**Elektronik Sağlık Kayıtlarındaki Gizliliğin Kontrolünü Sağlayacak Yeni Bir Yaklaşım : Kayıtların Kullanımının Açıklığının Sağlanması**

**Mustafa Rüştü Soyal1**

**1**Dokuz Eylül Üniversitesi, Bilgisayar Mühendisliği, İzmir

rustu\_soyal@hotmail.com

**Özet :** Ülkemizde Elektronik Sağlık Kayıtları diğer birçok ülkeye göre çok daha yaygın kullanıldığı halde elektronik sağlık kayıtlarında gizliliğin ne derece sağlandığı konusunda hemen hemen hiç bir veri (geri bildirim vs.) mevcut değildir ve bu veriyi üretecek bir mekanizma da kullanılmamaktadır. Elektronik sağlık kayıtlarında gizliliğin ne derece sağlandığının araştırılmasına, izlenmesine veya kontrolünün yapılmasına yönelik hukuksal düzenlemelerin de yeterince etkili olmaması gizliliğin tanımlanmasını ve sağlanmasını kurum ve kişilerin inisiyatiflerine bırakmaktadır. Diğer taraftan da konunun asıl muhatabı olan hastalar (halk) da kendilerine ait verilerin hukuka veya etiğe uygun veya uygunsuz kimlerin ne amaçla kullandığı konusunda bir bilgi edinememektedirler. Ayrıca Elektronik Sağlık Kayıtlarındaki gizliliğin sağlanmasına yönelik çalışmaların başarısının geri bildirimine ve kullanıcının Elektronik Sağlık Kayıtlarında gizliliğe olan güveninin artırılmasına yönelik Elektronik Sağlık Kayıtlarındaki gizliliğinin ne kadar sağlandığına dair kullanılabilecek çok az mekanizma vardır. Çoğu zaman gizliliğin ihlal edildiği, uygunsuz olarak ele geçirilen veriler ancak bir şekilde teshir edilirse tespit edilebilmektedir. Hali hazırda çözüme yönelik hazırlanmış olan log ları izleyerek gizliliğin ihlalini tespit etmeye yönelik çalışmalar ise fiiliyata geçirilmesindeki zorlukları ve gizlilik ihlalini tespitteki başarısı bakımından tartışmalı konulardır. Bu çalışmada sağlık hizmeti veren kurumların çoğunda ve sağlık bakanlığının merkezi biriminde saklanan Elektronik Sağlık Kayıtlarının doğal sahibi olan hastalara kendi kayıtlarına yapılan erişimlerde ve güncellemelerde gerçek zamanlı bilgi gönderimini öngören bir çözüm önerilmektedir. Bu çözüm Elektronik Sağlık Kayıtlarındaki gizliliğin ne şekilde ve derece uygulandığının kontrolünün sağlanmasına ve hastaların kayıtların gizliliği ile ilgili endişelerin azaltılmasında önemli katkı sağlayacaktır. Ayrıca Elektronik Sağlık Kayıtlarındaki gizliliğin sağlanması ile ilgili çalışmaları desteklemesi konusunda önemli bir geri bildirim imkanı sağlayacaktır. Özellikle aşamalı olarak devreye sokulabilmesi sayesinde burada sunulan çözümün uygulanabilirliği, başarısı ve sağlayacağı diğer katkılar bakımından etkili olduğu görülmektedir.

**Anahtar Sözcükler** : Elektronik Sağlık Kayıtları, Gizlilik, Açıklık, Mahremiyet, yeni bir yaklaşım

**New Approach For Detecting The Violation Of Privacy By Transparency On Accession To Electronic Health Records**

**Abstract :** In spite of the fact that, Electronic Health Records (EHR) in Turkey are comparatively much more widely used than many other countries, there is almost no feedback available about the extent of privacy preservation and there is no mechanism available to generate this feedback. Definition and provision of privacy are left to the discretion of entities and individuals due to inadequacy of legal regulations about researching, monitoring and controlling the extent of privacy provided for EHR. On the other hand, patients who are principal correspondant of the subject would not be able to get information on how, by whom or for what purpose their own data are used whether in obedience with legal regulations or in an ethical way. Also there are too few mechanisms available which can measure the privacy level attained on EHR, in order to increase the user’s reliance on privacy preservation of EHR and in order to acquire feedback regarding the success level attained on privacy preservation of EHR. Most of the time, privacy violation can only be detected, when the data improperly captured are publicly exposed. Present efforts for detecting privacy violations based on tracing logs is still a controversial issue, because uncertainty in accomplishment on privacy violation detection and their difficulty in putting into practice. In this study, a solution is proposed suggesting real time information transmission to the patient when access to or updating of their own data which are stored in health care entities and in central unit of the Ministry Of Health is actualized. This solution will make significant contribution in reducing the patients’ concerns on privacy of the records, and in controlling the extent and method on privacy provision of EHR. Besides, this solution creates a considerable opportunity for facilitating feedback for studies on privacy provision of EHR. Particularly by means of its stepwise applicability, it appears that the solution presented here is effective in terms of its applicability, achievement and its supplementary contributions.

