BİLGİ GÜVENLİĞİ İLE İLGİLİ KRİTERLERİN DEĞERLENDİRME ESASLARI

1. Yılda En Az Bir Kez Bilgi Güvenliği Eğitimi Alan Personel Oranı

Bilgi güvenliğinin bilgi sistem güvenliğinden daha geniş bir kavram olması; personel güvenliği, evrak güvenliği, fiziki güvenlik gibi konuları da içermesi nedeniyle eğitimin sadece bilgisayar kullanan kişilere değil, kurum tarafından işlenen bilgiler ile bu bilgilerin işlendiği sistem ve tesislere erişen tüm personele verilmesi gerekmektedir.

Sağlık tesislerinde işlenen verilerin ağırlıklı olarak kişisel veriler ve kişisel verilerin daha da özel koruma gerektiren bir parçasını oluşturan kişisel sağlık verisi olması nedeniyle, bu verilere erişim ihtimali olan tüm personelin eğitim planlamasına alınması uygun olacaktır. Eğitim içeriği hazırlanırken bilgi sistem güvenliği ile ilgili konulara ilave olarak başta kişisel veriler ve sağlık verilerinin korunması olmak üzere diğer konuların da mutlaka dikkate alınması önem arz etmektedir.

Eğitimin içeriği hazırlanırken Sağlık Bakanlığı Bilgi Güvenliği Politikaları Yönergesinde yer alan ana esaslar ve Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzunda yer alan ve son kullanıcıları doğrudan ilgilendiren başlıkların (**kurum bilgi güvenliği organizasyonu, insan kaynakları güvenliği kapsamında işe başlama, görev değişikliği ve işten ayrılma süreçlerinde dikkat edilmesi gereken hususlar, bilgi güvenliği farkındalık bildirgesi içeriği, e-posta güvenliği, parola kullanımı, sosyal medya ve sosyal mühendislik, oltalama e-postalarından korunma, kişisel verileri koruma kanunu kapsamında çalışanların sorumlulukları, ihtiyaç olduğunda bilgisayarlardaki verilerin güvenli olarak silinmesi ve güvenli imha işlemleri, taşınabilir medya kullanımı, kurum bilgisayarlarının iş dışında kullanımı prensipleri, kurum dışı ağlar/kablosuz ağlar kullanılırken dikkat edilecek hususlar, bilgi güvenliği ihlal bildirimlerinin ne şekilde yapılacağı, fiziki güvenlik kapsamında dikkat edilecek hususlar, kurum bilgi kaynaklarına uzaktan erişim, lisanslı yazılım kullanımı vb.**) dikkate alınması gerekmektedir.

Farkındalık eğitimleri yüz yüze veya uzaktan eğitim şeklinde yapılabilecektir. Eğitimlerin ideal şartlarda yüz yüze eğitim şeklinde yapılması tercih edilmekle beraber, pandemi koşulları dikkate alınarak uzaktan eğitim şeklinde verilmesinde de bir mahzur bulunmamaktadır.

SYPD Yönergesinde bu gösterge için veri toplama ve analiz periyodu bir yıl olarak belirlenmiştir. Bu kapsamda tüm kurumlarımız tarafından bünyelerinde çalışan tüm personel dikkate alınarak bilgi güvenliği farkındalık eğitimleri verilecek ve eğitim yapıldığına dair bilgiler ÇKYS/İKYS/Eğitim modülü vasıtasıyla elektronik ortama işlenecektir.

Eğitim kayıtları **"ÇKYS/İKYS→Eğitim Ana Menüsü→Personel Hizmet İçi Eğitim Bilgileri→Sağlık Tesisleri Eğitimleri (71) → Bilgi Güvenliği (9) →Çalışan ve Hasta Bilgi Güvenliği"** menüsü kullanılarak sisteme girilecektir.

