Elektronik sağlık kaydı ve mahremiyet

İlker Köse

1977 Nevşehir'de doğdu. İstanbul Ünversitesi Elektronik Mühendisliği'nden mezun oldu. Yüksek lisansını, Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği bölümünde 2003'te tamamladı. Halen aynı enstitüde doktora eğitimine devam etmektedir. 1999-2004 yılları arasında İstanbul Büyükşehir Belediyesi Ulaşım A.Ş.'de değişik görevlerde bulundu. 2003'ten itibaren Sağlık Bakanlığı'nın bilişim projelerinde danışman ve koordinatör olarak çalışmaktadır. Üzerinde çalıştığı projeler: Aile Hekimliği Bilgi Sistemi ve Ulusal Sağlık Bilgi Sistemi'dir.

Hayatı kolaylaştırma, verimliliği artırma ve mobil hizmet özellikleri sayesinde bilgisayar ve internetin hayatımıza oldukça hızlı bir şekilde girmiş olması, bireylerin ve toplumların bu ürünleri nasıl, nerede ve ne için kullanacağı konusunda doğru ve sağlıklı bir kültürün oluşmasını zorlaştırmıştır. Sağladıkları faydalar nedeniyle kullanıcılar tarafından sorgusuzca kabul gören bu ürünler, son günlerde yol açtıkları sorunlar nedeniyle önemli tartışmaların odağına yerleşmiş durumdadır. Bu sorunların başında ise, kişisel bilgilerin, özellikle de kişisel sağlık bilgilerinin mahremiyetinin ihlali yer alıyor.

Sağlık sektörü, bilişim konusunda hızlı bir yükseliş yaşamaktadır. Özellikle son 20 yılda, hastanelerde, sağlık ocaklarında, aile hekimlerinde, laboratuarlarda, görüntüleme merkezlerinde, kan ve doku bankalarında müstakil ya da birbiriyle entegre bilgi sistemleri kullanılıyor. Hatta bu bilgi sistemleri, sağlık hizmetinin verimini ve kalitesini artırmak için vazgeçilmez araçlar ola-

rak görülmeye başlandı. Bunun neticesi olarak daha önceleri ciddi bir sorun olarak görülmeyen veya en azından bir ihlal söz konusu olsa bile faili kolaylıkla bulunabilen kişisel mahremiyet konusu hepimizi hazırlıksız yakalamış önemli bir sorun olarak karşımızda durmaktadır.

Bilişimle büyüyen sorun: Mahremiyet

O kadar hazırlıksız yakalandık ki, tıp, hukuk ve bilişim uzmanları bu konuyu tartışmak üzere bir araya geldiklerinde, sorunu doğru bir şekilde tanımlamakta bile zorlanmaktadırlar. Diğer taraftan, bilişim imkânlarının şimdiye kadar mahremiyet konusu dikkate alınmadan kullanılagelmiş olması, mahremiyeti koruma adına alınabilecek önlemlerin, şimdiye kadar kullanmaya alıştığımız bilişim imkânlarının bir kısmından feragat etmemizi gerektirecektir ki, bu dahi problemin çözümünü zorlaştıran önemli bir etken olacaktır.

Ancak, bireysel hak ve özgürlüklerin giderek önem kazandığı modern dünyada, kişisel bilgilerin mahremiyeti konusu bir an önce ve ülke şartlarına uygun bir şekilde çözülmek durumundadır.

Kavramları doğru kullanmak

Sağlık bilgilerinin mahremiyeti konusunda çözüm bulmak amacıyla bir otu-

O kadar hazırlıksız yakalandık ki, tıp, hukuk ve bilişim uzmanları bu konuyu tartışmak üzere bir araya geldiklerinde, sorunu doğru bir şekilde tanımlamakta bile zorlanmaktadır. Bilişim imkânlarının şimdiye kadar mahremiyet konusu dikkate alınmadan kullanılagelmiş olması, mahremiyeti koruma adına alınabilecek önlemlerin, şimdiye kadar kullanmaya alıştığımız bilişim imkânlarının bir kısmından feragat etmemizi gerektirecek.

