BGYS ve KVYS Politikası Hakkında Bilgilendirme Metni

1. Amaç ve kapsam

İşbu "BGYS ve KVYS Politikası Hakkında Bilgilendirme Metni"nin amacı; HEALTHİS ASSISTANCE SAĞLIK HİZMETLERİ ANONİM ŞİRKETİ ("Şirket") tarafından yürütülen sağlık turizmi faaliyetleri kapsamında kullanılan dijital kanallar (internet sitesi, başvuru formları, iletişim kanalları, çağrı merkezi süreçleri ve Şirketin bilgi işlem altyapısı dâhil) yönünden **bilgi güvenliği** ve **kişisel verilerin korunmasına ilişkin yönetim yaklaşımımız** hakkında genel bilgilendirme yapmaktır.

Bu metin:

- Şirketin bilgi varlıklarının gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamaya dönük BGYS yaklaşımını,
- Kişisel verilerin (özellikle sağlık verilerinin) hukuka uygun işlenmesi, erişimlerin sınırlandırılması ve veri güvenliğinin sağlanmasına ilişkin KVYS yaklaşımını,
- Sağlık turizmi mevzuatı kapsamında yürütülen kayıt, arşivleme ve yetkili kurumlara bildirim/aktarım süreçlerine ilişkin temel prensipleri

genel hatlarıyla açıklar.

Önemle belirtmek gerekir ki; bu metin **KVKK kapsamındaki Aydınlatma Metni** veya açık rıza metinlerinin yerine geçmez. Kişisel verilerin işlenme amaçları, hukuki sebepler, alıcı grupları, saklama süreleri ve KVKK kapsamındaki haklarınıza ilişkin ayrıntılar için lütfen **Kişisel Verilerin Korunması ve İşlenmesi Aydınlatma Metni**'ni inceleyiniz.

2. Tanımlar (kısa açıklamalar)

- BGYS (Bilgi Güvenliği Yönetim Sistemi): Şirketin tüm bilgi varlıklarını (hasta/başvuru sahibi bilgileri, operasyonel kayıtlar, sözleşmeler, finansal veriler, sistem logları vb.) korumak amacıyla uyguladığı politika, prosedür, risk yönetimi ve kontrol bütünüdür.
- KVYS (Kişisel Veri Yönetim Sistemi): Kişisel verilerin işlenmesinin hukuka uygun yürütülmesi; verilerin sınıflandırılması, erişim yetkileri, saklama-imha, üçüncü taraf yönetimi, ihlal yönetimi, denetim ve eğitim faaliyetleri gibi süreçleri kapsayan mahremiyet ve veri koruma yönetim yaklaşımıdır.
- Kişisel sağlık verisi: Sağlık bilgileri, tıbbi değerlendirmeler, raporlar, tetkik bilgileri, geçmiş hastalık/ameliyat bilgileri gibi veriler olup KVKK kapsamında "özel nitelikli kişisel veri" niteliğindedir.

3. Hukuki uyum prensibimiz (KVKK ve sağlık turizmi mevzuatı ile uyum)

Şirket, kişisel verileri işlerken **6698 sayılı Kişisel Verilerin Korunması Kanunu** başta olmak üzere ilgili mevzuata uyumlu hareket etmeyi hedefler. Özellikle sağlık verileri, KVKK'da özel nitelikli kişisel veri olarak düzenlenmiş olup Şirket bu verileri işlerken daha yüksek güvenlik standartları ve erişim kontrolleri uygular.

Sağlık turizmi kapsamındaki hizmet süreçlerinde; mevzuatta öngörülen durumlarda **kayıt, arşivleme, Bakanlık sistemlerine bildirim/aktarım** yükümlülükleri bulunabilir. Şirket, bu süreçleri yerine getirirken verilerin güvenliğini sağlamak ve yalnızca gerekli kişilerce erişilebilir olmasını temin etmek için teknik ve idari tedbirler uygular.

4. BGYS yaklaşımımız (bilgi güvenliğinin yönetimi)

Şirket, bilgi güvenliğini yalnızca bir "teknoloji" konusu olarak değil, tüm iş süreçlerini kapsayan bir **risk yönetimi** alanı olarak ele alır. Bu kapsamda BGYS yaklaşımımızın ana unsurları aşağıdaki gibidir:

1. Risk temelli güvenlik yönetimi: Bilgi varlıkları (uygulamalar, sunucular, veri tabanları, ağ bileşenleri, uç cihazlar, kullanıcı hesapları vb.) envanterlenir; tehdit ve zafiyetler değerlendirilerek uygun kontroller belirlenir.

2. Erişim yönetimi ve yetkilendirme: Şirket sistemlerine erişimler "ihtiyaç kadar yetki" prensibiyle sınırlandırılır. Yetkilerin verilmesi, değiştirilmesi ve kaldırılması kontrollü yürütülür.

3. Kimlik doğrulama ve kayıt (log) yönetimi: Kritik sistemlerde kimlik doğrulama yöntemleri ve erişim kayıtları (loglar) ile şüpheli hareketlerin izlenmesi hedeflenir.

4. Ağ ve sistem güvenliği: Güvenlik duvarı, güncel yamalar, zararlı yazılım önleme, ağ segmentasyonu, güvenli uzaktan erişim ve benzeri önlemlerle sistem güvenliği güçlendirilir.

