1. Amaç: Bilgi Yönetimi kapsamına giren alan ve faaliyetlerin koşullarını, esaslarını, işleyişini ve kurallarını belirlemektir.

2. Kapsam: Demo Sağlık Tesisi'nin tüm birimlerini kapsar.

3. Tanımlar :

HBYS: Hastane Bilgi Yönetim Sistemi

PBS: Personel Bilgi Sistemi

Server: Ana Bilgisayar (Sunucu Bilgisayar) . Üzerinde tüm bilgilerin saklandığı ve genellikle diğer bilgisayarlara oranla daha hızlı ve kapasitesi yüksek bilgisayar.

LAN: Yerel Ağ. Yüksek hızda veri transferi özelliğine sahip server, PC, printer gibi birimlerden oluşan bir ağ türüdür.

Network: İkiden fazla bilgisayarın birbirleriyle iletişim halinde olmasıdır. (Ağ kablolama)

Switch: Network sistemlerinde, LAN içerisindeki aygıtların ortak kullanım için birbirine bağlanmasını sağlayan ve LAN içerisindeki cihazlardan gelen veri paketlerini filtreleyerek sadece ilgili porta gönderen cihazdır.

Admin (Administrator) : Bilgi İşlem Sistemi içindeki üst düzey yetkili.

DÖF: Düzeltici Önleyici Faaliyet

4. Sorumlular:

• Başhekim,

• Başhekim Yardımcısı,

• Hastane Müdürü, Müdür Yardımcısı,

• Bilgi İşlem Sorumlusu,

• Bilgi İşlem Çalışanları,

• Teknik Hizmetler Amiri,

• Teknik Servis Çalışanları,

• Sistemi kullanan tüm çalışanlar.

5. Bilgi Güvenliği:

Bilgi güvenliği risklerinin azaltılması, ortadan kaldırılması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik bilgi/verinin güvenliğinin sağlanması için asgari güvenlik tedbirlerinin belirlenmesi ve belirlenen tedbirlerin uygulanması için yürütülecek faaliyetlerin tanımlanmasıdır. Bilgi güvenliğine ilişkin süreçlerin detayları "Bilgi Güvenliği Politikası" içerisinde yer alır.

6. Faaliyet Akışı:

6.1. Bilgi Yönetimine İlişkin Faaliyetlerin Yürütülmesi ve Koordinasyonuna Yönelik Sorumlular Ve Sorumluluklar

6.1.1. Hastane Bilgi Yönetimi Sistemini kullanan tüm çalışanlar: HBYS sistemini kullanan tüm çalışanlar hastanedeki mevcut tüm bilgisayarlardan kendilerine verilmiş ve görevleri ile yetkilendirilmiş kullanıcı kodu ve şifresi ile yaptığı tüm işlemlerden sorumludur. (Veri girişi, değiştirmesi, silmesi vb.)

6.1.2. Bilgi İşlem Sorumlusu:

• Bilgi işlem merkezinde görevli personelle hastanede çalışan tüm personellere otomasyon ile ilgili destek

vermek.

• Hastane birimlerinde çalışan tüm personellerin yazılım üzerinde oluşabilecek yenileme, düzeltme gibi işlemleri tespit edip firma yöneticisine teslim etmek.

• 24 saat boyunca icap yöntemi ile hastane çalışanlarına uzaktan veya bizzat hastaneye gelerek soruna müdahale etmek.

• Yazılım üzerinde her türlü gelişmeye destek vermek.

• Bilgi işlem merkezi personeli tarafından, hastane çalışanları tarafından bildirilen istekleri yazılım şirketine iletmek, takip etmek ve sonucunu bilgi işlem merkezi sorumlusuna rapor etmek.

• Hastane ile yazılım şirketi arasında koordineyi sağlamak.

• Hastaneye ait bilgisayar sisteminin verimli ve amaca uygun çalışmasını sağlamak.

• Sistemlerin arızalanması durumunda ön inceleme ve bakımını yaparak, gerekli servis hizmetlerinin verilmesini sağlamak.