rum yapıldığında ilk göze çarpan şey, tarafların konuyu doğru tespit etmekte zorlanmalarıdır. Tıp, hukuk ve bilişim uzmanları, meseleyi alışageldikleri kavramlarla tanımlamaya gayret ettikleri için, sorunu doğru tarif eden bir kavram üzerinde uzlaşmakta zorlanmaktadırlar. Bu arada, aynı kavramın, farklı disiplinler tarafından farklı algılanması da ayrı bir sorun olarak karşımıza çıkmaktadır. Ortada dolaşan kavramlardan bazıları şunlardır: “Gizlilik”, “güvenlik”, “bilgi güvenliği”, “hasta güvenliği”, “mahremiyet”, “özel yaşam”, “kişisel haklar”.

Tartışma sırasında bunlardan birkaçı peşpeşe zikredildiğinde, bu kavramların taraflarda uyandırdığı anlamlar farklı olduğundan, problemi tanımlama ve çözüm için ortak bir tartışma zemini bulmakta zorlanılmaktadır.

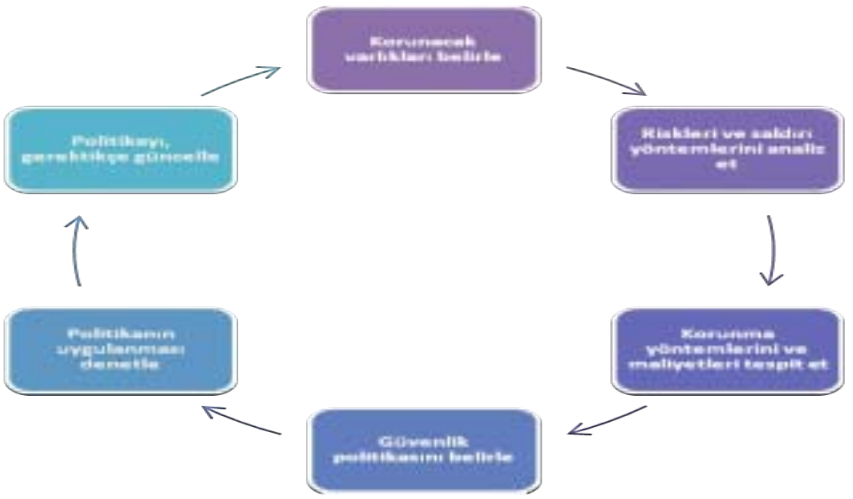
Örneğin, “güvenlik” kavramı, bilişim dünyasında veri ve ağ güvenliği kapsamında anlaşılan ve başlı başına bir sektör haline gelmiş müstakil bir branştır. Bugün artık bilgi güvenliği alanında çalışan sertifikalı bilişim uzmanları mevcuttur. Bu uzmanlardan güvenli bir bilgi sistemi kurmaları istendiğinde, askeri yöntemleri andıracak bir metodoloji takip ederler. Önce korumaları gereken değerleri (veri, verinin bütünlüğü, sürekli ve istikrarlı hizmet sunumu, kurumsal saygınlık vb.) güvenlik altına alabilmek için optimum maliyetle uygulanacak “güvenlik politikaları” geliştirirler. Politikanın belirlenmesi için öncelikle bir “risk analizi” yapılır. Risk analizinde sırasıyla, korunacak değerlerin envanteri çıkarılır, ardından bu değerlerin kime ve hangi tehditlere karşı korunacağı konusunda analizler yapılır. Tehditlerin türleri, geliş şekil ve yöntemleri düşünülür. Muhtemel bir zarar karşısında ivedi ve orta vadeli “geri kazanma maliyetleri” hesap edilerek, bir değeri korumak için ne kadar maliyete katlanılabileceği gibi gayet teknik çalışmalar yapılır.