**Keywords : Electronic Health Records, confidentiality, Transparency, Privacy, New Approach**

**Giriş**

Günümüzün hızla gelişen bilgi teknolojilerinin faydaları sağlık hizmetlerinin de daha hızlı, ekonomik ve hatasız çalışmasına olanak sağlayabilmektedir. ABD nde yapılan bir araştırmaya göre temel sağlık hizmetlerinde çalışanların %75 i bilgi teknolojilerinden faydalanıldığında daha az hata olacağını, %75 i verimliliklerinin artacağını, %60 ı maliyetlerin azalacağını ve hastaların daha sorumlulukla hareket edildiğini düşünmektedir.[1] Ne var ki bilgi teknolojilerinin kullanımının değeri çok iyi bilindiği halde hasta mahremiyeti ile ilgili endişeler elektronik sağlık kayıtlarının yaygınlaşmasını yavaşlatmaktadır [2].

Ülkemizde hasta kayıtlarının mahremiyetini de kapsayan kişisel verilerin korunmasına yönelik anayasa ve kanunlar ile bazı düzenlemeler mevcuttur. Örneğin anayasanın 20. maddesinde aşağıdaki gibi bir düzenleme mevcuttur:

" (Ek fıkra: 7/5/2010-5982/2 md.) Herkes, kendisiyle ilgili kişisel verilerin korunmasını isteme hakkına sahiptir. Bu hak; kişinin kendisiyle ilgili kişisel veriler hakkında bilgilendirilme, bu verilere erişme, bunların düzeltilmesini veya silinmesini talep etme ve amaçları doğrultusunda kullanılıp kullanılmadığını öğrenmeyi de kapsar. Kişisel veriler, ancak kanunda öngörülen hallerde veya kişinin açık rızasıyla işlenebilir. Kişisel verilerin korunmasına ilişkin esas ve usuller kanunla düzenlenir. "

Ayrıca 5237 Sayılı Türk Ceza Kanunu da kişisel verilerin korunması ile ilgilidir:

"Verileri hukuka aykırı olarak verme veya ele geçirme

Madde 136-(1) Kişisel verileri, hukuka aykırı olarak bir başkasına veren, yayan veya ele geçiren kişi, bir yıldan dört yıla kadar hapis cezası ile cezalandırılır.

Nitelikli haller

Madde 137-(1) Yukarıdaki maddelerde tanımlanan suçların;

a) Kamu görevlisi tarafından ve görevinin verdiği yetki kötüye kullanılmak suretiyle,

b) Belli bir meslek ve sanatın sağladığı kolaylıktan yararlanmak suretiyle, İşlenmesi halinde, verilecek ceza yarı oranında artırılır. "

Bu tip hukuki düzenlemeler, (kanunlar, kanun hükmünde kararnameler, yönetmelikler vs.) çoğu zaman ya yurt dışındaki benzerlerine (AB, ABD, HIPAA vs.) bakılarak yapılmakta veya kişisel bilgiyi bir varlık olarak kabul edip hukuki olarak değerlendirilmektedir. Halbuki her ne kadar kişisel veriler o kişiye ait bir varlık ise de diğer varlıklarla farklılık gösterdiği noktalar da vardır. Kişiler diğer varlıkları söz konusu olduğunda genelde tam bir sahiplenme ve koruma içindeyken kişisel veriler konusunda tutumları ve esneklikleri farklı olabilmektedir. Kişisel verilerde gizliliğin artırılmasının sağlık hizmeti, sağlık araştırmaları ve hatta hastanın konforuna zaman zaman olumsuz etkisi olabileceği konusunda araştırmalar vardır[3]. Bu durumda hukuki düzenlemeler yapılırken bazı zorunlulukların (bildirimi zorunlu hastalık kayıtları vs.) dışında da kişisel verilerin gizliliğinin esnetileceği noktalar mevcut olabileceği gibi tam tersi diğer varlıklara göre daha farklı bir korumaya ihtiyaç duyan gizlilik konuları da olabilir. Bunların ortaya çıkartılabilmesi için hastaların/halkın tutum ve davranışlarını bir fiil takip edip geri bildirim alınabilecek şekilde hastaların/halkın dahil olduğu ortamların oluşturulması gerekmektedir.

Hukuken korunan ve ihlali durumunda cezaları kanunlar ile belirlenmiş olan kişisel veriler ile ilgili düzenlemelere rağmen bu suçların tespiti ve ispatı ile ilgili de önemli zorluklar vardır. Örneğin hasta kayıtlarını uygunsuz olarak ele geçiren ve bu sayede maddi menfaat sağlayan bir firmanın ele geçirdiği verileri teşhir etmediği sürece böyle bir suç eylemini gerçekleştirdiğinden başkalarının haberi olmayabilmektedir. Kişisel verilerin gizliliği ile ilgili bir suç unsuru oluştuğunun ispatı için ise yeni bazı sorular ortaya çıkmaktadır;

Kimler veriye erişebilmeli?

