Fərdi Tibbi Məlumatların On-line Mühitdə Təhlükəsizliyi Problemləri

Rasim Əliquliyev[1], Fərqanə Abdullayeva[2]
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*rasim@science.az*, [2]*farqana@iit.ab.az*

***Xülasə*—Təqdim olunan məqalədə fərdi tibbi məlumatların onlayn mühitdə təhlükəsizlik problemləri tədqiq olunur. Elektron tibb qeydləri və sistemləri terminlərinə aydınlıq gətirilir, eSəhiyyə sahəsində fəaliyyət göstərən standartlaşdırma təşkilatları, fərdi tibbi məlumatların toplanmasını həyata keçirən tətbiq modelləri təsvir edilir. Fərdi tibbi məlumatların qorunması üzrə beynəlxalq təcrübə araşdırılır, təhlükəsizlik və gizlilik problemləri müəyyən olunur və onların həlli üçün təklif və tövsiyələr verilir.**

Açar sözlər— eSəhiyyə; elektron tibbi qeydlər; fərdi tibbi məlumatlar; eResept; pasiyent bioqrafiyası; smart hospital; mobil səhiyyə.

I. GİRİŞ

Son zamanlar səhiyyə xidmətləri elektron səhiyyə (eSəhiyyə) mühitinə böyük sürətlə keçid edir. eSəhiyyə informasiya-kommunikasiya texnologiyalarının (İKT) tibbi informasiya sisteminə tətbiqidir. eSəhiyyə pasiyentin sağlamlığı ilə bağlı kağız yazılarının idarə edilməsində meydana çıxan fasiləsiz artan problemlərini aradan qaldıra bilən həllər təqdim edir.

eSəhiyyə Avropa Kommisiyasının (ing. *European Commission, EC*) prioritet məsələsidir. Avropa Kommisiyasının eSəhiyyə fəaliyyətinin başlıca məqsədi vətəndaşların xəstəliyinin diaqnozunu, müalicəsini, monitorinqini, idarə edilməsini yaxşılaşdırmaq, şəxslərin səhiyyə müəssisələrinə girişini asanlaşdırmaq, tibbi məlumatların pasiyentlə xəstəxana provayderi, hospitallar, tibb işçiləri arasında paylaşılmasını təmin etməkdir. Bu məqsədə nail olmaq üçün bir sıra təşəbbüslər irəli sürülmüşdür. Bu təşəbbüsün ilk addımı olaraq Avropa Kommisiyası 2012-2020-ci illəri əhatə edən eSəhiyyə fəaliyyət planı qəbul etmişdir [1].

eSəhiyyənin altseqmentlərini səhiyyə informasiya şəbəkələri, elektron tibbi qeydlər (ETQ) (ing. *Electronic Health Record, EHR*), onlayn eResept, elektron sağlamlıq kartı (ing. *Health Care Card*) kimi müxtəlif informasiya sistemləri təşkil edir.

Dünya səhiyyə provayderləri təhlükəsiz, effektiv, əlçatan və paylaşılan tibbi xidmətlər göstərmək məqsədi ilə EHR sistemlərinə böyük axınla miqrasiya edir. Dünya Səhiyyə Təşkilatına (ing. *World Health Organization, WHO*) daxil olan əksər regionlar pasiyentə yönəlik bu tibbi xidmətlərin formalaşmasına böyük investisiyalar qoyurlar.

Azərbaycanda elektron tibbi qeydlərin aparılması Azərbaycan Respublikası Prezidentinin 2005-ci il 21 oktyabr tarixli 1055 nömrəli sərəncamı ilə təsdiq edilən "Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafı üzrə 2005-2008-ci illər üçün Dövlət Proqramı (Elektron Azərbaycan)"nın həyata keçirilməsi üzrə Tədbirlər Planının 7.3.11 bəndinə [2] və Azərbaycan Respublikası Prezidentinin 2012-ci il 29 dekabr tarixli fərmanı ilə təsdiq edilmiş "Azərbaycan 2020: Gələcəyə baxiş" inkişaf konsepsiyasının 7.1 bəndinə əsasən [3] yaradılmış vətəndaşların "Elektron Sağlamlıq Kartı" sistemi (VESKS) konsepsiyası çərçivəsində həyata keçirilir [4].

