim sistemi, veritabanı, Yazılım Firması elemanları tarafından, Bilgi İşlem Bölümü denetiminde yapılır. Tüm fax-modem üniteleri ile haberleşme ve İnternet erişim yazılımlarının kurulması ve ayarları Bilgi işlem Dairesi Başkanlığı yetkisinde olacaktır.

5.1.3. Hasta Bilgileri mernis sorgusu kullanılarak mernisten alınır. Mernisten alınan bilgilerin ışığında hasta bilgileri, hastanın beyanı esas alınarak sisteme girilir.

5.1.4. Hasta bilgi güvenliğinin sağlanması için hasta kayıt personellerine eğitimler düzenlenerek hastaların kayıt sırasında vermiş oldukları bilgilerinin doğruluğunu tespit etmesi sağlanır. Hasta yakınının birinci dereceden yakınlığı tespit edilir. Mahkeme kararıyla veya yayınlanan resmi bir evrakı bulunan hasta bilgileri önceden sisteme girilir, girişi engellenir veya kayıt personeli sistem tarafından uyarılır.

5.1.5. Hasta bilgisinin görülmesini veya duyulmasını istemeyen hastaların beyanı üzerine hastalara rumuz belirlenir. Hastalar bu rumuzlar üzerinden ilgili birimler tarafından çağırılır. Rumuzu değiştirilen hastanın asıl bilgilerine sistem yöneticisi ve rumuzu değiştiren personel görebilir ve işlem yapabilir.

5.1.6. Her kademedeki Fakülte personeli ancak yetkilendirilmiş olduğu işlemleri, diğer fakülte prosedürlerine uygun olarak uygular. Kişilere ait bilgilerin güvenliğinin sağlanması için öncelikle verilerin doğru olarak toplanması, depolanması, güvenlik önlemlerinin dâhili olarak gözden geçirilmesi, kişisel verilerin depoladındığı sistemlerin yetkisiz erişime karşı korunması için fiziksel güvenlik önlemlerinin alınmasını içerir.

5.1.7. Kişisel bilgilere erişim hizmetlerini işletmek, geliştirmek ve iyileştirmek için görev yapan veya çalışan personeller sınırlı tutulur. Bu bireyler gizliliği koruma yükümlülükleri altında çalışırlar ve bu yükümlülüklere uymamaları durumunda, disiplin cezası ve yasal işlemler başlatılır.

5.2. Veri Bütünlüğünün Sağlanması

5.2.1. Sağlık hizmetlerinin devamlılığını sağlamak veya geliştirmek için gerekli olan kişisel bilgileri topladığımızdan, depoladığımızdan ve kullandığımızdan emin olmak için, veri toplama, depolama ve kullanmaya ilişkin uygulamalar tekrar kontrol edilerek, kullanılan bilgilerin doğru, tam ve geçerli olmasını

sağlamak amacıyla kişisel bilgilerin güncellemeleri gerektiğinde hastalara başvurulur.

6. YEDEKLEME

6.1.1. Bilgi sistemlerinde oluşabilecek hatalar karşısında; sistemlerin kesinti sürelerini ve ısı bilgi kayıplarını en az düzeye indirmek için, sistemler üzerindeki konfigürasyon, sistem bilgilerinin ve kurumsal verilerin düzenli olarak yedeklenmesi gerekir.

6.1.2. Verinin operasyonel ortamda online olarak ayni disk sisteminde farklı disk ölümlerinde ve offline olarak Manyetik kartuş, DVD veya CD vb. ortamında yedekleri alınır.

6.1.3. Taşınabilir ortamlar (Manyetik kartuş, DVD veya CD vb.) fiziksel olarak bilgi işlem odalarından farklı odalarda veya binalarda güvenli bir şekilde saklanır/depolanır.

6.1.4. Veri yedeklerinin saklandığı kilitli dolabın/odanın anahtarı bilgi işlem birimi çalışanları dışında hiç kimsenin erişemeyeceği biçimde muhafaza altına alınır

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

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

6.1.7. Yeni sistem ve uygulamalar devreye alındığında yedekleme listeleri güncellenmelidir. Yedekleme işlemi için yeterli sayı ve kapasitede yedek üniteler seçilmeli ve temin edilmelidir. Yedekleme kapasitesi artış gereksinimi periyodik olarak gözden geçirilmelidir.

6.1.8. Yedekleme ortamlarının düzenli periyotlarda test edilmesi ve acil durumlarda kullanılması gerektiğinde güvenilir olması sağlanmalıdır.

6.1.9. Geri yükleme prosedürlerinin düzenli olarak kontrol ve test edilerek etkinliklerinin doğrulanması ve operasyonel prosedürlerin öngördüğü sureler dahilinde tamamlanabileceğinden emin olunması gerekir.