Neticede ortaya çıkan politika, kuruma ait bir politikadır. Bu nedenle kurumda çalışan kişilerin hizmet sözleşmelerine bile dâhil edilir ve imza ile teminat altına alınır. Sonuç olarak, bir bilişimci “güvenlik” söz konusu olduğunda ne yapacağını gayet iyi bilir. Yeter ki, bu mühendislik çalışması için probleme ait sınır koşulları mevcut olsun. Ancak “hasta bilgilerinin güvenliği”nden bahsedip, sınır koşullarını tanımlamazsak, bilişimcinin kafasında canlanan şey, sunucu güvenliği, saldırılara karşı önlemler ve kendi içerisinde yetkilendirme özelliği olan otomasyon sistemlerinin kullanılması gibi oldukça temel önlemlerden ibarettir ki, bunlar mahremiyet ihlallerinin önlenmesi için yeterli olmayan oldukça teknik konulardır.

Örneğin hangi doktorun, otomasyon içerisinde yer alan bir sağlık verisine hangi şartlarda erişebileceği ve bunun nasıl denetleneceği gibi konular bilişimcinin ilk aklına gelecek konular arasında yer almaz. Kaldı ki, bir bilişimci bunlara çözüm bulmayı kendi uzmanlığı kapsamında da görmez. Bilişimcinin güvenlik politikası belirleyebilmesi için “sınır koşullar” olarak algılanmak üzere daha önceden hazırlanmış bir mevzuat olmalıdır. Bu nedenle mahremiyet konusu, sadece güvenlik uzmanı bilişimcilerin eline bırakılmayacak kadar çok yönlü bir problemdir. Zaten ileride açıklayacağımız üzere, sorun da tam bu noktada başlamaktadır.

Kavram uyuşmazlığı konusuna bir başka örnek de belki “hasta güvenliği” kavramıdır ki, temel anlamda “hastalara yardım ederken, zarar vermekten kaçınma” şeklinde tariflenmiştir. Tıp disiplini tarafından, hastaya verilen sağlık hizmetinde yükselen bir değer olan “hasta güvenliği”, bir çatı kavram olarak hastanın kişisel mahremiyetini de kapsayabiliyor olsa da, doğrudan bu anlamı çağrıştırdığını ve mahremiyet konusunda düzenleyici hususlar ortaya koyduğunu söylemek zor. Nitekim sayıları giderek artan hasta hakları dernekleri bile, hangi hakkın hangi şartlar altında sahip olunduğu ve bu hakların nasıl korunacağı konularındaki belirsizliklerden şikâyetçidirler. Dolayısıyla sağlık bilgilerinin mahremiyeti konusunda daha net ve tanımlayıcı bir kavrama ihtiyaç var.

Kavram uyuşmazlığına bilişim ve tıp alanında birer örnek vermişken, bir örnek de hukuk disiplini için verelim... “Hasta hakları”. Malum hukuk, “haklar” anlamına geldiğinden, içerisinde hak geçen herşey, hukukçular açısından kanunlarla güvence altına alınması gereken değerler olarak görülmektedir. “Hasta hakları” söz konusu olduğunda da, hukukçuların aklına gelen ilk anlamlar, Hasta Hakları Yönetmeliği’nde bahsedildiği üzere, “(...) Sağlık hizmeti verilen bütün kurum ve kuruluşlarda ve sağlık kurum ve kuruluşları dışında sağlık hizmeti verilen hallerde, insan haysiyetine yakışır şekilde herkesin “hasta hakları”ndan faydalanabilmesine, hak ihlallerinden korunabilmesine ve gerektiğinde hukuki korunma yollarını fiilen kullanabilmesine dair usul ve esasları düzenlemek (…) şeklinde oluşmaktadır.



Hangi doktorun otomasyon içerisinde yer alan bir sağlık verisine hangi şartlarda erişebileceği ve bunun nasıl denetleneceği gibi konular bilişimcinin ilk aklına gelecek konular arasında yer almaz. Kaldı ki, bir bilişimci bunlara çözüm bulmayı kendi uzmanlığı kapsamında da görmez. Bu nedenle mahremiyet konusu, sadece güvenlik uzmanı bilişimcilerin eline bırakılmayacak kadar çok yönlü bir problemdir.