Elektron tibbi qeydlərin aparılmasının bir çox üstünlükləri vardır. Lakin bu texnologiya informasiya təhlükəsizliyi risklərinin ciddi təsirinə məruz qalır, səhiyyədə gizliliyin pozulmasına yönəlmiş böyük təhdidlər yaradır. Bu səbəbdən dünya üzrə səlahiyyətli təşkilatlar tibbi verilənlərin gizliliyinin qorunmasına xidmət edən hüquqi baza yaratmağa cəhd edirlər.

Təqdim olunan məqalədə fərdi tibbi məlumatların təhlükəsizlik problemləri tədqiq olunur, onların qorunması üçün beynəlxalq təcrübə araşdırılır. Fərdi tibbi məlumatların təhlükəsizlik və gizlilik problemləri müəyyən olunur və onların həlli üçün təklif və tövsiyələr verilir.

II. ELEKTRON TİBBİ MƏLUMATLAR

Müasir dövrdə eSəhiyyənin eResept, pasiyent bioqrafiyası, smart hospitallar, mobil səhiyyə, teletibb, elektron tibb qeydləri, fərdi tibbi qeydlər kimi tətbiq ssenariləri vardır [5].

Elektron tibb qeydləri milli və regional eSəhiyyə fəaliyyət planının nüvəsi hesab olunur.

Elektron tibbi qeydlərə olduqca çox sayda təriflər verilmişdir. Bu təriflər sırasında rəsmi tərif ISO təşkilatı tərəfindən aşağıdakı kimi verilir [6]:

- *Elektron tibbi qeydlər (*ing. *Electronic Health Record, EHR)* − müalicə subyektinin sağlamlıq vəziyyəti ilə bağlı məlumatlar repozitorisidir. EHR pasiyentin tibbi məlumatlarını EHR-un səlahiyyətli istifadəçiləri arasında paylaşmağa imkan yaradır, və başlıca məqsədi fasiləsiz, effektiv və keyfiyyətli inteqrasiya olunmuş xidmətlər təqdim etməkdir.
- *Elektron tibbi qeydlər sistemi (*ing. *EHR system)* − elektron tibb qeydləri yaratmağa, istifadə etməyə, saxlamağa və əldə etməyə imkan yaradan komponentlər toplusudur.

Beynəlxalq nəşrlərdə "Elektron tibbi qeydlər" termini ilə yanaşı fərdi tibbi qeydlər (ing. *Personal Health Record, PHR*), Elektron müalicə qeydləri (ing. *Electronic Medical Record, EMR*) terminləri də istifadə olunur. Bu terminləri bir-birindən fərqləndirən cəhət tibbi məlumatların sahibliyi ilə əlaqələndirilir.

- *Fərdi tibbi qeydlər.* Şəxs tərəfindən yaradılan və idarə edilən tibbi qeydlərdir. Bu sistemə giriş əldə etməyə, onu sazlamağa, idarə etməyə yalnız xəstələrin hüququ olur. Xəstələr PHR sistemindən öz tibbi məlumatlarını saxlamaq və idarə etmək məqsədi ilə istifadə edir. PHR sisteminə məlumatlar müxtəlif mənbələrdən məsələn, klinikalar, evdə monitorinq cihazları və xəstələrin özləri tərəfindən daxil ola bilir.

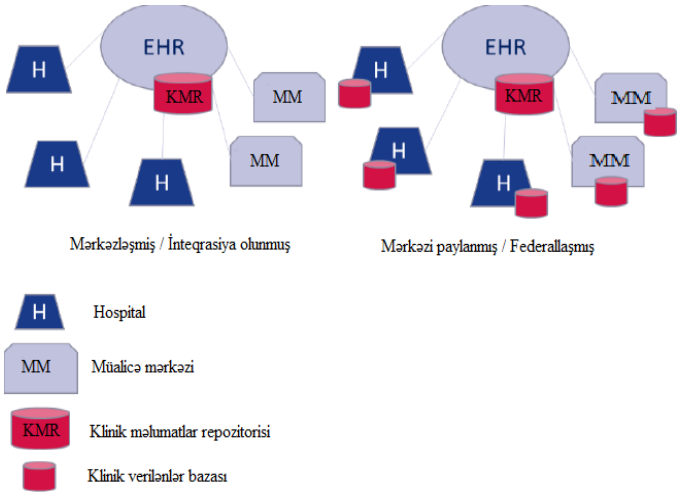
- *Elektron müalicə qeydləri.* Pasiyentlərin xəstəxana müəssisəsinə müraciəti zamanı stasionar və ambulator şəraitdə onlarla bağlı generasiya olunan qanuni qeydlərdir və tibb müəssisəsinin infrastrukturunda saxlanır. EMR tibb müəssisəsi daxilində tibbi xidmətlər göstərmək məqsədi ilə həkimlər tərəfindən yaradılır, istifadə edilir və idarə edilir.

