1. AMAÇ

Hasta ya da çalışanlara ait tıbbi ve kişisel bilgilerin, doğru ve güvenli şekilde kayıt altına alınması ve depolanması ile ihtiyaç duyulan doğru bilginin, bilgi mahremiyeti ve güvenliği gözetilerek, doğru zamanda, doğru kişiye ulaştırılması amaçlanmıştır.

2. KAPSAM

İl Ambulans Servisi Başhekimliğine bağlı tüm birimleri kapsamaktadır.

3. KISALTMALAR

ASOS: Acil Sağlık Hizmetleri Otomasyon Sistemi
ASH: Acil Sağlık Hizmetleri
ASHİ: Acil Sağlık Hizmetleri İstasyonu
KKM: Komuta Kontrol Merkezi
BYS: Bilgi Yönetim Sistemi
AÇM: Acil Çağrı Merkezi

4. TANIMLAR

5. SORUMLULAR

İl Ambulans Servisi Başhekimliği tüm birim çalışanları, KKM çalışanları, ASHİ çalışanları, Birim Sorumluları, Başhekim Yardımcısı, Başhekim, ASH Başkan Yardımcısı ve ASH Başkanı sorumludur.

6. FAALİYET AKIŞI

6.1. BYS süreçlerine ilişkin politika belirlenir.

6.1.1. BYS politikasına ilişkin yönetim süreçleri, bilgi güvenliği, BYS' ye ilişkin geri bildirimlerin değerlendirilmesi, BYS' de muhtemel sorunlar ve çözüm süreçlerine ilişkin düzenleme Sağlık Bakanlığı ve İçişleri Bakanlığı tarafından yapılır.

6.2. Bilgi yönetimine ilişkin süreçlerin güvenli bir şekilde yürütülmesi ve koordinasyonu sağlanır.

6.2.1. Bilgi yönetimine ilişkin sorumlular Başhekimlik tarafından belirlenir. Bilgi İşlem Haberleşme ve Teknik İşler Birim çalışanlarının BYS yetkileri düzenlenir ve yazılım üzerinde kayıt altına alınır.

6.2.2. Bilgi İşlem Haberleşme ve Teknik İşler Birimi 24 saat boyunca hizmet verir. Nöbet başlangıç sabah saat 09.00 olup nöbet değişim saatinden önce en az iki birim çalışanı hazır bulunur. Nöbeti devralırken, bir önceki nöbetçiden nöbetle ilgili bilgiler alınır.

6.2.3. Bilgi İşlem Haberleşme ve Teknik İşler Birimi tarafından, İl Ambulans Servisi Başhekimliği ve bağlı tüm birimlerdeki bilişim sistemlerinin donanımsal- yazılımsal kurulumu ve çalışırlığı sağlanır. Bu amaçla gerektiği durumlarda ilgili birim, kurum ve kuruluşlar ile irtibata geçilir.

6.2.4. BYS ilişkin rol ve yetki grupları tanımlanır.

6.2.4.1. ASOS üzerinde yazılımı kullanan tüm personellerin yetkilendirilmesi yapılır. Bu gruplardaki personeller yalnızca kendilerine verilen yetki kadar işlem yapabilir.
Bu rol grupları;

- Birim
- Depo
- Demirbaş
- KKM
- Kalite
- Tahakkuk
- İstasyon
- İstatistik
- MKYS
- Personel

- Eğitim
- Hasta Nakil
- Hava Vaka
- Hastane Koordinasyon
- Teknik Takip
- Duyuru, Anket

6.2.5. İşe yeni başlayan personelin yazılım sistemlerine kullanıcı kaydı yapılır, kullanıcı adı ve şifresi verilir, kullanıcı yetkilendirme işlemleri Yetki Verme ve İptal Etme Prosedürü' ne (BY. PR.02) uygun şekilde yapılır.

6.2.6. Çalışanlar yetki düzeyleri ile ilgili olarak bilgilendirilir ve yetki düzeyi yazılım sistemleri üzerinde kayıt altına alınır. Aynı görevi icra eden çalışanlar aynı yetki grubuna dâhil olur.

6.2.7. Her kullanıcının BYS uygulamalarında hangi bilgilere erişebileceği tanımlanır. Kullanıcıların yetki düzeylerinde yapılan değişiklikler güncellenir ve takip edilir.