• Bilgisayar sistemlerinin periyodik bakımlarında ve onarımlarında sözleşmeli firma elemanlarını ve çalışmalarını denetlemek, gerekli gördüğü hallerde yazılı-sözlü bilgi vermek.

• Teknik malzemelerin alımında malzemelerin şartnamelere uygunluğunun kontrolünü yapmak.

• Faaliyetler çerçevesinde, ihtiyaç duyulan yazılım sistemleri konusunda personele destek vermek; meydana gelen küçük teknik arızaları geciktirmeden gidermek veya giderilmesini sağlamak.

• Bilgisayar donanımlarında meydana gelen aksaklıkların giderilmesi için amirine bilgi vermek.

• Konusuyla ilgili olarak amiri tarafından verilen diğer işleri yerine getirmek.

6.1.3. Bilgi Yönetim Sistemine ilişkin rol grupları ve yetkileri

• Yetkilendirme işlemi personelin hastanede göreve başlamasıyla yapılır, birim ve/veya görev alanı değişmesi durumunda yetkiler yeni görev tanımına göre düzenlenir, personelin kurumdan ayrılışı durumunda yetkiler kaldırılıp kullanıcı hesapları pasif hale getirilir. Yapılan tüm işlemler personelin işlem tipine göre (başlayış, birim değişimi, ayrılış) formlar üzerinden yapılır.Otomasyon üzerinde yazılımı kullanan tüm personellerin yetkilendirilmesi yapılmıştır. Bu gruplardaki personeller yalnızca kendilerine verilen yetki kadar işlem yapabilir. Bu rol grupları;

- Hekimler
- Eczacı
- Hemşireler
- Laboratuvar
- Sekreterler vb.

• Çalışanların yetkileri düzenlenmiştir ve kayıt altına alınmaktadır. Aynı görevde çalışan personellerin yetkileri de aynıdır. İşe yeni başlayan, birim görev değişimi yapan veya ilave görevlendirme yapılan personel "HBYS Yetki Formu" doldurarak birim yöneticisinin onayı ile yetkilendirme yapılır. İşten ayrılırken ise ilişik kesmek için bilgi işleme başvurulup ilgili kişinin SBYS yetkileri sistem üzerinden kaldırılır. Rol grupları ile kullanıcılara atanan yetkiler periyodik olarak kontrol edilir.

6.1.3. Rol Grupları ve Disiplinler Arası Yetkilendirme:

• **Doktor;** Hastalara ait tedavi ile ilgili bilgilerin tümüne erişebilir. Elektronik ortamda kayıtlı olması gereken tüm hastaya ait tüm bilgileri girebilir. Onay işlemlerini kendi şifreleri ile yapmakla yükümlüdürler. Onaylanmadan önce kendilerine ait raporlar üzerinde silme ve değişiklik yapabilir. Hasta ‘Adli Olgu’ ise hasta raporu ancak Uzman tarafından girilebilir ve aynı Uzman tarafından onaylandıktan sonra değiştiril değiştirilemez.

• **Hemşire;** Hastalara ait tedavi ile ilgili bilgilerin tümüne erişebilir. Silme ve değiştirme yetkileri yoktur. Kendi işlerine ait laboratuar ve preop-postop. hasta bilgilerini, hastaya ait sarf ve işlem girişlerini yetkileri dahilinde yapabilirler.

• **Eczane:** Katlardan gelen eczaneyle ilgili taleplerin girişlerini yapar, otomasyon üzerinden girişlerin ve ilaçların karşılamasını yapar. Hastaların reçeteleri doğrultusunda ilaçların takibini sağlar.

• **Laboratuar ;** Doktorların hastaları için, yaptığı istemleri alır, çalışmasını yapar ve otomasyon üzerinde hastanın sonuçlarını girer. Otomatik cihazlar için bu işlemler barkotlu sistem ile çalışır. Hasta test sonuçları Laboratuar Uzman Doktoru tarafından onaylandıktan sonra istem yapan kişiler tarafından hasta dosyasında sonuçlar görülebilir. Hastalar muayene oldukları poliklinikten ve web üzerinden (hastane web sayfası) sonuçları alabilirler.