Çox sayda onlayn PHR xidmətləri vardır. Məsələn, Google Health, HealthVault, ZebraHealth, OnlineMedicalRegistry, Medical ID Card və s. Bu xidmətlər sırasında ən məşhuru Google Health xidmətidir. Google Health 2008-ci ildə yaradılmışdır və 2011-ci ildə fəaliyyəti dayandırılmışdır. Google şirkətinin layihəni dayandırmasının səbəbi onun geniş tətbiq tapmaması ilə əlaqələndirilir.

EHR-in bir sıra arxitektur modelləri vardır (şəkil 1):

1. *Mərkəzləşmiş/tam inteqrasiya olunmuş model.* Burada bütün səlahiyyətlər bir təşkilatın öhdəsinə verilir. Bu təşkilatlar qismində Səhiyyə Nazirliyi və ya eSəhiyyə mərkəzi çıxış edə bilər. Burada EHR-ə cavabdehlik bu təşkilatların üzərinə düşür və bütün səhiyyə müəssisələri (hospitallar) onlarla birbaşa mübadilə aparırlar.
2. *Mərkəzi-paylanmış/federallaşmış model.* Burada EHR səhiyyə operatorunun infrastrukturunda, instansiyaları isə bir neçə səhiyyə təşkilatında yerləşir.
3. *Hibrid model.* Yuxarıdakı iki modelin birləşməsi.

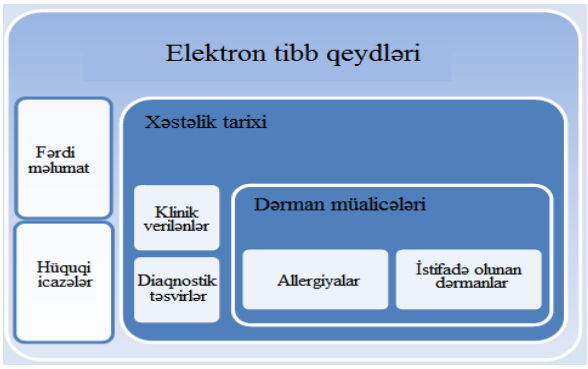
Avropa Birliyi, Birləşmiş Krallıq mərkəzləşmiş EHR arxitekturunu tətbiq edir, Almaniya, Danimarka, İspaniya servis-yönümlü arxitekturaya əsaslanan mərkəzi-paylanmış EHR arxitekturundan istifadə edir.



Şəkil 1. Elektron tibbi qeydlərin arxitektur modelləri

III. ELEKTRON TİBB QEYDLƏRİ SİSTEMİ

Elektron tibbi qeydlər sisteminə klinik tədqiqatlar, xəstəlik tarixi, müalicələr, allergiyalar, diaqnostik təsvirlər, hüquqi icazələr, pasiyent haqqında məlumat, qəbul edilən dərmanlar kimi məlumatlar daxil edilir (şəkil 2) [7].

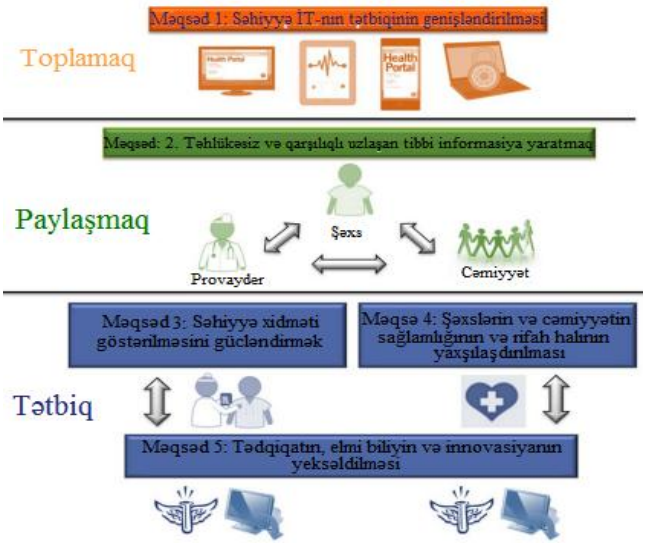


Şəkil 2. Elektron tibbi qeydlər

Elektron tibbi qeydlər sisteminə pasiyentin tibbi məlumatları müxtəlif tibb müəssisələrindən daxil olur [8].