6.1.10. Yedek ünitelerin saklanacağı ortamların fiziksel uygunluğu ve güvenliği sağlanır.

7. SUNUCULARIN GÜVENLİĞİ

7.1. Fakültemizde sunucular için ayrı bir oda ayrılmıştır. Yetkili personel dışında odaya giriş engellenir. Oda kapısı sürekli kilitli tutulur. Sunucu üzerinde çalışan işletim sistemlerinin güncelliği otomatik olarak yapılmaktadır. Hizmet sunucu yazılımları ilgili firma tarafından güncellenmekte, anti virüs koruma programları bilgi işlem/bilgi işlem daire başkanlığı tarafından güncellenir. Sunucular merkezi güç kaynağı paralel bağımsız bir kesintisiz güç kaynağına bağlı olarak çalışır. Odanın Isı nem kontrolleri yapılır ve ana sunucu soğutma sistemleri bulunur. Fakültemiz Bilgi İşlem Daire Başkanlığı tarafından sağlanan güvenlik duvarı tarafından korunur. Böylece fakültemizin genel bilgi güvenliği sağlanır.

7.2. Bilgisayarlarda merkezi sunucu tarafından kontrol edilebilen antivirus yazılımı bulunur. Sunucuların yazılım bakımları teknik servis elemanları/bilgi işlem daire başkanlığı veya ilgili firma tarafından, donanımların bakımı ise fakültemiz bilgi işlem birimi tarafından yapılır.

7.3. Kurumda bulunan bütün sunucuların kayıtları tutullur, Bu kayıtlar en az aşağıdaki bilgileri içerir;

- ✓ Sunucuların yeri,
- ✓ Sorumlu kişisi,
- ✓ Donanım,
- ✓ İşletim sistemi,
- ✓ İşletim sistemi üzerinde çalışan uygulama bilgileri.

8. SİSTEM ALT YAPISINA İLİŞKİN SÜREÇLER

8.1. Veritabanı güvenliği: Fakültemizde veri tabanı sistem logları tutulur. Gerektiğinde kontroller yapılır. Veriler offline ortamda her saat/gün/hafta taşınabilir diske aktarılır, 2 TB HDD alanını dolduran veriler en eski olandan başlanarak yenisi üzerine konulur, en az 1 Yıllık veri yedeği HDD ortamında tutulur ve kilitli bir dolapta süresiz muhafaza edilir. Yedeklemeler aracılığı ile yılda bir kez veri kurtarma testi yapılır. Veri Kurtarma testi işlemiyle yedeklemeden geri dönüşün sağlanıp sağlanmadığı ve veri kaybının olup olmadığı kontrol edilir ve işlem kayıt altına alınır.

8.2. Olası bir arızada kullanıcılar arızanın oluşmasıyla sistem üzerinden veya telefonla ilgili teknik

servis sorumlusuna haber verir. Durumun bildirilmesiyle gerekli süreç başlatılır. Veritabanı yedekleri ile karşılaştırılarak oluşan veri kayıpları önlenmeye çalışılır.

9. KİŞİSEL SAĞLIK KAYITLARININ GÜVENLİĞİ

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

9.2. Veri güvenliği konusunda üç temel prensibin göz önüne alınması gerekir

- ✓ Veri gizliliği
- ✓ Değiştirilmediği (bütünlüğü)
- ✓ Erişilebilirliği

9.3. Fakültemizde kimin hangi yetkilerle hangi verilere ulaşacağı çok iyi tanımlanır. Rol bazlı yetkilendirme yapılır ve yetkisiz kişilerin hastanın Sağlık kayıtlarına erişmesi mümkün olmaz.

9.4. Sağlık kayıt bilgileri hastaya aittir. Yetkilendirilmiş çalışanlar (hastanın tedavisinden sorumlu sağlık personeli) ancak kendisine kayıtlı olan hastaların sağlık kayıtlarına erişebilmelidirler. Ancak hastanın yazılı onayı ve diğer sağlık çalışanları bu veriye erişebilirler.

9.5. İlgili mevzuat hükümleri saklı kalmak kaydıyla hiçbir hasta kaydı, elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilmemelidir." Hastanın rızası olmadan hiçbir çalışan yazılı veya sözlü olarak hasta sağlık bilgilerini hastanın yakınları dışında üçüncü şahıslara ve kurumlara iletemez.

9.6. Hasta sağlık bilgileri ticari amaçlı olarak da üçüncü şahıslara ve kurumlara iletilemez. Hastanın kullandığı ilaçlar, diyet programlan vs. buna dahildir.

9.7. Hastaların dosyasının/bilgilerinin izlenmemesi için gerekli tedbirler alınır. Hasta dosyalarının/bilgilerinin gelişi güzel ortada bırakılmaması, bilgisayar ekranının başkalarınca okunabilecek şekilde bırakılmaması sağlanır.

9.8. Telefonda konuşurken hastanın mahrem bilgileri üçüncü şahısların eline geçmemesine azami özen gösterilir.

9.9. Bütün hasta sağlık kayıtları (online bilgi veya yedek medya) fiziksel olarak korunmuş mekanlarda saklanır.

9.10. Elektronik sağlık kayıtlarına internet ortamından erişim, ancak yetkilendirilmiş kullanıcılara güvenli erişim sağlandığında mümkün olabilir.