6.2.8. KKM' de işe başlayan personelin BYS kullanıcı eğitimleri sağlanır. Kurumdan ayrılan personelin BYS' den ayrılışı yapılır.

6.3. BYS' ye ilişkin riskler aşağıdaki şekilde yönetilir.

6.3.1. ASOS için yazılım ve donanım ile ilgili riskler sunucu ve yazılım lisansı Sağlık Bakanlığında olduğu için ilgili risk analizi Sağlık Bakanlığı tarafından yapılır.

6.3.2. ASELSAN için yazılım ve donanım ile ilgili riskler; sunucu ve yazılım lisansı İçişleri Bakanlığında olduğu için ilgili risk analizi İçişleri Bakanlığı tarafından yapılır.

6.3.3. İşe başlayışlarda hizmet içi eğitim olarak BYS' nin kullanımına yönelik Bilişim Sistemleri Kullanımı ve Bilgi Güvenliği Eğitimi verilir. Güncellemeler hakkında tüm çalışanlar bilgilendirilir.

6.4. BYS' ye ilişkin hata bildirimine yönelik düzenleme yapılır.

6.4.1. Muhtemel hatalarda çalışanlar AÇM, üzerinden telefon ile veya ASOS üzerinden Bilgi İşlem Haberleşme ve Teknik İşler Birimine mesaj göndererek ulaşırlar.

6.4.2. Birime ulaşan hataların çözülmesi için;

- ✓ ASOS için yardım masası yolu ile ASH Genel Müdürlüğüne anlık bildirim gönderilir.
- ✓ ASELSAN için AÇM' nin Bilgi İşlem Haberleşme ve Teknik İşler Birimine mail veya resmi yazı ile bildirilir.

6.4.3. Süreçte karşılaşılan ASOS ve ASELSAN hataları KKM tarafından Sağlıkta Bilgi Yönetim Sistemleri Günlük Arıza Tespit Listesi (BY.LS.04) ile kayıt altına alınır. Haftalık Kayıtlar Bilgi İşlem Haberleşme ve Teknik İşler Birimine EBYS üzerinden gönderilir. Bilgi İşlem Haberleşme ve Teknik İşler Biriminde dijital ortamda saklanır.

6.5. Bilgi güvenliği ve mahremiyetini sağlamaya yönelik gerekli tedbirler alınır.

6.5.1. Kullanılan yazılımlara kişisel şifre ile giriş sağlanır ve gerekli yetki tanımlamaları yapılır. Farkındalık eğitimleri verilir.

6.5.2. Şifre kullanımına yönelik kurallar kullanılan yazılımlar tarafından belirlenir.

6.5.3. BYS kullanıcılarına gizlilik sözleşmeleri tebliğ edilir.

6.6. BYS üzerinde yapılan işlemlerin izlenebilirliği; kullanılan yazılımlarda kullanıcı log kayıtları yazılımın kendisi tarafından tutulmaktadır.

6.7. BYS üzerinde verilerin yedeklenmesi yazılımları barındıran Sağlık Bakanlığı ve İçişleri Bakanlığı tarafından yapılır.

6.8. ASH kapsamında kullanılan bilgisayarlara yönelik düzenleme aşağıdaki şekilde yapılır.

6.8.1. Birimler tarafından kullanılan bilgisayarlar İl Sağlık Müdürlüğü Sağlık Bilgi Sistemleri etki alanına dâhil edilir. KKM' nin kullandığı bilgisayarlar AÇM' ye dâhil edilir ve çalışırlığı sağlanır. İl Sağlık Müdürlüğü Sağlık Bilgi Sistemleri Birimi adına etki alanı (Domain) sistem yöneticisi görev ve sorumlulukları yerine getirilir.

6.8.2. Lisanslı programlar kullanılır.

6.8.3. Bilgisayar Envanter Listesi (BY.LS.03) oluşturulmuş olup, Teknik Destek ve Ambulans Lojistik Birim çalışanı tarafından tutulur.

6.8.4. Anti virüs tüm bilgisayarlarımızda mevcuttur.

6.8.5. Kablosuz ağ bağlantıları için farklı olan (sanal yerel ağ) oluşturulur.

6.9. BYS' nin etkinliği ve sürekliliği için gerekli destek alt yapıları Sağlık Bakanlığı ve İçişleri Bakanlığı tarafından sağlanır.