Dünyada tətbiq olunan elektron tibbi qeydlər sistemləri aşağıdakı məqsədlərə xidmət edirlər [9] (şəkil 3):

- Tibbi informasiyanın şəxsin gizliliyini qorumaqla elektron şəkildə toplanmasını və paylaşılmasını təmin etmək;
- Səhiyyə xidmətlərini yaxşılaşdırmaq və xərcləri azaltmaq məqsədi ilə səhiyyə provayderləri, ümumi səhiyyə subyektləri, tədqiqatçılar və istifadəçilərin qarşılıqlı uzlaşan (ing. *interoperable*) informasiyadan istifadə etməsini təmin etmək üçün mühit yaratmaq.



Şəkil 3. Elektron tibbi qeydlər sisteminin məqsədi

IV. ELEKTRON TİBB QEYDLƏRİ SİSTEMLƏRİNİN SATANDARTLAŞDIRILMASI

Hazırda pasiyentin tibbi məlumatlarını toplayan sistemlər fraqmentlərlə, bir-biri ilə uzlaşmayan şəkildə mövcuddur. Bu isə pasiyentin öz tibbi məlumatlarını izləməsi və pasiyentin hər dəfə yeni səhiyyə provayderinə müraciətləri ilə əlaqəli verilənlərin sistemdə yenilənməsi prosesini çətinləşdirir. Bu problemi aradan qaldırmaq üçün dünyanın əksər standartlaşdırma təşkilatları bu sahədə standartlar işləyib hazırlamağa böyük səy göstərirlər [10].

Standart hər hansı proqram təminatı və yaxud aparat təminatı demək deyil, o müəyyən bir nümunədir texnologiya yaradıcıları ondan digər məhsullarla uzlaşa bilən məhsullar yaratmaq üçün istifadə edir. Aşağıdakı təşkilatlar eSəhiyyə sistemlərinin standartlaşdırılması sahəsində aktiv fəaliyyət göstərirlər:

DICOM (ing. *Digital Imaging and Communications in Medicine*) tibbi şəkillərin mübadiləsi standartını yaradan təşkilatdır.

CEN/TC 251 (ing. *European Committee for Standardization Technical Committee*) eSəhiyyə üçün standartlar yaradan təşkilatdır.

HL7 (ing. *Health Level Seven*) proqram tətbiqi səviyyəsində standartlar yaradan təşkilatdır.

ISO/TC 215 (ing. *ISO's Technical Committee*) elektron tibbi qeydlər üçün standartlar yaradır.

ISO/IEEE 11073 tibbi qurğuların interoperabelliyi üçün birgə standartlar yaradan təşkilatlardır.

V. ELEKTRON TİBBİ MƏLUMATLARIN TƏHLÜKƏSİZLİYİ

Səhiyyə infrastrukturuna olan kiberhücumların sayı durmadan artır [11]. 223 ölkənin Baş İnformasiya Rəhbərlərindən (Chief Information Officer, CIO), toplanmış sorğular əsasında KPMG (Kaiser Permanente Medical Group) təşkilatının hazırladığı “Səhiyyə və kiber təhlükəsizlik” adlı analitik materialında respondentlərin 13 faizi bildirir ki, səhiyyə təşkilatları kiber təhlükəsizliyin pozulması halları ilə hər gün rastlaşırlar. Səhiyyə infrastrukturuna zərərli proqramlar, botnetlər və s. kimi kiberhücumların da edilməsi halları çoxluq təşkil edir.