9.11. Hasta sağlık bilgileri bilginin üretildiği kurum tarafından veya fakültemizin Bilgi Yönetim sistemleri tarafından araştırma, istatistik ve Karar Destek Sistemleri için kullanılabilir,

9.12. Sağlık kayıt dosyalarının saklandığı kağıt veya elektronik medyalar (kartuş, CD, DVD, Flash disk, HDD, vb.) güvenli bir ortamda saklanır.

9.13. Üçüncü şahısların ve/veya kuruluşların hasta sağlık kayıtlarına erişimiyle ilgili olarak, Resmi Gazetede yayınlanan "Hasta Hakları Yönetmeliği"nin ilgili maddeleri uygulanır.

10. ERİŞİM

10.1. Uzaktan Erişim Dış ortamdan iç ortama yapılan erişimler kayıt altına alınır. Dies ortamdan erişim yapılabilmesi Bilgi İşlem Dairesi Başkanlığının yetk vermesiyle olur. Fakülteye HBYS destek hizmeti veren firma dış ortamdan iç ortama hangi durumlarda erişim yapacağı hakkında bilgilendiriir ve fakülte tarafından onaylanmış gizlilik sözleşmesi imzalatılır.

10.2. İnternet Erişimi: Fakültemizde üst yönetim veya üniversitemiz tarafından belirlenen birimlere internet erişimi saglanır. İnternet erişimi sağlanamayacak olan alanlar Bilgi İşlem dairesi tarafından kapatılır.

11. E POSTA KULLANIMI

11.1. Fakültemiz veya üniversitemiz tarafından E-posta kullanımı ile ilgili süreçler belirlenir ve kurum Bilgi İşlem Dairesi Başkanlığınca E posta adresi tanımlanır. Bu postaların kontrolu ilgili daire tarafından sağlanır.

12. ŞİFRE KULLANIMI

12.1. Otomasyon erişimi verilen personellerin kullanıcı adı ve şifreleri bilgi işlem tarafından verilir

ve, bu şifrelerin kısa süre içerisinde ilgili personel tarafından belirli zaman aralıklarında değiştirilmesi istenir. Şifre değişikliği yapılmadan sisteme erişim sağlanamaz. Personelin değiştirmiş olduğu şifreler otomasyon üzerinden hiçbir şekilde görülmemektedir. Şifreler veri tabanında farklı çözülemeyen bir algoritma aracılığı ile tutulmaktadır.

12.2. Genel Şifre Oluşturma Kuralları

12.2.1. 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.
  - ✓ Aaabbb, quwerty, zyxwuts, 123321 vs. gibi sıralı harf veya rakamlar.
  - ✓ Yukarıdaki herhangi bir kelimenin geri yazılış şekli.
  - ✓ Yukarıdaki herhangi bir kelimenin rakamla takip edilmesi(örnek gizli1, gizli 2)
- Güçlü şifreler aşağıdaki karakteristiklere sahiptir.
  - ✓ Küçük ve büyük karakterlere sahiptir (örnek, a-z, A-Z)
  - ✓ Hem dijit hem de noktalama karakterleri ve ayrıca harflere sahiptir. (0-9,!@#$%A&*O_+I=VO[]:<>?,/)
  - ✓ En az 5 adet alfa numerik karaktere sahiptir.
  - ✓ Herhangi bir dildeki argo, lehçe veya teknik bir kelime olmamalıdır.
  - ✓ Aile isimleri gibi kişisel bilgilere ait olmamalıdır.

12.2.1. Şifreler herhangi bir yere yazılmamalıdır veya elektronik ortamda tutulmamalıdır. Kolayca hatırlanabilen şifreler oluşturulmamalıdır.

12.2.2. Şifre oluşturma ekranında kullanıcıya şifresinin güvenlik durumu bildirilmektedir.

12.3. Şifre Koruma Standartları

12.3.1. Kurum bünyesinde kullanılan şifreler kurum dışında herhangi bir şekilde kullanılmaz. (örnek, internet erişim şifreleri, bankacılık işlemlerinde veya diğer yerlerde) değişik işlemler için farklı şifreleme kullanın. Örnek unix sistemler için farklı şifre, Windows sistemler için farklı şifre kullanınız. Kurum bünyesinde kullanılan şifreleri herhangi bir kimseyle paylaşmayınız. Bütün şifreler kuruma ait gizli bilgiler olarak düşünülmelidir.

12.3.2. Aşağıda belirlenen burumları yapmayınız.

- ✓ 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 istediğinde bulunursa bu dokümanı referans göstererek Bilgi İşlem Birimi yetkilisini aramasını söyleyiniz.
- ✓ Uygulamalardaki "şifre hatırlama" özelliklerini seçmeyiniz. (örnek: Outlook, İnternet 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).
- ✓ Şifre kırma ve tahmin etme operasyonları belli aralıklar ile yapılabilir. Güvenlik taraması sonucunda şifreler tahmin edilirse veya kırılırsa kullanıcıya şifresini değiştirmesi talep edilecektir.