Hasta haklarını düzenlemek üzere kaleme alınan bu yönetmelikte, bizim konumuz olan hasta bilgilerinin mahremiyeti 21. Madde'de (Mahremiyete Saygı Gösterilmesi) ele alınmakta ve bu kavrama şu anlamlar yüklenmektedir: "Hastanın, mahremiyetine saygı gösterilmesi esastır. Hasta mahremiyetinin korunmasını açıkça talep de edebilir. Her türlü tıbbi müdahale, hastanın mahremiyetine saygı gösterilmek suretiyle icra edilir. Mahremiyete saygı gösterilmesi ve bunu istemek hakkı; a) Hastanın, sağlık durumu ile ilgili tıbbi değerlendirmelerin gizlilik içerisinde yürütülmesini (...) kapsar".

Görüldüğü üzere, bu yönetmelikte hukukçuların diliyle neyin hak olduğu ifade edilse de, bu hakkın "nasıl" ve hangi şartlarla elde edileceği ve korunacağı açıklanmamıştır. Hele hele bir bilgi sistemi ortamında "bir tık uzaklıkta" olan hasta bilgilerinin kimler tarafından ve hangi şartlar altında erişilebileceği, bir ihlal söz konusu olursa ne olacağı tariflenmemiştir. Netice itibariyle, sağlık verilerinin mahremiyeti söz konusu olduğunda hukukçuların konuya bakışı, mevcut mevzuat çerçevesinde yapılan düzenlemelerden (ecnebi tabiriyle "as is") ibaret oluyor ve olması gereken konusunda ("how to") fikir yürütülmesi tek başına hukukçuları aşan bir konu olduğundan ilerleme kaydedilemiyor.

Yaygın olan bir diğer kavram hatası da "güvenlik" ile "gizlilik" arasında yaşanıyor. Bir şeyin gizli olması ile güvenliğin sağlandığı gibi yanlış bir kanı var ortada. Halbuki tek başına gizlilikle, bir başka deyişle meçhuliyetle güvenlik (security by obscurity) tesis edilmez. Gizlilik, güvenlik için kullanılan bir yöntem olsa da, bir şeyin gizli olması ile güvenli olması aynı şey değildir. Bir şeyin gizli olması, onun "erişilemez, bulunamaz" olduğu anlamına gelir. Hâlbuki güvenlik, bir şeye sadece izin/yetki verilenlerin erişebilmesi anlamına gelir. Örneğin, bir evin anahtarının yerinin gizli olması, ev sahibi için değil, yabancılar için geçerlidir. Dolayısıyla, anahtar güvenli bir yerdedir, ama mutlak gizli değildir.

Sonuç olarak, farklı uzmanlık alanlarının birlikte çalışabilmesi için, öncelikle aynı dili konuşmaları zorunlu olduğundan, akademik ya da pratik alanda, bu konuda yapılacak bir çalışmada öncelikle bir kavram çalışmasının yapılmasında fayda olduğunu düşünüyorum.

Çözüme yakın mıyız?

Çözüme ne kadar yakınız diye baktığımızda, yukarıda açıklamaya çalıştığımız kavram kargaşasının, çözüme yakınlığımıza da sirayet ettiğini görüyoruz. Şöyle ki, sağlık bilişimi konusunda çalışan firmalar (ve hatta Sağlık Bakanlığı), kendilerine mahremiyetle ilgili yöneltilen sorular karşısında her fırsatta sistemlerinin son derece "güvenli" olduğunu telkin ediyorlar. Burada soruyu soranın "mahremiyetten" neyi kastettiği, "sistemimiz güvenli" diye cevap verenin de güvenlikle mahremiyeti nasıl ilişkilendirdiği anlaşılamadığından, müzakereler de sağlıklı ilerlemiyor. Bu durumda da, mahremiyet konusunda çözüme ne kadar yakın ya da uzak olduğumuzu bile çözümlememiz güç oluyor. Benzer diyaloglar, hukukçular, hekimler ve bilişimciler arasında ikili kombinasyonlar halinde devam ediyor.