• **Poliklinik Sekretarya**

Hastaların gelişte otomasyon programına kayıtlarını yapar. Yatış öncesi işlemleri gerçekleştirir. 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 bağlı bulunduğu birime iletilmek üzere bir üst yetkiliye bildirmektedir. Tüm çalışanlar otomasyon üzerinde yetkili oldukları bilgileri herhangi bir şekilde farklı ortamlarda paylaşamaz bilgi taşıyamaz.

6.2. Bilgi Sistem Donanım ve Altyapı, Yönetim ve Talep Süreçleri :

Hastanemizde faaliyet gösteren Yazılım-Donanım Destek Birimi 24 saat kesintisiz hizmet sunmakta olup; ortaya çıkabilecek aksaklıklar için Yazılım Donanım Destek Birimi çalışanlarının güncel iletişim bilgilerine santralden ulaşılabilir. Hastane Bilgi Yönetim Sistemi dahilinde yer alan donanım ihtiyaçları bilgi işlem birimi tarafından belirlenerek hastane idaresine yazılı olarak bildirilir. İhtiyaç tespit komisyonu tarafından uygun görülen talepler işleme alınır temin süreçleri başlatılır.

6.3. SBYS İşletimi ve Değişiklik Yönetimi:

Hastane Bilgi Yönetim Sistemi'ne ait otomasyon yazılımı hastane bünyesi ve veya il sağlık müdürlüğü tarafından il genelini kapsayan ihale süreci ile temin edilir, Mevcut Bilgi Yönetim Sistemi'ni İşleten firmanın yasal işletim süresi sonunda ihale süreçleri tekrar başlatılır.

6.4. Hastane Bilgi Yönetim Sistemi’nde (HBYS) yer alan modüller tek bir veri tabanı üzerinden yönetilmelidir:

Hastane Bilgi Yönetim Sisteminde yer alan modüller tek bir veri tabanı üzerinden yönetilmektedir. Hastane Bilgi Yönetim Sisteminde yer alan temel modüller, Ayaktan Hasta Kabul, Yatan Hasta Kabul, Poliklinik, Klinik, Merkezi Sterilizasyon, TRSM, Eczane, Depo, Satınalma, Ayniyat, Laboratuvar, Vezne, Radyoloji, Fatura, Doğum ve ameliyathane, Danışma Modülü olarak bulunmalı ve kullanılmalıdır.

6.5. HBYS’de personel bilgi modülü bulunmalıdır:

Hastanemiz Hastane Bilgi Yönetim Sistemi Personel Bilgi Modülünde fotoğrafı, çalıştığı birim, kadro bölümü, kan grubu, iletişim bilgileri, izin ve rapor bilgileri, eğitim durumu, sertifikaları, hizmet içi eğitimleri, yabancı dil bilgisi bulunur ve Personel Özlük Birimi tarafından güncel olarak takip edilir.

6.6. BYS'yi Oluşturan Alt Sistemler :

LBYS, PACS, Web, E-Posta, Dosya Sunucu, Tarama Sunucu, İş Zekası ve benzeri gibi Bilgi Yönetim Sistemini'ni oluşturan uygulamalar hastane sunucu sistemi bünyesinde merkezi veritabanından bağımsız veri alışverişi noktasında birbirlerine bağlantılı olarak kurgulanmaktadır.

6.7. HBYS’ye bağlı tüm bilgisayarlara yönelik düzenleme yapılmalıdır: (Varlık Yönetimi)

Hizmet binamızda kullanılacak tüm bilgisayar donanım ve yazılımların güncel envanteri oluşturulur. Bilgisayar Donanım ve Yazılım Envanteri kullanılarak cihazların bulunduğu bölüm, donanım ve yazılım adı, işletim sistemi, ek aksamlar, varsa garanti süresi ayniyat birimi tarafından kayıt altına alınır.

6.8. Bilgi güvenliğini sağlamaya yönelik düzenleme ve RİSK yönetimi yapılmalıdır:

• Bilgi güvenliğine ait süreçlerin detaylı açıklaması "Bilgi Güvenliği Politikası" içerisindedir.

• Sunucuların fiziksel ve sistemsel güvenliğinin sağlanması; veri merkezince yapılmaktadır.

• Yedekleme işlemi; veri merkezince yapılmaktadır.