Hangi şartlarda erişim uygun kabul edilebilmeli?

Ne şekilde kullanımı uygun kabul edilmeli?

Verinin doğruluğu/bütünlüğünün korunması nasıl sağlanmalı? (O'Brien, & Yasnoff, 1999)

Kişisel verilerin ihlalinin önlenmesine yönelik çalışmalar bir yana kişisel verilerin ihlalini tespit edebilecek çalışmalar da büyük önem taşımaktadır. Bu çalışmalar sayesinde her şeyden önce ihlalin olup olmadığını bildirmesi sayesinde kişisel verilerin ihlalinin önlenmesine yönelik çalışmaların ne derece başarılı olduğu konusunda bir geri bildirim edinilmektedir. Ayrıca ihlalin oluştuğunun erken bildirimi durumunda olası sucun daha da (verinin kopyalanması, kullanılması, teşhir edilmesi vs) büyümeden önlenebilmesi imkanı sunmaktadır.

Günümüzde elektronik sağlık kayıtlarında gizliliğin ihlalini tespit için önemli çalışmalar vardır. Bu çalışmaların çoğu Health Insurance Portability and Accountability Act (HIPAA) nın Section 164.308(a) ve Section 164.312(1)(b) maddelerinde öngördüğü gibi tutulması gerekli olan log dosyalarını kullanmaktadır. Jihoon Kim et al. ın "Anomaly and Signature Filtering Improve Classifier Performance For Detection Of Suspicious Access To EHRs" çalışmasında olduğu gibi gizlilikten sorumlu kişinin dahil olduğu yarı manuel sistemler veya Aditya Krishna Menon et al. ın "Detecting Inappropriate Access to Electronic Health Records Using Collaborative Filtering" ve Boxwala AA et al. "Using statistical and machine learning to help institutions detect suspicious access to electronic health records" çalışmalarında olduğu gibi makine öğrenme tekniklerinin kullanıldığı çalışmalar bu konudaki iyi örneklerdendir. Ancak bu çalışmaların hiç biri hastaları çözüm sürecinin içine dahil etmemektedir. Halbuki gizlilik konusunda halkın hassasiyetlerindeki değişkenlikler tam olarak bilinmeden halk için bir gizlilik politikası ve buna uygun sistemler tasarlamak, tasarlanacak sistemlerin ileride eksik veya kısmen gereksiz durumlarını ortaya çıkartabilir. Daha da önemlisi hali hazırdaki diğer çözüm çalışmalarının başarısı için onların kontrolünü yapacak aynı tekniği kullanmayan paralel bir çalışmanın da olması faydalı olacaktır. Örneğin makine öğrenme tekniği ile gizliliği tespit etme metodunu kullanan bir çalışmanın öğrenme sürecinin başında gizlilik ihlallerini tespit edip bir vaka olarak sisteme aktaracak bir başka mekanizmaya ihtiyaç olabilir. Gizliliğin tespiti konusundaki çalışmaların yeni olması nedeniyle gizlilik ihlallerini büyük ölçüde tespit edecek bir çözüm seçeneği henüz mevcut olmadığından pratik olası çözümler üzerinde durulması faydalı olacaktır. Hızlı fiiliyata geçirilebilecek bu tip çözümler hem hemen hemen hiç gizlilik ihlali tespiti çözümü olmayan sağlık kuruluşları için acil bir kısmi çözüm olabilecektir, hem gizlilik ihlali tespiti çalışmalarında daha insan bağımsız çalışan sistemlerin eğitilmesi ve test edilmesinde hem de gizlilik ihlali önleme çalışmalarının testinde kullanılabilecektir.

Tüm bu zorluklar ve karmaşa içinde çözüm sürecine hastaların ya dahil edilmemesi veya az dahil edilmesi belki de olası pratik bazı çözümlerden veya çözüm desteklerinden de mahrum kalınıyor anlamına gelebilir.