Bu gösterge için hesaplama yapılırken;

o İlgili kartların Yönetim Hizmetleri Genel Müdürlüğü / Yönetim Hizmetleri Dairesi Başkanlığının web sayfasında (https://yhgm.saglik.gov.tr/TR-34890/yonetim-izleme-ve-degerlendirme-dairesi-baskanligi.html) yayımlanan en son sürümlerinde yazan kriterler dikkate alınacaktır.

o Hesaplama yapılırken 31 Aralık 2022 tarihi itibarı ile ilgili kurumun "**aktif**" personel mevcudu ve bu personelin 01 Ocak 2022-31 Aralık 2022 tarihleri arasında eğitim alıp almadığına bakılacaktır. Eğitimin hangi kurum tarafından verildiği önemli değildir. Personelin herhangi bir kurumdan bir kez eğitim alması yeterli olacaktır.

o Aktif personel sayısı hesaplanırken o kuruma geçici görevle gelenler kurumun personel mevcuduna eklenecek; geçici görevle başka kuruma gönderilenler, açıkta olanlar, tutuklu veya hükümlü olanlar, askerde olanlar, doğum izninde olanlar, muvafakat ile başka kuruma görevlendirilenler, ücretsiz izinde olanlar aktif personel hesabına dâhil edilmeyecektir.

o Hesaplamaların doğru sonuçlar vermesi için ilgili kurumların personel ayrılış ve katılış işlemlerinin doğru ve zamanında ÇKYS'ye girilmiş olması büyük önem arz etmektedir. İtiraz

safhasında, hesaplamanın kurumların personel kayıtlarındaki eksik ve hatalardan kaynaklandığının tespit edilmesi halinde, yapılacak müracaatlar kabul edilmeyecektir.

o Yıl içerisinde atama gören personel, eski kurumunda bilgi güvenliği eğitimi almış ve alınan bu eğitim ÇKYS/İKYS/Eğitim modülüne işlenmiş ise, personele yeni kurumunda ayrıca eğitim verilmesine gerek bulunmamaktadır.

o Eğitimlerin Bakanlığımız Uzaktan Sağlık Eğitim Sistemi (USES) veya kurumların kendi bünyelerinde mevcut uzaktan eğitim sistemleri üzerinden verilmesi halinde, ÇKYS/İKYS ile bahse konu sistemler arasında doğrudan bir entegrasyon olmadığı dikkate alınarak, eğitim girişlerinin yukarıda belirtildiği şekilde ÇKYS/İKYS'ye ayrıca girilmesi gerektiği dikkate alınacaktır.

2. İl Genelindeki Tüm Kurumların Bilgi Güvenliği Politikalarına Uyum Oranı

Göstergede yer alan "**İl Genelindeki Kurumlar**" ifadesi 2022 yılı için "**E1 kategorisindeki ilçe devlet hastaneleri de dâhil tüm 2 ve 3'ncü basamak kamu hastaneleri**" olarak uygulanacaktır.

1'nci basamak sağlık tesisleri ve E2/E3 kategorisindeki entegre ilçe devlet hastaneleri bu başlık kapsamında yer almamaktadır.

Bilgi güvenliği politikaları ile uyum kapsamında İl Sağlık Müdürlüğünün kendisi ve ilgili kamu hastanelerince, Ek-1'de yer alan başlıklarda açıklanan konuları gerçekleştirmeleri ve bunun delili olarak yine Ek-1'de belirtilen çıktıların üretilmesi ve sunulması beklenmektedir.

Kurumların SYPD işlemleri açısından bu göstergeden "başarılı/uyumlu" sayılabilmeleri için başlıklar için belirlenen puanlar dikkate alınarak toplamda (100 tam puan üzerinden) en az 80 puana ulaşmaları gerekmektedir.

Her bir başlık için değerlendirme yapılırken, ilgili başlık için belirlenen işlemlerin tümünün yapılması gerekmekte olup bir başlık için istenen bilgi ve belgelerden birinin bile eksik olması halinde, ilgili kuruma söz konusu başlıktan "0 (sıfır)" puan verilecektir. Bir başka ifade ile başlıklara "0" ya da "tam" puan verilecektir.

Kapsam dâhilinde yer alan tüm kurumlarca, Ek-1'de belirtilen başlıklar ile ilgili çalışma yapılacak, yapılan çalışmaların sonuçları (İSM'ler tarafından belirlenecek bir tarihe kadar) İSM'ye gönderilecektir.