eTibb sistemlərinə olan kibertəhlükəsizlik insidentlərinin böyük sosial təsiri vardır. eTibb xidmətlərinə və infrastrukturlarına təsir göstərən kibertəhlükəsizlik insidentləri böyük fəsadların yaranmasına səbəb olur. 2014-cü ildə ENISA (European Union Agency for Network and Information Security) səhiyyəni kompüter infrastrukturunun təhlükəsizliyinin təmin olunması zəruri olan kritik sektorlar siyahısına daxil etmişdir [12]. ENISA 2015-ci ildə nəşr etdirdiyi “eTibdə təhlükəsizlik və elastiklik” adlı sənədində [13] eTibdə istifadə olunan bulud servislərinin, elektron tibb qeydlərinin, milli eTibb xidmətlərinin meydana gətirdiyi təhlükəsizlik problemlərinin geniş təsvirini vermişdir.

Elektron tibbi qeydlər sisteminin təhlükəsizlik problemlərinə aşağıdakıları aid etmək olar [7, 13]:

Sistemin əlçatanlığı. Fərdi tibbi məlumatlara səlahiyyətli şəxslərin fasiləsiz girişinin təmin olunması.

İnteroperabellik. eSəhiyyə infrastrukturu bir-biri ilə müxtəlif miqyasda qarşılıqlı əlaqələnmiş müxtəlif sistemlərdən ibarət ola bilir. Bu sistemlərdən effektiv istifadə olunması üşün onlar arasında interoperabelliyi təmin etmək lazımdır.

Girişə nəzarət və autentifikasiya. EHR mühitində tibbi məlumatların üçüncü tərəf şəxs və insayderlər (səhiyyə işçiləri) arasında paylaşılması verilənlərin təhlükəsizliyinə ciddi təsir göstərə bilir.

Verilənlərin tamlığı. Klinik məqsədlərlə saxlanan verilənlərin tamlığına zəmanəti təmin edir. Burada tibbi məlumatlarda yol verilən səhvlər şəxsin müalicə prosesinə ciddi təsir göstərə bilir.

Şəbəkə təhlükəsizliyi. eSəhiyyə aktivləri şəbəkənin təhlükəsizlik səviyyəsindən ciddi asılıdır. Burada şəbəkə insidentlərinin əksər hissəsi eSəhiyyə infrastrukturunda reallaşa bilir.

Verilənlərin itməsi. Verilənlərin itməsinə əsasən pasiyentin klinik məlumatlarına icazəsiz giriş cəhdləri səbəb olur.

Gizlilik. Fərdi tibbi məlumatların qanunvericilik aktları ilə qorunması məsələlərini əhatə edir.

Standartlaşma, uyğunluq və inam. eSəhiyyə infrastrukturunda təhlükəsizliyin əldə olunmasının yollarından biri interoperabellik vasitələrinin yaradılmasıdır. Avropa Komissiyası bu problemi HITCH və ANTILOPE layihələri vasitəsi ilə həll edir.

Sərhədlərarası insident. Sərhədlərarası eSəhiyyə xidmətləri xüsusən Avropada mühüm əhəmiyyət kəsb edir. Bu problem tibbi məlumatların sərhədlərarası səhiyyə sistemlərinə ötürülə bilməsi imkanlarını əhatə edir.

İnsidentin idarə edilməsi. Təhlükəsizlik insidentləri insan səhvləri, təbiət hadisələri, bədniyyətli əməllər (DDoS hücumu, MITM (ing. *Man-in-the-middle*) hücumları və s.), sistem sıradançıxmaları səbəbindən baş verə bilir. Bu səbəbdən eSəhiyyə təşkilatları insidentə cavabvermə imkanlarına malik olmalıdır.

Burada bir tərəfdən sistemin təhlükəsizliyi digər tərəfdən tibbi məlumatların təhlükəsizliyi təmin olunmalıdır. Sistemin təhlükəsizliyi adətən autentifikasiya, girişə nəzarət, şifrləmə və s. texnologiyalarından istifadə etməklə təmin edirlər.

Gizlilik və konfidensiallıq fərqli terminlərdir, gizlilik fiziki obyektə, konfidensiallıq informasiya materialına aid edilir.