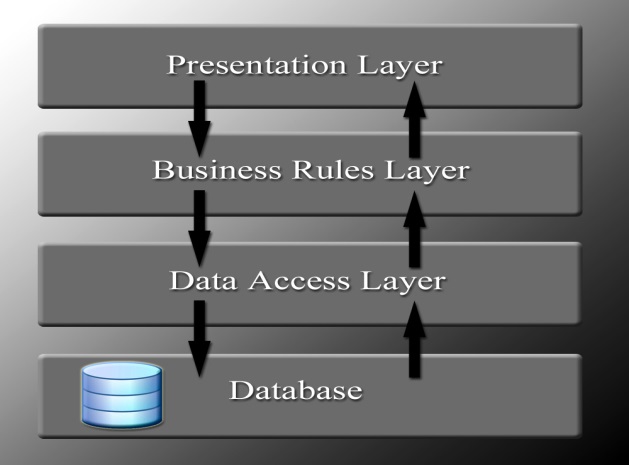
Elektronik sağlık kayıtlarında gizliliğin sağlanması için hukuki, idari bir çok düzenlemeler ve bu düzenlemelerin fiiliyata geçirilebilmesi için çalışmalar yapılmaktadır. Bu çalışmalar büyük ölçüde kanun/kural yapıcılar, sistem tasarımcıları, geliştiricileri ve sağlık sektörü mensupları tarafından yürütülmektedir. Gizlilik kavramının soyutluğu ve kişiden kişiye değişkenliği nedeniyle konulan kanun ve kuralların yapıcıları için ayrı bir zorluk olduğu kadar sistem tasarımcı ve geliştiricileri için de uygulamaya geçirmeleri gereken yeni kavramlar olduğundan nasıl yapılacağı kadar ne yapılacağı konusunu da gündemde tutmaktadır. Konunun asil muhatabı olan hastalar ise surecin içinde yeterince yer almamaktadır. Bunun sebeplerinden bir tanesi bu konuda sürece dahil olabilecekleri bir ortamın ve dolayısıyla da farkındalıklarının olmamasıdır. Bu katılımcılığı ve farkındalığı yaratmanın bir yolu da Elektronik Sağlık Kayıtlarının tam olarak neyi içerdiği, bunların kendilerine ait olduğu ve şu anki durum itibarıyla bu bilgilere kimlerin ne zaman ne sıklıkta erişim sağladığı konusundaki bilgilendirmedir. Böyle bir durum halkın geri bildirimleri sayesinde kanun/kural yapıcılar ve sistem tasarımcılar/geliştiriciler in çalışmalarına yön vermeleri konusunda önemli bir katkı sağlanacaktır. Ayrıca Elektronik Sağlık Kayıtlarındaki gizliliğin sağlanması için yapılan çalışmalarındaki hatalar ve eksikler çoğu zaman gizlilik ihlali ile erişim sağlanmış (ele geçirilmiş) veriler eğer teshir edilirse ve bu teshir ilgili kişi tarafından fark edilirse tespit edilebilmektedir. Halbuki hastaların kayıtlarının kullanımını izleyebildikleri bir durumda bu tip hata ve eksiklerin daha çabuk (neredeyse anında), kayıtlar teshir edilmese bile tespit edilebilecektir. Kayıtlar teshir edilmeden önce uygunsuz erişim tespit edilebileceğinden gizlilik çalışmalarının geliştirilmesinde de önemli bir katkı sağlayacaktır. Bu durumdaki erken uyarı gizliliğin ihlali durumunda kayıtlar teshir edilmeden veya menfaat amaçlı kullanılmadan zarar daha vahim bir hal almadan müdahale etme şansı vermektedir.

Genel olarak şu ana kadar hastaların Elektronik Sağlık Kayıtlarındaki çalışmalarında surece dahil edilmesi ile ilgili en belirgin nokta Elektronik Sağlık Kayıtlarında hastaların kendi kayıtlarına ulaşabilme haklarının verilmesi ve kayıtlarının saklandığı kurum/merkezlerdeki gizlilik politikalarının, prosedürlerin ve teknolojilerinin açıklığının sağlanması hakkıdır(HIPAA). Ancak günümüzde hemen hemen tüm sağlık kurumlarında (bazı laboratuvarlar hariç) haklı veri güvenliği endişeleri ile hastalara kayıtları hala sadece kağıtta verilebilmekte dijital olarak anlık görebilecekleri bir ortam sunulamamaktadır. Aslında hasta kayıtları en çok sağlık hizmeti sunan kurumların ve kişilerin (örn. hekimler) kullandıkları ve buradaki çoğu bilgiyi ancak onların anladıkları ve kullanabilecekleri bilgiler olduğu için hastaların kendi kayıtlarını görmeleri çoğu zaman ve belki de çoğu kişi için önem arz etmemektedir. Hasta kayıtlarının nasıl korunduğu ile ilgili yapılacak açıklamalar ise teknik konular olduğu için çoğu zaman ve çoğu kişi tarafından anlaşılmayacaktır. Buna karşın kayıtlarının doğal sahibi olan hastaların kayıtlarını bir noktada emaneten saklayan kurum ve kişilere önemli sorumluluklar düşmektedir. Bu kayıtlar maddi çıkar için kullanılabileceği gibi uygunsuz teshiri gibi durumlarda hastada telafisi zor maddi ve manevi zararlara da neden olabilecektir. Bu yüzdendir ki hastaların kendine ait bir varlığı olan hasta kayıtlarının kullanımının takibi hasta için daha kritik önem taşımaktadır.