Sanki problemin etrafında dolaşıyoruz da, bir türlü parmağımızı doğru yere bastıramıyoruz gibi bir durum var. Bu çerçeveden baktığımızda, bendeniz probleme yakınlığımızı dahi ölçmekte zorlandığımızı düşünüyorum.

Bu arada, Sağlık Bakanlığı'nın mahremiyet konusunda yıllardır Medula sistemi ile sağlık verisi toplayan SGK'ya ve diğer pek çok kuruma göre bu konuda daha hassas olduğunu da vurgulamamız lazım. Nitekim Sağlık Bakanlığı'nın 2005 yılında yayınladığı bir Veri Güvenliği Genelgesi mevcut. Şu sıralarda bu genelgenin daha detaylandırılarak güncellendiğini de biliyoruz. Ancak, yukarıda da söylediğimiz gibi, bu konu ne sadece bilişimcilerin, ne de hekim veya hukukçuların çözüm getirebileceği bir konu. Bu nedenle, böyle bir genelgenin sadece Bilgi İşlem Dairesi tarafından kaleme alınmış olması bile, meseleye eksik yaklaştığımızın göstergesidir. Nitekim bu genelgede, "verilerin hastanın izni olmadan başka kurumlara/şahıslara verilmemesi" gibi esasları getirilmiş olsa da, bunun nasıl yapılacağı tarif edilemediği için, uygulanabilir olmaktan uzak kalmaktadır.

Problemi tanımlama denemesi

Kavramların yanlış anlaşıldığını veya hatalı kullanıldığını söyledikten sonra, "meselenin aslı şudur" diye kesin bir ifade kullanmak haddi aşmak olur sanırım. Bu nedenle, sağlık sektöründe tecrübeli bir bilişimci olarak, diğer ülke örneklerinden de yola çıkarak sadece bir tanımlama denemesi yapabilirim.

Öncelikle doğru kavramı tespit etmek lazım. Yabancılar, bu kavram için güvenliğin karşılığı olan "security", ya da hakkın karşılığı olan "right" gibi kavramları kullanmıyorlar. Yaygın kullanım, eş anlamlı da kullanılabilen "privacy" ve "confidentiality" şeklindedir. Her iki kelime de mahremiyet ve özel/kişisel yaşam anlamlarına gelmektedir. Dolayısıyla bizim de kullanmamız gereken kavram, bu anlamları ve maksadımızı daha iyi karşılayan "mahremiyet", "özel yaşam" ya da "kişisel yaşam" olmalıdır. Ben mahremiyet kavramını tercih ediyorum.

"Sağlık verilerinin mahremiyeti" probleminin tanımına gelince şunları söyleyebiliriz: Sağlık verilerinin mahremiyeti, bir verinin kimler tarafından ve nasıl oluşturulabileceği, nasıl, ne kadar süreyle ve nerelerde muhafaza edilebileceği, verilerin hangi durumlarda, hangi yollarla ve nerelere transfer edilebileceği, verilere kimler tarafından ne kadar süreliğine ve hangi onay(lar)la erişilebileceği, erişimin nasıl kayıt altına alınabileceği ve yine erişimlerin de

kimler tarafından sorgulanabileceği konularının düzenlenmesi problemidir. Bu problemin sınır koşulları, halen yürürlükte olan kanunlar ve AB kriterleri ile birlikte, hasta hakları, tıp ve hukuk uzmanlarının uygulanabilir gördüğü esaslardır. Çözüm, bu daire içinde belirlenmeli, yasalaşmalı ve pratiğe geçirilmesi için bilişim uzmanlarının çalışması istenmelidir.

Kısacası verinin hayat çevrimi boyunca başına gelebilecek tüm muhtemel senaryolar için düzenlemelerin yapılması gereklidir.