Dünyada tibbi məlumatların gizliliyi aşağıdakı qanunlarla qorunur:

İnsan Hüquqları haqqında Ümumi Bəyannamə

İkinci dünya müharibəsində törədilən vəhşiliklərə birbaşa cavab məqsədi ilə Birləşmiş Millətlər Baş Assambleyası tərəfindən 1948-ci ildə qəbul olunmuşdur. Bu sənəd icrası məcburi olan beynəlxalq qanunvericilik aktıdır, insan hüquqlarının qorunmasına xidmət edən ötuz maddədən ibarətdir. Gizlilik məsələsi bəyannamənin 12-ci maddəsində yer almışdır və aşağıdakı kimidir [14]:

Heç bir kəs nə onun şəxsi həyatına, ailəsinə, evinə və yazışma sirrinə olan qeyri-qanuni müdaxiləyə, nə də ki, şərəf və reputasiyasına hücumlara məruz qala bilməz. Hər bir kəsin bu

növ müdaxilələrə və ya hücumlara qarşı qanunla müdafiə olunmaq hüququ vardır.

İnsan Hüquqları üzrə Avropa Konvensiyası.

Avropa Şurası tərəfindən 1950-ci ildə qəbul olunmuşdur və bütün Avropa Şurası ölkələrini bu konvensiyaya riayət etməyə məcbur edir [15]. Ümumi Bəyannamədən fərqli olaraq şəxs konvensiyaya görə hüquqlarının pozulduğunu aşkarladıqda İnsan Hüquqları üzrə Avropa Məhkəməsinə (ing. *European Court of Human Rights*) müraciət edə bilir.

Konvensiyanın 8-ci maddəsi şəxsi və ailə həyatı ilə bağlı hüquqları tənzimləyir:

Hər bir kəsin özünün şəxsi və ailə həyatını, mənzilini və yazışma sirrini müdafiə etmək hüququ vardır.

Fərdi məlumatların avtomatlaşdırılmış emalı zamanı fiziki şəxslərin *mühafizəsi haqqında konvensiya.*

108-də adlandırılan konvensiya İnsan Hüquqları üzrə Avropa Kommisiyasının 8-ci maddəsinə əsaslanır və hər bir şəxsin millətindən və yaşayış yerindən asılı olmayaraq fərdi məlumatlarının emalı prosesində gizliliyini qorumaq hüququnun olduğunu təmin edir [16]. Konvensiya dünyada avtomatlaşdırılmış emalın meydana gətirdiyi gizlilik məsələsinə ünvanlanan birinci qanunvericilik aktıdır. Konvensiyada əsasən fərdi məlumatların emalı prinsipləri şərh olunur. Tibbi verilənlər baxımından konvensiya tibbi məlumatların emalını qanunsuz hesab edərək onu qadağan edir.

Fərdi məlumatların emalı zamanı fiziki şəxslərin müdafiəsi və bu verilənlərin sərbəst ötürülməsi haqqında 95/46/EC direktivi.

95/46/EC direktivi tibbi məlumatları xüsusi kateqoriyalı verilənlər qrupuna aid edir və aşağıdakı tərifləri irəli sürür [17]:

Fərdi məlumat identifikasiya olunan fiziki şəxslə bağlı istənilən informasiyadır; şəxsin identifikasiya nömrəsinə və ya onun fiziki, psixoloji, mədəni, sosial faktorlarına istinadən birbaşa və ya bilavasitə identifikasiya oluna bilən şəxs identifikasiya olunan şəxs adlanır (Maddə 2) .

Fərdi məlumatların qorunması üzrə Direktivin 8-ci maddəsi şəxsin tibbi xarakterli fərdi məlumatlarını xüsusi kateqoriyalı verilənlər sinfinə aid edir və onların emalını qadağan edir:

Üzv Dövlətlər şəxsin irqi və etnik mənsubiyyəti, siyasi fikirləri, dini və fəlsəfi inancları, həmkarlar ittifaqına üzvlük və başqa fərdi məlumatlarının emalını, o cümlədən, şəxsin sağlamlığı və seksual həyatı ilə bağlı verilənlərin emalını qadağan etməlidir (Maddə 8).

Tibbi məlumatların qorunması üzrə 5 nömrəli tövsiyə.