• İnternet erişim ve kullanımı, Demo Sağlık Tesisi yerleşkesinde bulunan Veri Merkezinde merkezi olarak yapılmaktadır.

• Herhangi bir virüs tehdidine karşı tüm bilgisayarlarda Veri Merkezindeki merkezi sunucu tarafından kontrol edilebilen antivirüs yazılımı kurulmuştur.

• Virüslü olduğu tespit edilen meteryal (Cd, DVD, Flaşh Bellek, External Harddisk) temizlenmeli, temizlenemiyor ise imha edilmelidir.

• Şifre Kullanımı otomasyon sistemi yetkilendirme yapıldıktan sonra imza karşılığında birimlerde bulunan form ile verilmektedir.

• Kişisel bilgilere erişim hizmetlerimizi işletmek, geliştirmek ve iyileştirmek için, onları, bilmeleri gereken hastane çalışanları, yüklenicileri ve aracılarıyla sınırlı tutulur. Bu bireyler gizliliği koruma yükümlülükleri altında çalışırlar ve bu yükümlülüklere uymamaları durumunda, işlerine son verilmesi, disiplin cezası ve yasal işlemler başlatılır.

• Uzaktan erişim konusunda bilgi işlem personeli tarafından önceden oluşturulmuş şifreler ile bilgi işlem personeli ile otomasyon firmasının yetkilendirdiği kişiler tarafından ulaşılabilecek şekilde yapılandırılmış olup; süreçten Hastane Bilgi İşlem birimi sorumludur.

• Çalışanların yer değiştirmesi veya işten ayrılması durumunda şifrelerinin kapatılma işlemi bilgi güvenliği açısından ilişiği kesilen personelin şifresinin bir an önce iptali esastır. İlişiği kesilen personelin tüm şifreleri ve kullanıcı yetkileri kullanıma kapatılır. Şifrenin, ilişiği kesilen personelin haber verilmesi ile birlikte 24 saat içerisinde iptali Bilgi İşlemin sorumluluğundadır.

• Bilgi işlem birim sorumlusu Başhekim, İdari ve Mali İşler Müdürü ve Bilgi İşlem Sorumlu Memurunun katılımı ile Bilgi Güvenliği Ekibi oluşturulmuştur. Bilgi Güvenliği Ekibinin sorumlulukları;

- Bilgi güvenliği ile ilgili mevcut durum tespit edilir.

- Bilgi güvenliği için olası riskleri belirleme

- Tanımlı kullanıcılar için yapılan yetki değişikliklerini izleme.

- Bilgi güvenliği konusunda çalışanlara yılda en az bir kez eğitim verilir.

• Risk analizleri en az altı ayda bir olacak şekilde düzenli aralıklar ile ve gerektiğinde güncellenmektedir.

6.9. Bilgi güvenliği yönetimi ihlali yönetimi

• İhlal bildirimleri **“İstenmeyen Olay Bildirim Formu”** aracılığı ile gerçekleştirilir.

• BGYS Birim sorumlusu bildirimin bilgi güvenliği ihlal olayı olup olmadığını tespit eder, analizini yapar ve yayılmasını önlemek için alınması gereken acil eylem gerekli ise süreci başlatır. Olayın ciddiyeti değerlendirilip yasal işlem öngörülmekte ise, ilgili hukuki ya da güvenlik otoriteleri sürece dâhil edilir.

• Gerekli görülen durumlarda DÖF başlatılır.

6.10. Bilgi Teknolojileri İmha Yönetimi

Kişisel verilerin hiç kimse tarafından hiçbir şekilde erişilemez, geri getirilemez ve tekrar kullanılamaz hale getirilmesi işlemidir verilerin korunması kanunu çerçevesinde yapılmaktadır. "Bilgi Saklama ve Ortamları Yok Etme Prosedürü" ile detaylı olarak işlenmektedir.

6.11. Sunucu odalarının güvenliği sağlanmalıdır:

Sunucular Veri Merkezinde bulunmakta, hastanemiz Web tabanlı otomasyon yazılımı ile VPN bağlantısı

kullanılarak bağlantı sağlamaktadır. Sunucu odası fiziki olarak diğer birim alanlarından izole ayrı bir ortamda kurgulanıp, İlgili odaya erişim yalnızca yetkili kişilerce sağlanmaktadır.