Bir paragrafta ifade etmeye çalıştığım kurallar (sınır koşullar) yasalarla belirlendikten sonra, bilişimcilerin bu kurallara uygun bir Güvenlik Politikası belirlemesi oldukça kolaydır. Mevcut teknolojik imkânlar, verinin saklanması, transferi ve erişilmesi gibi durumlarda ihtiyaç duyduğumuz tüm unsurları bize sağlamaktadır. Ancak, bu kuralların belirlenmesi, sanıldığı kadar kolay değildir. Örneğin, hastaneye gelen bir hastanın üroloji polikliniğindeki bilgilerinin, psikiyatri polikliniği tarafından görülebilmesinin ya da hastanede yapılan işlemlerin, hastanın aile hekimi tarafından görülebilmesinin ve benzer pek çok erişim senaryosunun ne kadar gerektiği ya da gerekmediği, hekimler ve hasta hakları savunucuları arasında bitmeyen bir tartışma konusu olacaktır, olmaktadır.

Diğer ülke örnekleri

AB'ye girme yolunda ilerleyen bir ülke olarak bu konuda AB'nin nasıl bir yol izlediğine bakarsak, sanırım zaman kazanmış oluruz. AB kriterlerine göre, sağlık verisinin sahibi hastanın kendisidir ve acil durumlar hariç hastanın onayı (patient consent) olmadan sağlık verilerine erişilmesi yasal değildir. Ancak, bunun nasıl uygulanacağı elbette çok karmaşık ve çoğu yerde de fazlasıyla teknik bir konu olduğundan, AB parlementosu uygulamayı tariflerken, e-sağlık alanında ISO (International Organization for Standardization) ve CEN (the European Committee for Standardization) tarafından belirlenmiş pek çok standardı referans etmiştir. Bu standartlardan bazıları şunlardır:

Elektronik Sağlık Kaydı sistemi kayıt standardı, CEN 1306

Elektronik Sağlık Kaydı sistemi kayıt yönetimi standardı, ISO 14589

Elektronik sağlık kayıtlarının arşivlenmesi için güvenlik gereklilikleri, ISO TC 215/SC

Bilgi sistemleri için açık arşivleme standardı, ISO 14721

Benzer düzenlemelerin 1996'dan beri ABD'de yürürlükte olan meşhur HIPAA (Health Insurance Portability and Accounting Act) yasasında da yapıldığını görmekteyiz. HIPAA yasa metni, içerisinde bilişimcilerin kullandığı UML (Universal Modelling Language) diyagramlarını içeren, teknik yönü ön plana çıkan bir dokümandır. Öyle ki, verinin hayat çevrimi içerisinde başına gelebilecek senaryolar bu diyagramlarla gösterilmiş ve hangi aktörlerin, hangi durumlarda verilere erişebileceği modellenmiştir. Böylelikle konu, sadece hukukçular ve hekimlerin değil, en az onlar kadar bilişimcilerin de kolay anlayabileceği bir formda sunulmuştur.

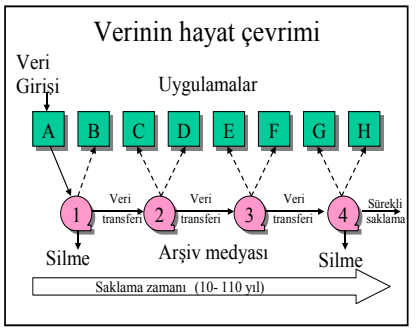
Bununla birlikte, HIPAA'nın pratiğe aktarılması, hastaya verdiği haklar nedeniyle kimi zaman sağlık hizmetinde aksamalara neden olduğu ya da hekimin hizmetten feragat etmesine yol açtığı iddia edilmektedir. Yine ABD'deki mahkemelerin HIPAA yasası gereği açılan pek çok davayla uğraşmak zorunda kaldıkları da şikâyet edilen diğer bir konudur.

Sonuç olarak bu konuda yasal çalışmasını tamamlamış ve uygulamakta olan ülkeler, özellikle hastaya önemli haklar vermişler, fakat bu durumun başka önemli sorunlara yol açtığını da tecrübe etmeye devam ediyorlar.