13. KABLOSUZ ERİŞİM

13.1. Fakülte içerisinde kablosuz erişim kullanılmaktadır. Tüm network erişimleri kablolu ve

kablosuz bağlantı ile yapılmaktadır. Kablolu ve kablosuz erişim için otomasyon ile bağlantıyı sağlayacak olan cihazların MAC (fiziksel) adresleri modem üzerinde kayıtlıdır. İzinsiz olarak dışarıdan girişlere kapalıdır. Kablosuz cihazların sisteme entegre edilmesinde güvenlik açısından sadece parola prosüdürü kullanılmamaktadır. Kablosuz bağlantı veya kablolu bağlantı sisteme bağlanabilmesi için Sistem yöneticisinin onayı olmadan cihazın kimlik bilgileri kaydedilmeden sisteme girişi sağlanamamaktadır.

14. YETKİLENDİRME

14.1. Fakültemizde yetkilendirmeler kullanıcıların ilgi alanlarına göre belirlenmekte ve ilgili modül yetkisi verilmektedir. Kullanıcılar yönetici, memur, laboratuar, veri giriş olarak ayrılmakta ve yetkilendirmeleri kullanım alanlarına göre yapılmaktadır, aynı görevi icra eden kullanıcılara aynı yetkiler verilmektedir. Her kullanıcıya kullanıcı adı ve şifresi verilmektedir. Tüm kullanıcıların yaptığı işlemler kayıt altına alınmakta ve bilgi işlem tarafından izlenebilmektedir. Veri tabanı ya da tablolara bilgi sisteminde yönetici olarak yetkilendirilmiş kişiler ulaşabilmektedirler.

14.2. Disiplinler arası yetkilendirme aşağıdaki gibidir

- **Dekan:** Fakültedeki tüm bilgilere ulaşır.
- **Dekan Yardımsı:** Yetki verilen alanlara ulaşır
- **Fakülte Sekreteri:** Fakültedeki alanı ile ilgili tüm bilgilere ulaşır
- **Hekimler:** Hastalara ait tedavi ile ilgili bilgilerin tümüne erişebilir. Elektronik ortamda kayıtlı olması gereken hastaya ait tüm bilgileri girebilir. Onay işlemlerini kendi şifreleri ile yapmakla yükümlüdürler. Onaylanmadan önce kendilerine ait raporlar üzerinde silme ve değişiklik yapabilir.
- **Hemşire:** Hastalara ait tedavi ile ilgili bilgilerin tümüne erişebilir. Kendi işlerine ait laboratuar ve pre-op, post- op hasta bilgilerini, hastaya ait sarf ve işlem girişlerini yetkileri dahilinde yapabilirler.
- **Personel Özlük Birimi:** Personel özlük bilgilerine ulaşabilir, mesai, izin, sevk gibi personelin tüm işleyişini otomasyon üzerinden gerçekleştirir.
- **Faturalama Birimi:** Ay içerisinde başvuran tüm hastaların faturalamasını ve anlaşmalı kurumlara teslimatı yapar. Döner sermayeden sorumlu kurumlara yapılan faturaların tutarlarını ve yapılan işlemleri görebilir inceleyebilir.
- **Eczane:** Katlardan gelen eczaneyle ilgili taleplerin girişlerini yapar, otomasyon üzerinden girişlerin ve ilaçların karşılamasını yapar. Hastaların reçeteleri doğrultusunda ilaçların takibini sağlar.
- **Radyoloji:** Hastaların radyolojik işlemlerini yapar. Tetkik işlemlerinin sonuçlarını otomasyon üzerinden onaylar. Doktorlara havale eder
- **Protez Laboratuarı:** Hekimlerin hastaları için, yaptığı protoz işlerini alır, dezenfekte eder ve sisteme kaydeder. Hastalara ait tamamlanan protezleri system üzerinden hekimlere gönderir.
- **Klinik Sekreterleri:** Hastaların gelişte otomasyon programına kayıtlarını yapar. Yatış öncesi işlemleri gerçekleştirir. Ayrıca Birimle ilgili iş ve işlemleri de yerine getirir.
- **Kalite Yönetim Birimi:** Yetki verilen alanlara ulaşır

14.3. Her kademedeki çalışan sadece yetkilendirilmiş olduğu işlemleri yürütebilmektedir. Yetkilendirilmemiş kimseler tarafından yapılan herhangi bir işlemi saptayan bölüm yetkilileri bu durumu en kısa zamanda yeterli delilleri ile birlikte dekanlığa bildirir.

14.4. Tüm çalışanlar otomasyon üzerinde yetkili oldukları bilgileri herhangi bir şekilde farklı ortamlarda paylaşamaz bilgi taşıyamaz.

14.5. Kullanılan yazılımlarla ilgili şifreler kullanıcılara BİLGİ İŞLEM tarafından verilir ve gerektiğinde değiştirilir.

14.6. Kullanıcılara Verilen Şifrelerle İlgili İşlemler Aşağıdaki Şekilde Yürütülmektedir

14.6.1. Belirli bir şifre ile yapılan tüm işlemlerin idari ve yasal sorumluluğu söz konusu şifrenin tanımlanmış kullanıcısına ait olduğundan, belli bir kullanıcıya ayrılmış şifre hangi şartla olursa olsun başkalarına verilemez.