Avropa Şurasının Nazirlər Kabinetinin qərarı ilə 1997-ci ildə qəbul edilmişdir, avtomatlaşdırılmış sistemlərdə toplanan tibbi məlumatların tənzimlənməsi prinsiplərini müəyyən edir. Bu sənəd səhiyyə sektorunda geniş kompüterləşdirmə həyata keçirildiyi səbəbindən yaradılmışdır. Burada qeyd edilir ki, gizliliyi təmin edən qanunvericilik aktları bütün növ tibbi məlumatlara tətbiq olunmalıdır, tibbi məlumatların toplanmasını və emalını yalnız səhiyyə işçiləri həyata keçirə bilər [18]

Avropada pasiyentlərin hüquqlarının təmin olunması üzrə deklarasiya.

Dünya Səhiyyə Təşkilatı tərəfindən 1994-cü ildə qəbul edilmişdir, tibbi məlumatların gizliliyinin təmin olunması üçün pasiyentlərin, səhiyyə işçilərinin və səhiyyə müəssisələrinin hüquqlarını, səlahiyyətlərini və öhdəliklərini müəyyən edir. Deklarasiyada əsasən "Hər kəsin özü-müəyyən etmək hüququ vardır", "Hər kəsin özünün gizliliyini qorumaq hüququ vardır" kimi məsələlər diqqət mərkəzinə alınır. Deklarasiyanın 4-cü maddəsində qeyd edilir:

4.1. Pasiyentin sağlamlıq vəziyyəti, tibbi vəziyyəti, diaqnozları, proqnozları, müalicələri və fərdi xarakterli digər bütün məlumatları, hətta vəfatından sonra da konfidensial saxlanmalıdır.

4.2. Konfidensial informasiya yalnız pasiyentin razılıq verdiyi halda açıqlana bilər.

4.3. Pasiyentin identifikasiya olunan bütün məlumatları qorunmalıdır.

4.4. Pasiyentlərin özlərinin diaqnozları və müalicələri ilə bağlı tibbi məlumatlarına giriş əldə etmək hüquqları vardır.

4.5. Pasiyentlərin özlərinə aid fərdi və tibbi məlumatların yalnış, natamam, müəmmalı və ya köhnəlmiş olduğunu, və ya diaqnozlarına və müalicələrinə uyğun olmadığını müəyyən etdikdə onların düzəliş edilməsini, tamamlanmasını, ləğv edilməsini, aydınlaşdırılmasını, yenilənməsini tələb etmək hüququ vardır.

4.6. Pasiyentin şəxsi və ailə həyatına heç bir müdaxilə olmamalıdır. Xüsusi halda pasiyent müdaxiləyə icazə verdikdə, bu müdaxilənin pasiyentin diaqnozları və müalicəsi üçün vacib olduğu əsaslandırılmalıdır.

İnformativ sənəd: Müştəri hüquqlarının müdafiəsi.

Beynəlxalq Telekommunikasiya Birliyi (ing. *International Telecommunication Union, ITU*) tərəfindən 2012-ci ildə dərc edilmişdir. Təlimatda onlayn mühitdə fərdi məlumatlara giriş qaydalarının tənzimlənməsi prinsipləri verilir [19]. Burada qeyd edilir ki, gizlilik məsələləri sadəcə açıq şəbəkə üzərindən ötürülən fərdi məlumatların təhlükəsizliyi demək deyil. O, həmçinin verilənlərin toplanması, saxlanması və ondan istifadə olunması, şəxsin onun fərdi məlumatlarının başqaları tərəfindən nə vaxt, necə, hansı məqsədlərlə paylaşması səbəblərini müəyyən etmək hüquqlarının olması ilə də əlaqələndirilir.

Qeyd edək ki, pasiyentin xəstəlik tarixinin yaradılması tibb praktikası başlandığı andan mövcud olmuşdur. Bu dövrlərdə həkim-pasiyent münasibətlərinin gizliliyinin saxlanmasına olan inam qədim Hipokrat Andı ilə təmin edilirdi. Andiçmə gizliliklə bağlı aşağıdakını şərh edir:

Müalicə prosesində və ya heç bir halda kənara çıxmamalı olan müalicədən kənar şəxsin həyatı ilə bağlı gördüklərimi və eşitdiklərimi, bu informasiyanın yayılmasını qalmaqal hesab edərək onu özümdə saxlayacağam.

Hipokrat andının əsas ideyaları tibbi məlumatların gizliliyi ilə bağlı müasir deklarasiyaların və qanunların mətninə transformasiya edilmişdir.