6.12. Sunucunun güvenliğini sağlamaya yönelik tedbirler alınmalıdır.:

Sunucu güvenliği veri merkezince sağlanmaktadır. Veritabanı güvenliği: "İz Kayıtları Yönetim Talimatı" içinde detaylı olarak işlenmektedir.

6.13. Veritabanı güvenliğini sağlamaya yönelik tedbirler alınmalıdır:

Veritabanı güvenliği Veri merkezince sağlanmaktadır.

6.14. Dış ortamdan iç ortama erişimlerde güvenlik tedbirleri alınmalıdır:

Hastane destek hizmeti veren firmanın dış ortamdan iç ortama hangi durumlarda erişim yapacağı bilgi işlem biriminin bilgisinde, dış ortamdan iç ortama yapılan erişimler Sağlık Bakanlığı SBA altyapısı ile İl Sağlık

Müdürlüğü bünyesinde VPN hesapları ile kontrol edilmektedir.

6.15. HBYS üzerindeki verilerin yedeklenmesine yönelik düzenleme bulunmalıdır:

Yedekleme işlemi veri merkezince sağlanmaktadır. Yedekleme düzeni ve kuralları kendi içerisinde ayrı bir

prosedör olarak oluşturulmalıdır. (bkz "Yedekleme Politikası")

6.16. Hastane bilgi sisteminde yetkilendirme yapılmalıdır:

• Her kullanıcı veri tabanından hangi bilgilere erişebileceği tanımlanmıştır. Çalışanlar yetki düzeyleri ile ilgili olarak bilgilendirilmiş, bilgilendirme ve yetki düzeyi kayıt altına alınmıştır. Aynı görevi icra eden çalışanlar aynı yetki gruplarına sahiptir. Verilere ve sisteme ulaşmada yetkilendirme OKU, OKU+YAZ, OKU+YAZ+DÜZELT, OKU+YAZ+DÜZELT+SİL ve ADMİN olmak üzere şekilde yapılır. Modüllere ulaşılması için kullanıcılara, kullanıcı kodu ve kullanıcı şifresi verilir. Kullanıcıların kendi çalıştığı alan ve o alanla ilgili diğer modüllere ulaşılmasına izin verilir. Yetkilendirme sistemi içinde izin öncelikle sisteme giriş, modüle giriş, modül alanı içindeki alt modüle giriş ve alt modül içinde OKU, OKU+YAZ, OKU+YAZ+DÜZELT, OKU+YAZ+DÜZELT+SİL sırasını izler.

• Yetkilendirme Dereceleri;

- Bilgi İşlem için sistem yöneticisi,
- Hastane yönetimi için gözlemci
- Medula sistemi için ileri düzey
- Poliklinikler için Oku-yaz-sil
- Servis takip için Oku-yaz-sil
- Diğer birimler için oku-yaz yetkisi verilmekte ancak birim sorumlularının belirlediği kişilere oku-yaz- sil olarak yetkilendirme yapılmaktadır.
- Raporlama işlemleri için oku şekilde yetkilendirme yapılmıştır.
- Yetki değişikliği talebi ve değişiklik onay yetkilisi tanımlanmıştır.

6.17. HBYS üzerinde yapılan işlemler izlenebilir olmalıdır:

Veritabanı sisteme giriş yapan kullanıcılar gerçekleştirdikleri işlemler, sistem ayarlarında gerçekleştirilen değişiklikler, sistem mesajları ve hatalar ile ilgili kayıtlar kayıt altına alınır. Bu veritabanına da sadece bilgi sisteminde yönetici olarak yetkilendirilmiş kişiler ulaşılabilmektedir. Bilgi Yönetimi Sistemi'nde yapılan işlemlere ait kayıtlar ve detaylı bilgilendirme "İz Kayıtları Talimatı'nda yer almaktadır.