14.7. Çalışanların Yer Değiştirmesi Veya İşten Ayrılması Durumunda Şifrenin Kapatılma İşlemleri

14.7.1. Bilgi güvenliği açısından ilişiği kesilen personelin şifresinin bir an önce iptali esastır. İlişiği

kesilen personelin tüm şifreleri ve kullanıcı yetkileri kullanıma kapatılır. Personel çıkışı veya izinli olarak ayarlandığında otomasyon otomatik olarak kullanıcı girişini kilitler.

14.8. Otomasyon Bilgi İşlem Çalışanlarının Yetkilendirme İşlemleri

14.8.1. Aşağıda belirtilen işlemler doğrultusunda çalışanları yetkilendirmektedir.

✓ Yazılım kurma ve silme işlemleri
✓ Bilgi Sistemleri Yöneticisine açık otomasyon sistemi işlemleri
✓ Üst yönetime açık otomasyon sistemi işlemleri

14.9. Yazılım Kurma ve Silme İşlemleri

14.9.1. Otomasyon sistemi dâhilindeki her türlü yazılımın kurma, silme ve düzenleme işlemleri ile işletim sistemi ayarlarının yapılması ve değiştirilmesi BİLGİ İŞLEM yetkisindedir. BİLGİ İŞLEM bilgisi dışında herhangi bir yazılım kurma ve silme işlemi ve işletim sistemi ayarları yetkilendirilmemiş bir işlem olarak değerlendirilecektir ve tamamen ilgili cihazın kullanıcısının sorumluluğundadır. Otomasyona ve fakülte güvenliğine zarar verebilecek herhangi bir yazılım fakülte network üne dahil edildiğinde bundan sorumlu kullanıcı olacaktır.

14.10. Otomasyon sistemi işlemleri

14.10.1. Fakülte bilgi yönetim sistemi işlemleri, BİLGİ İŞLEM' in onayladığı şartlar kapsamında saptanan çalışanın yetkisinde olacaktır. Verilen standart yetkiler dışında istenilen bir yetki, bağlı bulunduğu yöneticinin onayından sonra, uygun görüldüğü seviyede BİLGİ İŞLEM tarafından verilir.

14.11. Bilgi Sistemleri Yöneticisine Açık Hastane Bilgi Sistemi İşlemleri

14.11.1. Aşağıda belirtilen ve otomasyon sistemi üzerinde normal kullanıcı şifreleri ile yapılamayan işlemler BİLGİ İŞLEM 'in yetkisinde olacaktır. Bu işlemlerin yapılabilmesi için gereken şifreler BİLGİ İŞLEM Sorumlusu tarafından verilecek ve gerektiğinde değiştirilecektir.

◆ Otomasyon sistemi üzerinde rutin kullanım yolları ile ancak yanlış olarak girilmiş ve aynı yollarla değiştirilmesi mümkün olmayan bilgilerin düzeltilmesi.

◆ Doğru olarak girilmekle beraber kullanıcıların kontrolü dışında yanlış sonuçlar doğuran ve aynı yollarla değiştirilmesi mümkün olmayan bilgilerin düzeltilmesi.

◆ Yetkilendirmeye uygun olmayan hastane bilgi sistemi işlemlerinin hangi operatörler tarafından ve ne zaman yapıldığının sistem kayıtlarından açığa çıkarılması. BİLGİ İŞLEM bünyesinde halledilmektedir.

14.12. Üst Yönetime Açık Hastane Bilgi Sistemi İşlemleri

14.12.1. Üst Yönetiminin kurum planlaması, tıbbi, işletme, mali değerlendirmeler ve benzeri amaçlar ile otomasyon sistemi üzerinden alacakları raporlar BİLGİ İŞLEM tarafından yapılır.

15. GENEL KULLANIM

15.1.1. Laptop bilgisayarlar güvenlik açıklarına karşı daha dikkatle korunmalıdır. İşletim sistemi şifreleri aktif hale getirilmelidir.

15.1.2. Kurumda domain (çalışma alanı) yapısı varsa mutlaka login olunmalıdır. Bu durumda, domain' e bağlı olmayan bilgisayarların yerel ağdan çıkarılmalı, yerel ağdaki cihazlar ile bu tür cihazlar arasında bilgi alışverişi yapılmamalıdır.

15.1.3. Laptop bilgisayarın çalınması/kaybolması durumunda en kısa sürede Bilgi İşlem Birimi' ne haber verilmelidir.

15.1.4. Bütün Cep Telefonu ve PDA (Personal Digital Assistant) cihazları kurumun ağı ile senkronize olsun veya olmasın şifreleri aktif halde olmalıdır. Kullanılmadığı durumlarda kablosuz erişim (Kızılötesi, Bluetooth, vs) özellikleri aktif halde olmamalıdır ve mümkünse anti virüs programları ile yeni nesil virüslere karşı korunmalıdır.

15.1.5. Bütün kullanıcılar kendi bilgisayar sisteminin güvenliğinden sorumludur. Bu bilgisayarlardan kaynaklanabilecek, kuruma veya kişiye yönelik saldırılardan (Örneğin; elektronik bankacılık, hakaret-siyaset içerikli mail, kullanıcı bilgileri vs.) sistemin sahibi sorumludur.