Bu çalışma hastaların Elektronik Sağlık Kayıtlarındaki gizlilik çalışmalarının yönlendirilmesine katkı sağlayacak ve bu çalışmaların sonuçlarının kontrolünü sağlayacak bir çözüm önermektedir. Çözümde hastaların sağlık kurum ve merkezlerinde saklanan kendilerine ait kayıtlarına yapılan erişimler ve güncellemelerden haberdar olması sağlanacaktır. Çalışmada böyle bir tasarımın nasıl gerçekleştirilebileceği, gerçekleştirme risk ve maliyetleri, faydaları ve ileriye donuk ne şekilde geliştirilebileceği anlatılmıştır.

**Çözümün Sağlık Kurumlarında Bilgi Sistemlerine Entegrasyonu**

Sağlık kurumlarındaki bilgi sistemleri, sadece klinik hasta kayıtlarını değil aynı zamanda finansal ve malzeme (stok) yönetimi işlemlerini de yürüttüğünden ve bu konulardaki hatalar somut olarak daha çabuk ve kolay tespit edilebildiğinden belirli bir kalite standardında sahip olmaları gerekmektedir. Bu nedenledir ki gerek yazılım teknolojileri gerekse kullanılan ürünler/araçlar ı bakımından kendilerini geliştirdiklerini ve yenilediklerini söyleyebiliriz. Özel sektör bu gelişmeyi finansal, malzeme yönetimi ve hasta memnuniyeti gibi nedenlerden sağlarken devlet kurumları da benzer nedenlerden yeniledikleri alım şartnameleri ile sağlamaktadırlar. Bunun sonucu günümüzde sağlık sektöründe n-katmanlı yazılımlar veya en azından veri tabanı ile bir şekilde ayrışmış yazılımlar kullanıldığını görmekteyiz. Örnek bir mimariyi Tablo 1 de görmekteyiz.



Tablo1

Ülkemizde çoğu sağlık sektöründeki yazılımların yıllardır kullanılıyor olduğunu düşünecek olursa bu katmanlar içinde kullanım sırasında en az geliştirme ve tasarımsal değişikliğe ihtiyaç duyan katmanın "database" katmanı olduğunu söyleyebiliriz. Diğer katmanların örneğin veri güvenliği ve gizliliği veya kullanıcı ihtiyaçları gibi sebeplerle yapılan değişiklikler ile nispeten daha çok geliştirme ve tasarımsal değişiklik nedeniyle geliştirici yetkisinde/seviyesinde müdahaleye ihtiyaç duymaktadır. Normalde veri güvenliği ve gizliliği ile ilgili belirli bir çalışmanın yapılmış olduğunu varsaydığımız bir yazılım paketine her yapılan müdahalenin veri güvenliği ve gizliliği acısından riski artırma olasılığı vardır. Bu nedenle daha az ve ender müdahale gerektiren "database" katmanının daha iyi korunan ve daha az kişi tarafından müdahale iznine sahip olması beklenir. Bu durum aynı zamanda "database" katmanına entegre edilen işlemlerin de daha iyi korunduğu anlamına gelecektir.

Verilerin gizliliğinin sağlanması ile ilgili birçok çalışmada bu konudaki işlemler genellikle "database" katmanının dışında (üstündeki katmanlarda) gerçekleşmekte ve en son işlem olarak erişim talebi "database" katmanına yapılmaktadır. Yani eğer erişim talebi veri tabanına kadar gelmişse gerekli gizlilik politikalarından geçtiğini ve alıcısına ulaştırılacağı anlamına gelmektedir. Bu nedenle hastaya kendi bilgisine bir erişimin olduğu bilgisinin oluşturulacağı yer "database" katmanının hemen üstü veya mümkün ise "database" katmanının içinde olmalıdır. Tüm uygulamaların tek/aynı "data access layer" i kullandıkları durumda erişimin olduğu bilgisinin oluşturulacağı yer "data access layer" i de olabilir. Eğer "database" katmanına farklı bir uygulamadan "örn: mobil, web vs" aynı "data access layer" kullanılarak erişim sağlanmama olasılığı var ise o durumda erişimin olduğu bilgisinin oluşturulacağı yer için üç seçenek karşımıza çıkmaktadır. 1. "database" katmanı 2. ortak kullanılacak yeni bir "data access layer" 3. diğer uygulama için de erişimin olduğu bilgisinin oluşturulacağı ve hastaya gönderileceği yeni bir "data access layer". Kontrolün zorluğu ( "data access layer" i güncellemede aynı işlemlerin farklı yerlerde yapılma zorunluluğundan oluşabilecek güncelleme anomalileri) nedeniyle 3. olasılık son çare olarak düşünülmelidir. Hem günümüzdeki değişik uygulama ortamlarının çokluğu hem de veri tabanlarının üstünde kontrol ve yazılım yapma imkanları (örn: procedure ler, trigger ler vs.) düşünülecek olursa en güvenli çözümün 1. seçenek olduğu gözükmektedir.