6.18. İş Sürekliliği Yönetimi'ne yönelik düzenleme yapılmalıdır:

Sisteme veri girişi ile ilgili kullanıcı hataları acil olarak telefon veya arıza bildirim ekranı aracılığı ile Bilgi İşlem yazılım-donanım- destek birimine bildirilir ve en kısa sürede hatalı/yanlış bilgi düzeltilir, eksik bilgi tamamlanır. Donanım arızaları HBYS üzerindeki Arıza Bildirim ekranı veya telefon aracılığı ile Bilgi İşlem Birimine bildirilir. Arızalara müdahale önceliği Tıbbi Hizmet Birimleri Mali Hizmet Birimleri ve İdari Hizmet Birimleri şeklindedir. Sorunun giderilinceye kadar işlerin aksamamasına yönelik olarak ilgili birime donanım desteği sağlanır. Arıza bildirimi yapılırken; Hatanın oluştuğu tarih ve saat, bildirimin yapıldığı tarih ve saat, hatanın içeriği ve hatanın giderildiği tarih ve saat bilgileri arıza modülü ile kayıt altına alınır.

• Mesai sonrası, hafta tatili, Resmi ve Dini Bayramlarda ise nöbetçi memur tarafından santralden bilgi işlem personeli aranılarak bildirim yapılır.

HBYS de oluşabilecek sorunlar ve Çözümleri		
Birim Adı	Hatanın Tanımı	Çözüm
Ayaktan hasta Kabul	Kullanıcı Hatası	Yanlış Veri düzeltilir ve kullanıcıya eğitim verilir
Yatan Hasta Kabul	Kullanıcı Hatası	Yanlış Veri düzeltilir ve kullanıcıya eğitim verilir
Vezne	Kullanıcı Hatası	Yanlış Veri düzeltilir ve kullanıcıya eğitim verilir
Poliklinik	Kullanıcı Hatası	Yanlış Veri düzeltilir ve kullanıcıya eğitim verilir
Cihaz Takip	HBYS	Teknik Birimler
Laboratuar	Donanım	Acil hallerde Arıza Bitinceye kadar manuel çalışma
İdari Birimler	HBYS/donanım	Arızanın durumuna göre müdahale
Tüm Birimler	Network	Teknik olarak anında müdahale
Veri tabanı arızası	Yazılım	Anında Müdahale (Veri Merkezi bildirim)

• HBYS tekrar aktif olduğunda bu süreçte elde edilen veriler HBYS'ye birimlerin kendileri tarafından veri doğruluğu kontrol edilerek ve bilgi işlem teknik ekibinin belirlediği metotla kaydedilir.

• HBYS ile ilgili sorumlular ve çözümler kayıt altına alınırken;

• Sorunun oluştuğu tarih ve saat,

• Bildirimin yapıldığı tarih ve saat,

• Hatanın içeriği

• Sorunun çözüldüğü tarih ve saat kayıt altına alınır.

• Sorunlar ile ilgili olarak birim ve kullanıcı bazında hata sayısı, birim ve kullanıcı bazında hata nedeni, sorunun oluştuğu saat ve bildirimin yapıldığı saat arasındaki süre, bildirimin yapıldığı saat ve soruna müdahale saati arasında geçen süre sorunun giderilme sürelerini kapsayan aylık istatistiksel çalışma yapılır. Sorunlar ile ilgili düzeltici önleyici faaliyet başlatılır.

6.19. Diğer Uygulamalar

6.19.1. Bilgi İşlem Altyapısı:

• Bilgi İşlem çalışmaları için bir Network Ağı sağlanır. Ağa bağlı veya bağlanacak bilgisayarlar yönetimini organize etmek üzere (switch, cat 6 kablo, RJ45 connector) malzeme temin edilir. Tüm faaliyetleri yürütmek ve kayıt altına almak amacıyla, HBYS ve ayrıca Sağlık Bakanlığı ve Sağlık Müdürlüğü direktifleri ile kurum ihtiyaçları doğrultusunda Hastane Otomasyon Sistemi kurulur. Laboratuar Hizmetleri için Laboratuar Cihazları tedarikçisinin sağlamış olduğu yazılım kullanılır. Bu yazılım Hastane Bilgi yönetim sistemi ne entegre edilir.