15.1.6. Kurumun bilgisayarlarını kullanarak taciz veya yasadışı olaylara karışılmamalıdır.

15.1.7. Ağ güvenliğini (Örneğin; bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya

ağ trafiğini bozacak (packet sniffing, packet spoofing, denial of service vb.) eylemlere girişmemelidir.

15.1.8. Port veya ağ taraması yapılmamalıdır.

15.1.9. Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. DoS saldırısı, port-network taraması vb. yapılmamalıdır.

15.1.10. Kurum bilgileri kurum dışından üçüncü kişilere iletilmemelidir.

15.1.11. Kullanıcıların kişisel bilgisayarları üzerine Bilgi İşlem Biriminin onayı alınmaksızın herhangi bir çevre birimi bağlantısı yapılmamalıdır.

15.1.12. Cihaz, yazılım ve veri izinsiz olarak kurum dışına çıkarılmamalıdır.

15.1.13. Kurumun kullanmakta olduğu yazılımlar hariç kaynağı belirsiz olan programları (Dergi CD' leri veya internetten indirilen programlar vs.) kurmak ve kullanmak yasaktır.

15.1.14. Yetkisi olmayan personelin, kurumdaki gizli ve hassas bilgileri görmesi veya elde etmesi yasaktır.

15.1.15. Kurumsal veya kişisel verilerin gizliliğine ve mahremiyetine özel önem gösterilmelidir. Bu veriler, fakültemizin bu konudaki ilgili mevzuat hükümleri saklı kalmak kaydıyla elektronik veya kağıt ortamında üçüncü kişi ve kurumlara verilemez.

15.1.16. Personel, kendilerine tahsis edilen ve kurum çalışmalarında kullanılan masaüstü ve dizüstü bilgisayarlarındaki kurumsal bilgilerin düzenli olarak farklı ortamlara (CD, DVD, USB, External Harddisk vb) yedeklenmesinden sorumludur.

15.1.17. Bilgi İşlem birimi tarafından atanan yetkili kişiler kullanıcıya haber vermeksizin yerinde veya uzaktan, çalışanın bilgisayarına erişip güvenlik, bakım ve onarım işlemleri yapabilir. Bu durumda uzaktanbakım ve destek hizmeti veren yetkili personel kişisel bilgisayardaki kişisel veya kurumsal bilgileri görüntüleyemez, kopyalayamaz ve değiştiremez.

15.1.18. Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/ kopyalanmamalıdır.

15.1.19. Bilgisayarlar üzerinde resmi belgeler, programlar ve eğitim belgeleri haricinde dosya alışverişinde bulunulmamalıdır.

15.1.20. Kurumda Bilgi İşlem biriminin bilgisi olmadan Ağ Sisteminde (Web Hosting, E-posta Servisi vb) sunucu niteliğinde bilgisayar ve cihaz bulundurulmamalıdır.

15.1.21. Birimlerde sorumlu Bilgi İşlem personeli ve ilgili teknik personel bilgisi dışında bilgisayarlar üzerindeki ağ ayarları, kullanıcı tanımları, kaynak profilleri vs. üzerinde mevcut yapılmış ayarlar hiçbir surette değiştirilmemelidir.

15.1.22. Bilgisayarlara herhangi bir şekilde lisanssız program yüklenmemelidir.

15.1.23. Gerekmedikçe bilgisayar kaynakları paylaşıma açılmamalıdır, kaynakların paylaşıma açılması halinde de mutlaka şifre kullanma kurallarına göre hareket edilmelidir.

15.1.24. Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, ivedilikle Bilgi İşlem Birimine haber verilmelidir. Kuralların uygulanmasından birim amirleri sorumlu olup; şahısların yapmış olduğu kural ihlallerinde ilgili sistem kullanıcından başlamak üzere silsile yolu ile sorumludurlar.

16. ARIZA BİLDİRİMİ

16.1. Bilgisayar Arızaları

16.1.1. Kurumumuzda bilgi işleme yönelik arıza bildirimleri Bilgisayar Arıza Bildirimi otomasyon üzerindeki ARIZA BİLDİRİM bölümünden yapılmakta ve kayıt altına alınmaktadır. Arızlar Bilgi işleme bu yoldan iletilir. Bilgi işlem elemanı arızayı değerlendirir. Sistem üzerinden sonuçlar kayıt edilir. Kurum içinde halledilebilecek bir sorunsa sorun giderilir. Halledilemeyecek bir sorun ise ve parça değişimi gerekliyse satın alma süreci başlatılır.

16.2. HBYS Arızası ve HBYS'ye İlişkin Yazılımsal Süreçler

16.2.1. HBYS Arızalarında günün Her saatinde bilgi işlem görevlisine arıza bildirimi yapılabilir. Bildirim yapılacak kişinin iletişim adresi fakültenin tüm birimlerinde bulunmaktadır. Sorun en kısa sürede giderilir. Sorunun belirtilen sürelerde giderilemediği durumlarda ilgili firmaya cezai hükümler uygulanır.

