1. AMAÇ:

Bu prosedürün amacı, sağlık tesisimizdeki taşınabilir ortamda depolanan malzemelerde meydana gelebilecek kaybolma, kolayca çoğaltma vb. nedenlerden dolayı özellikle elektronik medya (CD/DVD, USB girişli hafif taşınabilir bellekler, taşınabilir diskler, hafıza kartları, teyp kartuşları vb.) ve basılı evraklar (yazılar, dosya klasörleri, etüdler, çizimler, krokiler, proje evrakları vb.) olmak üzere taşınabilir ortamlarda saklanan her türlü bilginin korunması ve yetkisiz kişilerin eline geçmemesi için özel önlemler alınmasını sağlamaktır.

2. KAPSAM:

Bu prosedür ..... Hastanesi bünyesinde taşınabilir medya ortamında her türlü bilgiyi saklayan tüm kişileri kapsamaktadır.

3. UYGULAMA

3.1. Elektronik medya kullanımı ile ilgili olarak aşağıdaki hususlar göz önünde bulundurulur:

3.1.1. Kuruma ait veriler, kişilere ait medyalar üzerinde saklanamaz. Verilerin bir taşınabilir ortama aktarılması ihtiyacı kaçınılmaz ise bu maksatla kuruma ait medyalar kullanılır.

3.1.2. Kuruma ait medyalar varlık envanteri içinde listelenir ve kimler tarafından kullanıldığı kayıt altına alınır. Görev devir teslimlerinde veya işten ayrılışlarda, kişilere teslim edilmiş olan medyaların iade edilmesi istenir veya ne şekilde sarf edildiği bilgisi sorgulanır.

3.1.3. Özellikle eski SBYS verileri ve SBYS yedeklerinin saklandığı medya ortamlarının mutlak surette envanter listesi oluşturulur, 6 (altı) aydan az olmayacak şekilde belirlenecek sürelerde sayım işlemleri yapılır ve sayım sonuçları kayıt altına alınır.

3.1.4. ÇOK GİZLİ, GİZLİ, ÖZEL ve HİZMETE ÖZEL veriler, taşınabilir ortamda saklanamaz. Özellikle bu tür ortamlarda saklama zorunluluğu var ise Sabit Ortamdaki Verilerin Şifrelenmesi standardına uygun şekilde şifreli olarak saklanır.

3.1.5. Bir bilgi sadece taşınabilir medya ortamında saklanıyorsa, bozulma/kaybolma gibi ihtimallere karşı bir başka medya ortamında da yedeklenmesi tavsiye edilir. Veriler çok kıymetli ise yedeklenen medya ortamı, doğal afet vb. tehditlere karşı önlem olmak üzere fiziksel olarak farklı bir yerde muhafaza edilir.

3.1.6. Yeni medya teknolojilerinin ortaya çıkması nedeniyle üç yıldan uzun süredir eski teknolojilerin kullanıldığı bir medya ortamında saklanan verilerin daha yeni bir medya ortamına taşınması tavsiye edilir.

3.1.7. Gizlilik derecesi taşıyan kurumsal verilerin saklandığı medya ortamları, kişisel (şahsın kendisine ait) bilgisayarlarda kullanılamaz. Bu tip veriler kişisel bilgisayarlarda işlenemez.

3.1.8. Tüm ortamlar üretici talimatında belirtildiği şekilde toz, nem vb. çevresel şartlardan etkilenmeyecek şekilde güvenli bir ortamda saklanır.

3.2. Taşınabilir ortamda yer alan verilerin bütünlüğünün sağlanması (değişmediğinin garanti altına alınması) için özetleme (hash) algoritması kullanılmak suretiyle verilerin bir özeti (parmak izi) alınır. Alınan özet, kullanılan algoritma ve anahtar ile birlikte bir tutanak ile kayıt altına alınır ve taşınabilir ortam ile birlikte muhafaza edilir. İhtiyaç duyulan durumlarda verinin tekrar özeti alınarak herhangi bir değişiklik olup olmadığı kontrol edilir.

3.3. Elektronik medya da dâhil tüm taşınabilir ortamlar, kullanılmadığı zamanlarda içinde bulunan verilerin gizlilik derecesi dikkate alınarak fiziki güvenlik tedbirleri alınmış kasa, dolap, çekmece gibi ortamlarda saklanır.

3.4. Taşınabilir ortamların bir yerden başka yere taşınması esnasında yetkisiz erişim, kötüye kullanım ve bozulmaya karşı gerekli önlemler alınır. Bu çerçevede;

3.4.1. Güvenilir kargo/taşıma şirketleri ya da kuryeler kullanılır,

3.4.2. Yönetim tarafından yetkili kurye listeleri oluşturulur.

3.4.3. Paketleme ve taşıma sırasında ortaya çıkabilecek herhangi bir fiziksel hasardan korumak için üreticinin belirlediği teknik özelliklere uygun önlemler (ısı, nem ya da elektromanyetik alanlara maruz kalma gibi çevresel faktörlere karşı koruma vb.) alınır.

3.4.4. Ortamın içeriğini tanımlayan kayıtlar ile birlikte kaç kez transfer edildiği, transfer sorumluları ve alıcı tarafından alındığının kayıtları tutulur.

4. YAPTIRIM

Bu politikanın ihlali durumunda, Bilgi Güvenliği Komisyonu ve ilgili yöneticinin onaylarıyla Bilgi Güvenliği komitesinde alınacak kararlarla işlem yapılır.