• Bilgisayar donanım ve yazılımlarının güncel envanteri oluşturulur. Envanterde; bu yazılım ve donanımların bulunduğu bölüm, marka, model, seri no, demirbaş numarası, donanım ve yazılım adı, işletim sistemi, ek aksamlar, alınma tarihi, varsa garanti süresi gibi bilgileri kapsamalıdır.

6.19.2. Bilgi İşlem Birimi Faaliyetlerinde Görev Alan Personel:

Bilgi İşlem Birimi Başhekim, Hastane Müdürü, Sorumlu Memur ve hastanenin kendi yapmış olduğu hizmet

alımı ile görevlendirdiği personel ile otomasyon hizmeti satın alınan firmanın Hastane Otomasyon Hizmetleri Sözleşmesine göre sözleşmede belirtilen sayı kadar görevlendirdiği en az lise düzeyinde Bilgisayar Operatörlüğü veya Programcılığı Bölümü mezunu personelden oluşur.

6.19.3. Hastane Otomasyon Hizmetleri Sözleşmesinin Kapsamı:

• Kumru Devlet Hastanesinde HBYS' in kurulması ve verimli bir şekilde işletilmesidir. Hastane Bilgi Sistemleri (HBS) sadece hastane içi süreçleri etkileyen ve bu süreçlerden etkilenen bir yapı olmayıp diğer sistemlerle de veri alış verişi yapabilen sistemlere dönüşmüştür.

• Bu nedenle veri tabanında yer alan tüm verilerin gerektiğinde kullanılmak üzere başka bir veri tabanına eksiksiz aktarılması, ihtiyaç duyulacak başka verilerin (Kimlik Paylaşım Sistemi (KPS), Çekirdek Kaynak Yönetim Sistemi (ÇKYS), elektronik faturalama süreçleri (MEDULA), Sağlık –NET vb, Kan Merkezi, , Merkezi Randevu Sistemi ve çalışma süresince eklenebilecek başka projelere) diğer sistemlerden hastane sistemine elektronik olarak aktarılması, sisteme veri aktarabilecek cihazların sistemle entegrasyonu, hastane içi iş akış süreçlerinin iyileştirilmesi, kaynak tasarrufu sağlanması gibi beklentilere de cevap verir.

• Barkot okuyucuların, etiket ve kart basma makinelerinin kurulması ve işletilmesi, HBS ile bütünleşmiş ve çalışır hale getirilmesi,

• Sıra yönetimi Merkezi Hastane Randevu Sistemi (MHRS), Tele-Tıp/Tele-Sağlık, vb. (telefon ve internet, v.b) HBYS ile entegre edilmesi, Hastane web sitesi, Sağlık- Net, Performans Takip Sistemi vb. veri aktarılması,

• Hastane idaresi tarafından belirlenen personele ve çalışanlara HBYS ile ilgili işlerini eksiksiz yapması için teorik ve pratik (uygulamalı) eğitim verilmesi, Yetkilendirilen yönetim ve birim şeflerinin bilgiye

erişimlerinin sağlanması, HBYS'in güvenlikli bir şekilde, hasta ve kişisel bilgilerin gizliliği esasına uygun olarak yürütülmesi, Hastane Otomasyon Hizmetleri Sözleşmesinin Kapsamı içindedir. İlgili sorunlar için aylık istatistiksel çalışma yapılması, kayıt tutulması ve muhafaza edilmesi.

6.19.4. Bilgi Güvenliği Politikası:

Bilgi Güvenliği Politikası yardımcı dokümanlarda ayrıca belirtilmiştir.

6.19.5. Hastane Otomasyon Sistemini Oluşturan Modüller ve Yetkili Kullanıcılar:

Modül Adı	**Yazılım**	**Kullanıcılar**
Ayaktan hasta Kabul	HBYS	Hasta kabul işlemleri
Yatan Hasta Kabul	HBYS	Servisler
Vezne	HBYS	Vezne
Poliklinik	HBYS	Poliklinikler
Cihaz Takip(Lab)	HBYS	Teknik Birimler
Laboratuar	HBYS	Laboratuar
Eczane	HBYS	Eczane
Radyoloji	HBYS	Radyoloji Birimleri
Doğum ve ameliyathane	HBYS	Ameliyathane
Faturalama	HBYS	Fatura ve tig
İstatistik	HBYS	İstatistik

• Hastane otomasyon sisteminde veri girişleri yukarıda belirtilen modüllere belirtilen yetkiler çerçevesinde, hastanemiz tıbbi sekreterleri, hemşireler, hastane memurları ve veri hazırlama elemanları tarafından yapılır.