16.2.2. HBYS' de oluşan sorun giderilinceye kadar;

a. Hasta Kabul: Başvurularda Adı-Soyadı, TC Kimlik No' su, doğum tarihi, telefon numarası, adresi ve hangi poliklinikte muayene olacağı v.b. hasta bilgileri "HBYS'nin Hizmet Vermediği Durumlarda

Hasta Bilgi Formuna" eksiksiz doldurularak hasta kaydı yapılır. HBYS' de sorun düzelince sistem üzerinden hasta kayıt işlemleri yapılır.

b. Acile Başvurular: Acil hasta kabul defterine hastaların Adı-Soyadı, TC Kimlik No' su, doğum tarihi, baba adı, telefon numarası, adresi kayıt edilir. Hastalar muayene edilip yapılan işlemler, uygulanan ilaçlar hasta kabul defterine ve ilgili formlara kayıt edilir. Tetkik istemlerinde "HBYS'nin Hizmet Vermediği Durumlarda **Tetkik İstem Formu"** doldurularak istemler yapılır. Sevk olan hastalar için **Hasta Sevk Formu** doldurulur. HBYS' de sorun düzelince sisteme hastaların, yapılan işlemlerin ve sevklerin girişleri yapılır.

c. Klinik Hastaları: K linik hasta kabul defterine hastaların Adı-Soyadı, TC Kimlik No' su, doğum tarihi, baba adı, telefon numarası, adresi kayıt edilir. Muayene işlemi yapılır. İstenen tetkikler, uygulanan ilaçlar, yapılan işlemler ve hastanın reçetesi kayıt edilir. Tetkik istemlerinde "HBYS'nin Hizmet Vermediği Durumlarda Tetkik İstem Formu" doldurularak istemler yapılır. Sevk olan hastalar için Hasta Sevk Formu doldurulur. HBYS' de sorun düzelince sisteme hastalara yapılan işlemler ve reçetelerin girişleri yapılır.

d. Hasta Yatış İşlemleri: HBYS' de sorun düzelinceye kadar hastaların Adı-Soyadı, TC Kimlik No' su, doğum tarihi, baba adı, telefon numarası, adresi hasta yatış defterine kayıt edilerek hastaların yatış-çıkış işlemleri yapılır, hasta dosyası doldurulur. Hasta dosyasındaki Hasta Tabelasına yazılan ordera göre eczaneden ilaçlar alınır ve uygulanır. Tetkik istemlerinde HBYS'nin Hizmet Vermediği Durumlarda Tetkik İstem Formu doldurularak istemler yapılır. Sevk olan hastalar için Hasta Sevk Formu doldurularak sevk işlemi yapılır. HBYS' de sorun düzelince sistemden hastaların yatış-çıkış ve sevk işlemleri yapılır. Hastaya yapılan tüm işlemler, e-order, uygulanan ilaçlar, hasta reçetesi ve ilaç raporu girişleri yapılır.

e. Eczane: Eczanede ilaç çıkışları e-order ile yapılmaktadır. HBYS' deki sorunlarda sistem düzelinceye kadar Hasta Tabelasının fotokopisi çekilir ve tabelaya göre eczaneden ilaç çıkışları yapılır. HBYS' de sorun düzelince sistemden hasta tabelalarına göre ilaç çıkışları yapılır.

f. Radyoloji: Tetkik istemlerinde HBYS'nin Hizmet Vermediği Durumlarda Tetkik İstem Formu doldurularak istemler yapılır. Radyoloji biriminde çekim işlemleri yapılır. Sorun giderilince HBYS üzerinden çekimlerin girişleri yapılır.

g. Labaratuvar: Tetkik istemlerinde HBYS'nin Hizmet Vermediği Durumlarda Tetkik İstem Formu doldurularak istemler yapılır. Laboratuarda yapılabilecek tetkikler manuel olarak yapılır. Sistem gelince cihazlardan HBYS'ye veriler transfer edilir.

17. BİLGİ İSTEME HAKKINI KULLANMASI

17.1.1. Fakültemize başvuran kişiler için hazırlanmış Fakülte Bilgi Rehberi'nden yararlanılabilir. Fakültemize başvuran kişiler sosyal, dinsel, fiziksel, ruhsal ve düşünsel özelliklerine bakılmaksızın, var olan tanı, tedavi ve rehabilitasyon olanaklarından en üst düzeyde yararlanma hakkına sahiptir.

17.1.2. Fakültemizde verilen tüm hizmetler için fakülte tanıtım broşürü bulunmaktadır. Bu tüm hizmetlerimize ulaşım konusunda gereken bilgiyi içerir. Ayrıca Fakültemizde verilen hizmetler, topluma yönelik tanıtım seminerleri vb. bilgiler duyuru panoları aracılığı ile de yapılır.

17.1.3. Hastalarımızın, kendileri ya da yasal vasileri kanalı ile tanı ve tedavinin tüm süreçlerine ve hastalığın olası gidişatına ilişkin tam ve yeni bilgi alma, kuruluşumuzun kendilerine ilişkin tıbbı dokümantasyonun bir kopyasını alma hakkı vardır.

18. KAYITLARI İNCELEME HAKKINI KULLANMASI

18.1.1. Hastalar, dosyasında bulunan bilgi kayıtlarını, doğrudan veya vekili veya kanuni temsilcisi vasıtası ile inceleyebilir ve bir suretini alabilir. Bu kayıtlar, sadece hastanın tedavisi ile doğrudan ilgili olanlar tarafından görülebilir.