Çözüm için öneriler

Sağlık verilerinin önemi ve mahremiyeti konusunda referans alabileceğimiz yasalar, Anayasa'nın özel hayatın gizliliğini düzenleyen 20. Maddesi, Medeni Kanun'un 23 ve Türk Ceza Kanunu'nun 135. Maddeleridir. Ancak bu kanunlar, bırakın özelde sağlık verilerin mahremiyetini korumayı, sağlıkla ilgili olmasa bile diğer kişisel verilerin mahremiyetini bile detaylı şekilde düzenlemekten uzaktır. Diğer taraftan bu kanunları bir araya getirdiğinizde konuya bir bütün olarak bakmadıklarını görüyoruz. Bu nedenle kişisel verilerin mahremiyeti konusunu bir bütün olarak ele almayı ve düzenlemeyi hedefleyen Kişisel Verilerin Korunması Kanunu tasarısı hazırlanmıştır. Ancak yaklaşık 10 yıldır gündemde olan bu tasarı hala yasalaşmamıştır.

Yasal durum böyleyken sağlık kurumları, aile hekimleri, kan ve doku bankaları, laboratuarlar, uzaktan radyoloji ve pataloji gibi alanlarda TeleTıp hizmeti veren kurumlar, gün geçtikçe bilişimi daha fazla kullanıyorlar ve tüm kayıtlarını elektronik ortamda saklıyorlar. Sağlık Bakanlığı, hazırlıksız yakalandığımız bu durumu bir nebze olsun düzenleyebilmek için, başta yukarıda zikrettiğimiz Veri Güvenliği genelgesi olmak



üzere bir dizi adım atmış durumda.

Örneğin, Mart 2008'de Ankara Barosu, Türk Tabipler Birliği, Hasta Hakları Dernekleri ve diğer pek çok ilgili kurumu toplayarak bu problemi masaya yatırmış ve en azından bir zihin egzersizi yapılmasını sağlamıştır. Bu çalıştayda herkesin mevcut durumdan rahatsız olduğu ve yürürlükteki mevzuatın uygulamalardan çok geride olduğu konusunda mutabık olduğu gözlemlenmiştir.

Kanaatimce bundan sonra atılması gereken adımlar şunlardır: Herşeyden önce bizim yukarıda bir denemesini yaptığımız üzere, tarafların mutabakatıyla problemin tam olarak ne olduğunun tespit edilmesi gereklidir. Ardından, Kişisel Verilerin Korunması Yasası (henüz tasarı olsa da) referans edilerek, müstakil bir "e-sağlık yasası" hazırlanmalıdır. Bu yasa, bir temel yasa olmalı ve elektronik sağlık verilerinin nasıl ve hangi standartlara göre saklanacağı gibi teknik konuların kimler tarafından belirleneceği ve sağlık verisinin hayat çevriminde başına gelebilecek her türlü senaryoyu tariflemelidir. Bunun için ya mevcut TSE, ISO veya CEN standartlarına referans edilmeli, ya da bu konuların kimler tarafından düzenlenebileceği belirtilmelidir. Bununla birlikte, sağlık verilerinin mahremiyetinin ihlali söz konusu olduğunda bunun nasıl tespit edileceği ve ne tür müeyyidelerin uygulanacağı da açıkça belirtilmelidir.

Bu hedeflere ulaşılması önümüzdeki 5 yıl içinde olabilecektir. Ancak, bu kadar beklemeye tahammülümüz var mı, hep birlikte göreceğiz...

Kaynaklar

SD Platform, Sayı 7, Medine Budak, "Hasta Güvenliği Kültürü"

Sağlık Bakanlığı, Hasta Hakları Yönetmeliği, 01.08.1998, Resmi Gazete No. 23420

www.saglik.gov.tr (Sağlık Mevzuatı, Genelgeler, Bilgi İşlem Daire Başkanlığı)

Avrupa Parlementosu ve Konsülünün 24 Ekim 1995 tarihli ve 95/46/EC sayılı Yönergesi (Resmi gazete L 281/31 of 23.11.95).

AB Bilgi Güvenliği Politikaları Analiz Raporu, Temmuz 2007, Sağlık Bakanlığı Bilgi İşlem Daire Başkanlığı

http://www.hhs.gov/ocr/hipaa/