Bu gösterge için illerin genel başarı durumları hesaplanırken, illerin kategorileri (İ1-İ7) ve hastane sayıları dikkate alınarak SBSGM tarafından belirlenecek sayıda kurumun belgeleri üzerinden değerlendirme yapılacak, hesaplanan oran il geneline yansıtılacaktır.

Örneklemde yer alacak kurumlar (İSM'lerin kendisi mutlaka örneklem içinde yer alacak şekilde) SBSGM tarafından seçilecek ve **27 Aralık 2022 tarihinde** https://bilgiguvenligi.saglik.gov.tr/Home/BGPerformansDegerlendirmesi adresinde yayımlanacak ayrıca Bakanlığımız e-posta sistemi üzerinden İSM'lerde görev yapan bilgi sistemleri koordinatörleri ve bilgi güvenliği yetkilisi/yedeklerine gönderilecektir.

İSM'lerin kendisine ve örnekleme dâhil edilen hastanelerine ait bilgi ve belgeler en geç **30 Aralık 2022 mesai bitimine kadar** tarihine kadar elektronik ortamda SBSGM'ye gönderilmiş olacaktır.

İSM'nin kendisi ve örneklemde yer alan kurumların evrakları, Genel Müdürlük BGYS ve SOME ekipleri tarafından incelenecek ve yukarıda belirtilen esaslar doğrultusunda puanlama yapılacaktır. Bu safhada gerekiyorsa ilgili kurumlarda çalışan personel ile birebir temas kurularak ilave bilgi ve belge istenebilecektir.

Hastaneler tarafından İSM'lere gönderilen kayıtlar, ihtiyaç olması durumunda örnekleme usulü ile yapılacak denetimlerde kullanılmak üzere, bir sonraki yılın Temmuz ayına kadar İSM tarafından saklanacaktır.

3. Ek-1 Başlıkların Sağlık Bakanlığı Birinci Basamak Sağlık Kuruluşları Ek Ödeme Yönetmeliği Uyarınca Yapılacak Ek Ödemeler İçin Kullanılma Esasları

Ek-1'de sıralanan başlıklardan İSM'ler ile ilgili olanlar, Sağlık Bakanlığı Birinci Basamak Sağlık Kuruluşları Ek Ödeme Yönetmeliği uyarınca İSM'lerde çalışan personele yapılacak ek ödemelere esas olmak üzere İSM Birim Performans Kriteri olarak kullanılacaktır.

Ek-1'deki başlıkların İSM Birim Performans Kriterleri açısından puanları aşağıdaki tabloda olduğu gibidir. İSM'ler için hesaplanan puanlar 2023 yılı şubat ayı içerisinde Yönetim Hizmetleri Genel Müdürlüğüne (Mali Hizmetler Daire Başkanlığı) gönderilecek ve alınan puan personelin 2023 yılı ek ödeme hesaplamasına esas olacaktır. Puanlama yapılırken SYPD hesaplamasında olduğu şekilde bir baraj olmayacak, İSM için toplam kaç puan hesaplanır ise hesaplanan puan üzerinden işlem yapılacaktır.

Bilgi güvenliği başlıkları için belirlenen 350 puan, İSM Birim Performans Kriterlerinin tamamı için belirlenen toplam performans puanının (20.000 puan) % 1.75'ini oluşturmaktadır.

S.No.	Değerlendirme Yapılacak Başlık	Puan
1	Tedarikçi ilişkilerinde bilgi güvenliği işlemleri	**55**
2	İl Sağlık Müdürlüğüne doğrudan bağlı birimlerde çalışan personele bilgi güvenliği farkındalık eğitimi verilmesi	**50**
3	İhlal bildirimlerine süresi içerisinde işlem yapılması	**35**
4	Bilgi güvenliği risk yönetimi işlemleri	**35**
5	Bilgisayarların merkezi olarak yönetim ve denetimi işlemleri	**70**
6	İşletim sistemi güncelleme işlemleri	**35**
7	Zararlı yazılımlardan korunma işlemleri	**35**
8	IP dağıtımı işlemleri	**35**
Toplam		**350**