18.1.2. Hasta katlarında bulunan hasta dosyalarımız hasta taburcu işlemleri tamamlandıktan sonra güvenliği sağlanmış arşivlerde ve bilgisayar sistemlerinde tutulmaktadır.

18.1.3. Bakım verecek sağlık çalışanları hastaya ait eski kayıtlara gerekli görüldüğü durumlarda ulaşabilmelidir.

19. BİLGİLERİN DÜZELTİLMESİNİN SAĞLANMASI

19.1.1. Fakültemize müracaat eden kişiler talep ettikleri kayıtlarda herhangi bir kayıt eksikliği, tanımlama hatası, açıklama ya da düzeltme talep ederler ise; hasta dosyası dekanlık ve onun belirleyeceği yetkili muhakkik tarafından incelenerek uygun bulunur ise düzeltme yapılarak kişiye düzeltme bildirilir. Yapılan inceleme neticesinde düzeltme tıbbi, etik ve yasal kurallara uygun bulunmuyor ise düzeltmenin yapılmayacağı ilgili kişiye bildirilerek yasal süreci başlatabileceği bildirilir.

20. BİLGİ VERİLMESİ UYGUN OLMAYAN VE TEDBİR ALINMASI GEREKEN HALLERLE İLGİLİ BİLGİNİN VERİLMESİ

20.1.1. Fakültemizde hasta ile ilgili tüm tıbbi bilgiler her gün hekim ve sorumlu hemşire tarafından hastaya ve hastanın kendi hastalığı hakkında bilgi verilmesini istediği kişilere durumu hakkında bilgilendirme yapılır.

20.1.2. Konulan teşhisin hastaya söylenmesinin doğuracağı olumsuz etkiler göz önünde bulundurularak hastalığının artması ihtimalinin bulunması veya hastalığın seyrinin ve sonucunun vahim görülmesi hallerinde, teşhis hastadan saklanabilir. Ancak hastanın yasal temsilcisine tüm bilgiler verilerek beraber karar oluşturulur.

20.1.3. Tedavisi olmayan bir teşhis, ancak bir hekim tarafından ve tam bir ihtiyat içinde bildirilir.

20.1.4. Yasal konular dışında, hasta, sağlık durumu hakkında kendisine veya ailesine, yakınlarına bilgi verilmemesini isteyebilir. Hasta veya hasta yakını hakkında bilgi almak istediği alanları ve sınırları tarafımıza bildirmelidir.

21. BİLGİ VERİLMESİNİ YASAKLAMA DURUMU

21.1.1. Hastalarımız sağlık durumu hakkında verilecek gerçek bilgilerin kendisini etkileyeceğini düşünüyor ise bu konuda kendisine ve ailesine bilgi verilmemesini talep edebilir. Bu durum Genel Bilgilendirme ve Onam Formu'na not olarak yazılır. Bu amaçla bilgi verilmesi yasaklanan durum ve kişiler (yasal yeterlilik çerçevesinde) kurumumuz yetkililerine yazılı olarak bildirilir. Hastalarımız tek kişilik odalardayken yapılan işlemler esnasında yanlarında bulunacak veya bulunmayacak yakınlarına karar vererek bunu bildirirler.

21.1.2. Hastalarımız ile ilgili bilgilerin paylaşımları hastalarımızın ve yasal temsilcilerinin belirlediği kişilerin yanında ve onların belirlediği ortamlarda yapılmaktadır. Hastalarımızın ismi ve kendileri tarif edilerek yapılacak bilgi paylaşımları genel ortamlarda ve başkalarının bulunduğu alanlarda yapılamaz.

21.1.3. Hastalarımızın sağlık değerlendirmelerine "Hastane Bilgi Sistemi"ndeki yetkilendirilmiş kişiler tarafından ulaşılabilmektedir.

21.1.4. Hastalarımızın ölümü halinde mahremiyet hakları bozulmaz.

21.1.5. Hastanemizde hasta ile ilgili bilgilerin bütünlüğü ve güvenliği kurulmuş olan bilgisayar yazılım programlarında yetkilendirilmiş girişler ile korumaya alınmıştır. Elektronik ortamdaki verilerin güvenliği sağlanmaktadır.

21.1.6. Hasta dosyalarına yetkili olmayan kişilerin ulaşımına / kullanımına izin verilmemektedir.

21.1.7. Basılı doküman ile ilgili güvenlikler Devlet Arşiv Hizmetleri Yönetmeliğinde belirlendiği şekilde güvenliği sağlanmakta ve belirli zaman aralıklarındaki denetimlerle kontrolü yapılmaktadır.

21.1.8. Resmi makamların kurumumuzdan istediği evraklar tarafımızdan onlara ulaştırılmaktadır. Ancak rutin dışı resmi evrak talepleri kurumumuzun ilgili birimlerinden talep edilmelidir.

Hazırlayan	**Kontrol Eden** Kal. Yön. Direkt.	**Onaylayan** Dekan