6.9.1. Bilgi İşlem Haberleşme ve Teknik İşler Birimi KKM' de bulunan bilgisayar donanımının bakımının yapılmasını sağlar.

6.9.2. Birimlerden gelen yazılım, internet ve donanım arıza ve talepleri tutanakla kayıt altına alınarak, Sağlık Bakanlığı ve İçişleri Bakanlığına bildiri sağlanır.

6.9.3. Sistemde tespit edilen aksaklıklara yönelik gerekli iyileştirme çalışmaları için Sağlık Bakanlığı ve İçişleri Bakanlığı ile iletişime geçilerek yazışmaları yapılır.

6.10. Sunucu odalarının güvenliği aşağıdaki şekilde sağlanır.

6.10.1. Sadece sunuculara tahsis edilmiş bağımsız bir oda olmalıdır.

6.10.2. Yetkisiz personelin girişinin engellenmesi için odalar şifreli olup sunucu odalarına Bilgi İşlem Haberleşme ve Teknik İşler Birim personeli dışında başka personelin girmesi engellenmiştir. Birim personeli her giriş çıkışında Sistem Odası Giriş Çıkış Takip Listesini (BY.LS.02) doldurur.

6.10.3. Sadece sunuculara tahsis edilmiş bağımsız bir oda olmalıdır.

6.10.4. Sunucu odaları suya karşı yalıtıma sahip olup yerden yüksektedir.

6.10.5. Sunucu odalarında kesintisiz güç kaynaklarından bağımsız güç kaynakları bulunur.

6.10.6. Bilgi İşlem Haberleşme ve Teknik İşler Birim personeli tarafından gün içinde 6 saat aralıklarla sıcaklık ve nem takibi yapılır, Sıcaklık Nem Kontrol Listesi (RY.LS.02) ve Sistem Odası Giriş Çıkış Takip Listesi (BY.LS.02) doldurur.

6.10.7. İdeal sıcaklık oranı; 15- 25 °C aralığında, nem oranı; %50 ve altındadır.

6.10.8. Sunucu adalarında yedekli olarak çalışan klima bulunur.

6.11. Sunucunun güvenliğini sağlamaya yönelik tedbirler alınmalıdır.

6.11.1. Bilgi İşlem Haberleşme ve Teknik İşler Birimi tarafından sunucular üzerinde işlem yapıldığında Sunucu Kayıtları Envanter Listesi (BY. LS.01) doldurulur.

6.11.2. Sunucu üzerinde çalışan işletim sistemleri, hizmet sunucu yazılımları ve anti virüs gibi koruma amaçlı yazılımların güncelliği otomatik olarak sağlanır gerekli durumlarda manuel olarak da güncellenmektedir.

6.11.3. Sunucuların yazılım ve donanım bakımları üretici firmanın uygun gördüğü süreler dâhilinde yetkili kişiler tarafından yapılır.

6.11.4. Sunucular güvenlik duvarının arkasında bulunur.

6.12. Veri tabanı güvenliğini sağlamaya yönelik tedbirler Sağlık Bakanlığı ve İçişleri Bakanlığı tarafından alınır.

6.13. Dış ortamdan iç ortama erişimlerde güvenlik tedbirleri, kullanılan yazılımların sunucu ve veri tabanları Valilik ve Sağlık Bakanlığında olduğu için erişim ihtiyacı bulunmamaktadır.

7. İLGİLİ DOKÜMANLAR

7.1.1. Sağlıkta Bilgi Yönetim Sistemleri Günlük Arıza Tespit Listesi (BY.LS.04)
7.1.2. Sistem Odası Giriş Çıkış Takip Listesi (BY.LS.02)
7.1.3. Sıcaklık Nem Kontrol Listesi (RY.LS.02)
7.1.4. Yetki Verme ve İptal Etme Prosedürü (BY.PR.02)
7.1.5. Sunucu Kayıtları Envanter Listesi (BY. LS.01)
7.1.6. Bilgisayar Envanter Listesi (BY.LS.03)

HAZIRLAYAN	KONTROL EDEN	ONAYLAYAN	ONAYLAYAN
Bilgi İşlem Haberleşme ve Teknik İşler Birim Sorumlusu	Kalite Yönetim Direktörü	Başhekim Yardımcısı	Başhekim