Sağlık Kurumlarında bilgi sistemlerinde eğer erişim talebi veri tabanına kadar gelmişse gerekli gizlilik politikalarından geçtiği ve alıcısına ulaştırılacağı varsayımının çok az da olsa bazı istisnası olabilir. Örneğin de-identified edilmiş veriler için erişim sağlanıp veriler "database" katmanından alındıktan sonra "database" in üstünde bir katmanda dönen sorgu sonuçlarının tamamına bakarak re-identified etme olasılığı değerlendirilip eğer böyle bir olasılık var ise sonuçların alıcısına gönderilmemesi yoluna gidilebilir. Bu durumda "database" katmanından veriye erişim bilgisi oluşurken aslında veri o erişimin yapılma amacı için kullanılmamış olacaktır. Bu durumda iki yol izlenebilir; birincisi zaten de-identified olarak erişim yapıldığında anonymous şartları oluşmamış ise bunun gönderilmeyeceği konusunda genel olarak hastaları bilgilendirilerek bu durumlar bu haliyle kabul edilir. Yani de-identified olarak yapılan erişim bildirimlerinin bazı durumlarda kullanıcılara/alıcılara ulaştırılmayacağı baştan kabul edilir. İkinci yol ise sistem içinde erişimi yapılmış verinin kullanıcıya ulaşmasını engelleyen durumlar için bilgilendirici bir log tutulur ve doğrudan bu bilginin kullanıcıya ulaştırılmadığı bilgisi hastaya iletilir. Böylece hastaya her ne kadar kişisel verisine erişim yapıldığı bilgisi gelse de aynı zamanda başka bir kontrol tarafından erişimin engellendiği bilgisi de ulaştırılır.

**Çözümün Aşamaları**

Çözümün uygulanabilirliğindeki en önemli avantaj aşamalı olarak uygulanması konusundaki esnekliğidir. Bu çözümü kullanarak çok basit veya daha karmaşık ve fonksiyonel bir çok tasarım/senaryo hazırlanabilir. Bu senaryolar en baştan fonksiyonel hazırlanabileceği gibi basit bir senaryo ile başlayıp aşamalı olarak daha fonksiyonel hale getirilebilir. Bu şekilde hazırlanabilecek birkaç senaryo örneği aşağıda verilmiştir;

Senaryo 1:

İstekli/gönüllü olan hastaların kendilerine ait sağlık kayıtlarına yapılan erişimleri izleyebilecekleri bir web uygulaması (internet sayfası) hazırlanır ve onlara hesap açılarak onların kullanımına sunulur. "database" katmanında hazırlanan prosedürler ile verilere erişim durumunda hangi veriye hangi kullanıcı ne zaman erişmiş bilgisi web uygulamasına gönderilir. Hangi veriye hangi kullanıcı ne zaman erişmiş bilgisi "database" katmanında zaten var olduğu için hazırlanacak prosedürlerde dışardan (diğer katmanlardan) herhangi yeni bir bilgiye ihtiyaç duyulmayacaktır. Hasta şüpheli gördüğü erişim kayıtları için aynı web uygulamasından bilgi talebinde bulunabilecektir. Gönderilen taleplerin ilgili sağlık kuruluşunda görevlendirilecek yetkili kişi (yurt dışındaki bazı kurumlarda bulunan "privacy officer" gibi) tarafından değerlendirilip sonucu geri dönmesi sağlanacaktır.

Senaryo 2:

Senaryo 1 deki tüm duruma ilaveten kayıtlar için risk değerlendirmesi yapacak bir sistem oluşturulur. Örneğin olağan "kabul edilebilecek" erişim kayıtlarına 1, "dikkat edilecek" erişim kayıtlarına 2 ve "riskli erişim kayıtlarına" 3 verilebilir. Hangi kayıtların hangi durumlarda hangi dereceyi alması gerektiği ile ilgili bir çalışma yapılır. Örneğin muayene kaydı açılmış bir hasta için ilgili doktorun belli bazı kayıtlara erişimde bulunması "kabul edilebilir" olabilir. İlk muayene kaydı açılırken (sonradan bununla ilgili erişimler olağan kabul edileceğinden) yapılan erişimler gerçekten o kaydı açanın hastanın kendisi olup olmadığını kontrol etmesi için "dikkat edilecek" kayıt olarak işaretlenebilir. Hiçbir giriş veya açılmış bir dosya yokken yapılan erişimler ise "riskli erişim kaydı" olarak değerlendirilir. Risk değerlendirmesinde kaydın içeriği de dikkate alınabilir. Örneğin psikiyatri, kadın hastalıkları veya üroloji gibi konularda daha yüksek risk derecesi verilebilir. Bu şekilde web uygulamasına erişim kaydı, risk derecesi ile birlikte gönderilir. Hastalardan sadece şüpheli durumlarda değil aynı zamanda kaydın kendine göre risk derecesi ile uyuşmadığı durumlarda da geri bildirim yapması talep edilir. Bu bildirim hem risk derecelendirme sisteminin geliştirilmesinde faydalı olacak hem hastalara kendilerine daha uygun risk derecelendirmesi yapılması sağlanacak hem de gelecekte geliştirilecek/tasarlanacak gizlilik ihlalini tespit eden sistemler için önemli bir bilgi birikimi oluşturacaktır. Hasta bazı risk gurupları için erişim kaydı oluştuğunda web uygulamasında görülmesinin dışında kendisine e-posta olarak gönderilmesini ve hatta hassasiyetine göre cep telefonuna mesaj (watsapp, viber gibi uygulamalar da olabilir) olarak gönderilmesini de talep edebilir.