6.19.6. Arızaların Bildirimi ve Giderilmesi:

• Sisteme veri girişi ile ilgili kullanıcı hataları ve donanım arızaları arızanın çeşidine göre arıza bildirim ekranı aracılığı ile bölüm sekreteri tarafından bildirilir ve bilgi işlem tarafından en kısa sürede düzeltilir.

Arızanın bildirilmesi ve takibi bölüm sekreterinin sorumluluğundadır.

6.17.7 Şifre güvenliği ve Şifre tanımı:

- Büyük/Küçük harf
- Sayılar
- Özel karakterler
- Noktalama işaretlerinden en az 2 sinin bulunması gerektedir.
- Şifre en az 8 karekterden oluşmalı ve üstteki maddeleri içermelidir.

Parola güvenliğine ait detaylı açıklamalar "Parola Yönetim Politikası" içerisinde yer almaktadır.

7. Genel Kullanım :

7.1 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.

7.2 Ağ güvenliğini (Örneğin; bir kişinin yetkili olmadığı halde sunuculara erişmek istemesi) veya ağ trafiğini bozacak eylemlere girişmemelidir.

7.3 Port veya ağ taraması yapılmamalıdır.

7.4 Ağ güvenliğini tehdit edici faaliyetlerde bulunulmamalıdır. Dos saldırısı, Port-network taraması vb. yapılmamalıdır.

7.5 Kurum bilgileri kurum dışında üçüncü kişilere iletilmemelidir.

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

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

7.8 Bilgisayarlarda oyun ve eğlence amaçlı programlar çalıştırılmamalı/kopyalanmamalıdır.

7.9 Bilgisayar üzerinde bir problem oluştuğunda, yetkisiz kişiler tarafından müdahale edilmemeli, ivedilikle bilgi işlem birimine haber verilmelidir. Kuralların uygulanmasından birim amirleri sorumlu olup, şahısların yapmış olduğu kural ihlallerinde ilgili sistem kullanıcısından başlamak üzere silsile yolu ile sorumludurlar.

8. Bilgi İsteme Hakkını Kullanması:

Hastalarımızın, kendileri yada yasal varisleri kanalı ile tanı ve tedavinin tüm süreçlerine ve hastalığın olası gidişatına ilişkin tam ve yeni bilgi alma, kuruluşumuzun kendilerine ilişkin tıbbi dokümantasyonun bir kopyasını alma hakkı vardır.

9. İLGİLİ DÖKÜMANLAR:

• Hasta Hakları Yönetmeliği (Resmi Gazete: Tarih: 01.08.1998; Sayı: 23420)

• Yataklı Tedavi Kurumları İşletme Yönetmeliği

• 06/11/2001 tarih ve 10588 sayılı Makam Oluru ile yürürlüğe giren Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arşiv Hizmetleri Yönergesi (Yataklı Tedavi Kurumları Tıbbi Kayıt ve Arşiv Hizmetleri Yönergesinde Değişiklik Yapılmasına Dair Yönerge:24/09/2004 tarih ve 7067 sayılı Makam Onayı)

• Sağlık Bakanlığı Bilgi İşlem Dairesi Başkanlığı'nın 2005/153 sayılı Genelgesi (17/09/2007 tarih ve 1249 sayılı Veri Güvenliği konulu yazısı).

- Bilgi Saklama ve Ortamları Yok Etme Prosedürü
- Veri Tabanı İzKayıtları Yönetim Talimatı
- Yedekleme Talimatı
- Parola Yönetim Politikası
- HBYS Yetki Talep Formu
- Erişim Kontrol Prosedürü
- Kişisel Verilerin Korunması Kanunu
- Bilgi Güvenliği Politikası
- Bilgi Yönetimi Hastane Politikası