5. Yedekleme ve süreklilik: Verilerin bütünlüğü ve erişilebilirliği için düzenli yedekleme, yedeklerin güvenli ortamda saklanması ve iş sürekliliği önlemleri uygulanır.

6. Olay yönetimi: Güvenlik olaylarının tespiti, sınıflandırılması, müdahalesi ve iyileştirme adımları için işleyen bir süreç oluşturulması hedeflenir.

7. Tedarikçi ve üçüncü taraf güvenliği: Hizmet alınan tedarikçilerin (barındırma, yazılım, çağrı merkezi, danışmanlık vb.) bilgi güvenliği sorumlulukları sözleşmesel ve operasyonel olarak yönetilir.

Şirket, BGYS süreçlerini sürekli iyileştirme anlayışıyla gözden geçirir; eğitim, denetim ve kontrol faaliyetleriyle güvenlik farkındalığını canlı tutmayı amaçlar.

5. KVYS yaklaşımımız (kişisel verilerin korunması ve mahremiyet)

Şirket, kişisel verilerin korunmasını ve mahremiyeti temel bir ilke olarak benimser. KVYS yaklaşımımızın öne çıkan unsurları şunlardır:

1. Hukuka uygunluk ve şeffaflık: Kişisel verilerin işlenmesine ilişkin süreçlerin hukuki dayanaklarının belirlenmesi, ilgili kişilerin bilgilendirilmesi ve gerekli hâllerde açık rıza mekanizmalarının işletilmesi hedeflenir.

2. Veri minimizasyonu: Hizmetin sunulması veya başvuru süreçlerinin yürütülmesi için gerekli olmayan verilerin talep edilmemesi ve toplanmaması prensibi esas alınır.

3. Amaçla sınırlılık: Toplanan verilerin, belirlenen amaçlar dışında kullanılmamasını sağlamak için idari ve teknik kontroller uygulanır.

4. Özel nitelikli kişisel verilerin korunması: Sağlık verileri gibi özel nitelikli kişisel veriler için artırılmış erişim kontrolleri, sınırlı yetkilendirme, kayıt altına alma ve güvenlik tedbirleri uygulanır.

5. Saklama ve imha yönetimi: Kişisel verilerin saklanma süreleri mevzuat ve işleme amaçları doğrultusunda belirlenir; saklama süresi dolan veriler için silme, yok etme veya anonimleştirme süreçleri işletilmesi hedeflenir.

6. İhlal yönetimi: Kişisel verilerin hukuka aykırı şekilde ifşa edilmesi, erişilmesi veya ele geçirilmesi gibi olaylarda değerlendirme, gerekli bildirimlerin yapılması ve risk azaltıcı tedbirlerin alınması yönünde süreçler işletilir.

7. Eğitim ve farkındalık: Çalışanların ve ilgili ekiplerin sır saklama, mahremiyet ve veri güvenliği konularında düzenli bilgilendirilmesi ve farkındalığının artırılması hedeflenir.

6. Veri işleyenler / tedarikçiler ve sözleşmesel güvence

Şirket, kişisel verilerin kendi adına işlenmesi söz konusu olduğunda (örneğin; bilgi işlem hizmetleri, yazılım destek hizmetleri, barındırma hizmetleri vb.) ilgili üçüncü taraflarla olan ilişkilerini **KVKK'ya uyumlu sözleşmesel hükümler** ve güvenlik kontrolleri ile yönetmeyi amaçlar.

Bu kapsamda; tedarikçi erişimlerinin sınırlandırılması, gizlilik yükümlülükleri, alt yüklenici kısıtları, olay bildirim yükümlülükleri ve denetim hakları gibi mekanizmalar değerlendirilir.

7. İletişim kanalları ve kullanıcıların dikkat etmesi gereken hususlar

Şirket ile iletişime geçerken (web sitesi formu, e-posta, telefon, mesajlaşma uygulamaları vb.) paylaşılan bilgilerin mahiyeti önemlidir. Şirket, güvenli iletişim kanallarını tercih etmeyi ve özellikle tıbbi bilgi/rapor gibi hassas içeriklerin paylaşımında resmi yönlendirmelere uyulmasını önerir.

Kullanıcılar; kendilerine ait olmayan bir kişiye ilişkin bilgileri Şirkete iletmemeli, üçüncü kişilere ait rapor veya kimlik bilgilerini paylaşmadan önce gerekli yetkilendirmelere sahip olmalıdır.

8. Güncellemeler

Şirket, BGYS ve KVYS uygulamalarını; mevzuat değişiklikleri, teknolojik gelişmeler, risk değerlendirmeleri ve iş süreçlerindeki değişiklikler doğrultusunda güncelleyebilir. Bu bilgilendirme metni de gerektiğinde revize edilebilir ve güncel sürüm web sitesinde yayımlanır.

9. İletişim

Bu metin kapsamındaki bilgi güvenliği ve kişisel verilerin korunmasına ilişkin sorularınız için bizimle aşağıdaki kanallardan iletişime geçebilirsiniz:

• Unvan: HEALTHİS ASSISTANCE SAĞLIK HİZMETLERİ ANONİM ŞİRKETİ

• Adres: İzzet Paşa, Yeni Yol Cd. Nurol Tower No:3 İç Kapı No:32, 34381 Şişli/İstanbul

• E-posta: info@healthis.com.tr

• Telefon: (0212) 809 99 07