Senaryo 3:

Senaryo 2 deki tüm duruma ilaveten sağlık bilgi sistemi kullanıcıları için de bir web uygulaması hazırlanabilir. Kullanıcıların kendi belirledikleri risk gurubundaki erişimlerde kendilerinin erişimde bulunduğunu içeren kayıtlar için bu web uygulamasına erişim kaydı gönderilebilir. Kullanıcılar bazı risk gurupları için erişim kaydı oluştuğunda web uygulamasında görülmesinin dışında kendisine e-posta olarak gönderilmesini ve hatta hassasiyetine göre cep telefonuna mesaj olarak gönderilmesini talep edebilir. Böylece bu durum özellikle başka kullanıcıların şifrelerini ele geçirerek yapılabilecek uygunsuz erişimler için hızlı bir erken uyarı olacaktır. Kullanıcılar için hazırlanmış web uygulamasına kullanıcıların açıklama yazma imkanı da tanınabilir. Böylece gerçekten belirli bir amaç için erişimde bulunan kişinin amacı rutinin dışında ise erişim eyleminin üstünden zaman geçmeden (unutulmadan) erişim gerekçesini web uygulamasına yazabilir. Yazdığı gerekçe hastanın kullandığı web uygulamasından da görüleceğinden belki de hastanın o erişim kaydı için normalde talep edeceği açıklamaya gerek kalmaz. Ayrıca bazı durumlarda kullanılan programlar erişim gerekçesini kendiliğinden erişim bilgisi kaydına ekleyebilir.

Bu şekilde senaryoları çeşitlendirmek mümkündür. Burada önemli olan ihtiyaçlar ve imkanlar doğrultusunda senaryonun şekillendirilmesidir.

**Çözümün Riskleri**

Bilgi sistemleri konusunda daha profesyonel kişilerce desteklenen sağlık kuruluşlarındaki verilerin güvenliği ve gizliliği konusunda bile endişe duyulurken genel olarak bu konuda daha amatör olan hastalara bazı verilerin gönderilmesi ile risklerin daha da artabileceği gibi bir düşünce doğru değildir. Bu gibi durumlarda en çok endişelenilen durum hastaların şifrelerinin bir şekilde iyi niyetli olmayan kişiler tarafından ele geçirilmesi durumudur. Çözümde öngörülen web uygulaması gerek hastalara gerek ise kullanıcılara sadece ilgili kayda erişim bilgisini verecektir. Bu bilgide kişilerin kişisel sağlık kayıtları ile ilgili verilerin güvenliğini veya gizliliğini ihlal edecek bir bilgi olmayacaktır. Örneğin herhangi bir muayene veya tetkik kaydına erişim yapıldığının bilgisini veren erişim bilgisi kaydı, muayene veya tetkikin içeriğini göstermeyeceğinden teşhiri durumunda sakıncalı bir durum oluşturmayacaktır.

**Çözümün Maliyeti**

Çözümün hazırlanacak basit bazı web uygulamaları ve sağlık da kullanılan bilgi sistemlerindeki bazı düzenleme ve yazılımlar dışında önemli bir maliyeti yoktur. Veri tabanlarında gidilecek bazı standardizasyonlar ile bu düzenlemelerin aynılarının çok daha yaygın olarak kullanılabilmesi mümkündür. Elektronik sağlık kayıtlarında veri güvenliği ve gizliliği ile ilgili çalışmaların zorluğu ve maliyeti göz önüne alınacak olursa bu çalışmalara destek ve katkı sağlayacak böyle bir çözümün maliyetinin önemsizliği ortaya çıkmaktadır.

Maliyetin düşük olmasının en önemli sebeplerinden biri de çözümden elde edilmek istenen faydanın aslında büyük ölçüde gönüllü hastalardan gelmesidir. Gönüllü hastalar ki onlar büyük ölçüde verileri konusunda hassasiyet gösteren kişiler olacaktır, ülkemizde yaygın olarak kullanılması nedeniyle internetteki uygulamaları kullanmakta zorluk çekmeyecektir. Türkiye'de nüfusun ve bununla orantılı hasta sayısının çokluğu, nüfus içindeki gençlerin çokluğu oransal olarak göz önüne alınacak olursa gönüllülerin sayılarının işe yarayacak geri bildirim almak için yeterli olacağını düşünebiliriz. İhtiyaç olursa katılımı artıracak teşvik edici tedbirler de alınabilir.

**Çözümün faydaları**

Elektronik sağlık kayıtlarındaki gizlilik ile ilgili hukuki ve idari bir takım düzenlemeler yapılmaktadır. Ancak bu düzenlemeler için çok az hastaların tutum ve düşünceleri ile ilgili bilgi kullanılabilmektedir. Sunulan çözüm ile hastaların tutum ve düşünceleri ve bunun sonucunda da ihtiyaçları konusunda değerli bir bilgi birikimi oluşacaktır.

Elektronik sağlık kayıtlarında gizliliğin sağlanması ile ilgili çalışmalar yapılmaktadır ve görünen odur ki bu çalışmalar artarak devam edecektir. Yapılan bu çalışmaların gizliliği ne kadar başarıyla sağladığını test edecek burada sunulan çözüm bu çalışmaların daha sağlıklı yapılmasını sağlayacaktır. Elektronik sağlık kayıtlarındaki gizlilik ile ilgili çalışmaların yeni olması nedeniyle kontrolü yapmak üzere geliştirilmiş çok iyi (tüm gizlilik ihlallerini tespit edebilecek) bir çözüm mevcut değildir. Hastaların dahil olduğu bu çözüm pratikliği ve basitliği nedeniyle iyi bir test ve otokontrol mekanizması olarak kullanılabilir.

Sağlık kurumları çalışanları çoğu zaman elektronik sağlık kayıtlarındaki gizlilik konusunda gerekli eğitimi almadığından veya başka sebeplerden bir şekilde tedarik ettiği yetki sahibi bir şifre ile çok da art niyetli olmadan gizlilik konusunda yeterli titizliği göstermeyip kolaylıkla hasta kayıtlarına erişim sağladığı durumlar mevcut olabilir. Burada sunulan çözüm uygulandığında başta sağlık kurumu çalışanları olmak üzere hasta kayıtlarına erişim yapılması durumunda erişim yapılan kaydın sahibine ve erişimin kim adına yapılıyorsa kullanıcısına bildirim gittiği bilindiğinde elektronik sağlık kayıtlarındaki gizlilik konusuna daha ciddiyetle yaklaşılacaktır.

Sağlık kurumları Elektronik sağlık kayıtlarındaki gizlilik ile ilgili bir çalışma yapsın veya yapmasın sağlık kurumlarında gizliliğin gerçekten ihlal edilip edilmediği tespit etmekte zorluklar vardır. Burada sunulan çözümün sonuçları ile bu tespitler daha kolay yapılabilecek ve eğer durum kötüyse (çok fazla gizlilik ihlali var ise) çözüm ile ilgili acil önlem almak için harekete geçilebilecek, durum iyi ise sonuçlar duyurularak halkın yersiz endişeleri ortadan kalkacaktır.

**Sonuç ve Öneriler**

Burada sunulan çözüm elektronik sağlık kayıtlarındaki gizlilik ile ilgili önemli bir ihtiyaca yöneliktir. Çözümün kendisi Elektronik sağlık kayıtlarındaki gizliliğin ne derece sağlandığına dair bilgi vermesi konusunda doğrudan ve dolaylı faydalar sağlamaktadır. Doğrudan Elektronik sağlık kayıtlarındaki gizlilik ihlallerinin ortaya çıkmasını ve halkın bu konudaki endişelerinin gerçekçi bir zemine oturtmasını sağlarken dolaylı olarak da Elektronik sağlık kayıtlarındaki gizlilik konusunda gerek hukuki ve idari kararlar alınırken gerekse sistem geliştirme ve tasarım konusunda yürütülen/yürütülecek çalışmalara destek sağlayacaktır.

Çözüm genel olarak sağlık kurumlarındaki bilgi sistemine kolaylıkla entegre edilebilecek şekildedir. Aşamalı ve esnek tasarlanabilmesi sayesinde çözümden fayda sağlamak süratle gerçekleştirilebilmekte ve istenirse daha fazla fayda sağlanacak süreçlere de geçilebilmektedir.

Gizlilik gibi hassas bir konuda ilave birtakım işler önerildiği halde çözümün kendisinin gizlilik konusunda hiçbir riski bulunmamaktadır.

Çözümün maliyeti bu konuda sağlayacağı maddi, teknik ve manevi katkı göz önüne alındığında çok makul seviyelerdedir.

Çözüm neredeyse tüm ayrıntılarıyla burada sunulmuştur. Herhangi bir sağlık kuruluşunda gerçekleştirilmeye hazırdır.

**Kaynaklar**

[1] J.G. Anderson, E.A. Balas, Computerization of primary care in the United States, Int. J. Health Inform. Syst. Inform. 1 (3) (2006) 1–23.

[2] Angst CM, Agarwal R. Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion.

[3] Charity Scottt IS TOO MUCH PRIVACY BAD FOR YOUR HEALTH? AN INTRODUCTION TO THE LAW, ETHICS, AND HIPAA RULE ON MEDICAL PRIVACY\*