VI. DÜNYA ÖLKƏLƏRİNİN FƏRDİ TİBBİ MƏLUMATLARIN GİZLİLİYİNİN QORUNMASI ÜZRƏ QANUNVERİCİLİK AKTLARI

Dünya ölkələrinin əksəriyyətində dövlət orqanları tərəfindən fərdi məlumatların toplanması və emalı qaydalarını tənzimləyən gizliliyin qorunması üzrə qanunvericilik aktları vardır. Bu qanunlar adətən informasiyanın gizliliyinin qorunması məsələlərini əhatə edir.

Xüsusi olaraq tibbi məlumatların gizliliyinin qorunmasına və hətta EHR sistemlərində gizliliyin və pasiyentlərin hüquqlarının təmin olunmasına xidmət edən qanunvericilik aktları yalnız bir neçə ölkədə mövcuddur. eSəhiyyə sahəsində gizlilik üzrə spesifik qanunvericilik aktları olan ən məşhur ölkələr sırasına Braziliya, Amerika Birləşmiş Ştatlarını aid etmək olar.

Braziliya. Braziliyada milli elektron tibb qeydləri sistemi 2014-cü ildən tətbiq olunur. Bu ölkədə şəxsin tibbi məlumatlarının gizliliyinin qorunması, telekommunikasiya mühitində gizlilik üzrə hüquqların təmin olunması, həkim-pasiyent münasibətlərinin gizliliyinin qorunması Habeas Data qanunu ilə tənzimlənir.

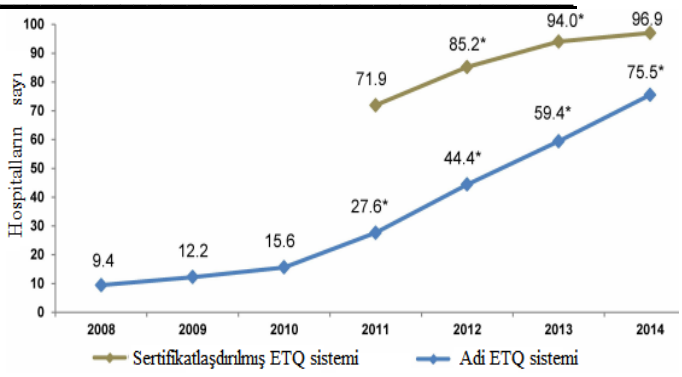
Habeas Data – vətəndaşların şəxsi hüquqlarının və azadlıqlarının müdafiəsi üçün yeni hüquqi sənəddir, ilk dəfə 1999-cu ildə Braziliya Konstitusiyasında təsbit edilmişdir və hazırda bir çox ölkələrdə istifadə olunur. Əksər ölkələrdə olduğu kimi, Braziliyada da EHR sistemlərində şəxsin fərdi tibbi məlumatlarının qorunmasına xidmət edən xüsusi qanunvericilik aktı qəbul edilməmişdir. Braziliyada tibbi məlumatlar Federal Tibb Şurası (ing. *Federal Medical Council, CFM*) tərəfindən idarə edilir.

ABŞ. Fərdi tibbi məlumatların gizliliyini təmin etmək üçün ABŞ dövləti 1996-cı ildə “Sağlamlıq sığortasının daşınaqlığı və hesabatlılığı haqqında” qanunvericilik aktını (ing. *Health Insurance Portability and Accountability Act, HIPAA*), 2003-cü ildə isə “İqtisadi və klinik səhiyyə üçün tibbi informasiya texnologiyası haqqında” (ing. *Health information technology for economic and clinical health, HITECH*) qanunvericilik aktını qəbul etmişdir. Bu qanunlar fərdi tibbi məlumatları emal edən subyektləri bu məlumatların gizliliyini və təhlükəsizliyini təmin etməyə və pasiyentlərin məlumatları təhlükə ilə qarşılaşdıqda onları məlumatlandırmağa məcbur edir.

ABŞ-da fəaliyyət göstərən Tibbi İnformasiya Texnologiyaları üzrə Milli Koordinator Ofisinin 2015-ci ildə dərc etdirdiyi analitik materialda aparılan statistik analizə görə HIPAA və HITECH sənədlərində irəli sürülən təhlükəsizlik tələblərinə uyğun sertifikatlaşdırılmış Elektron Tibb Qeydləri sistemlərinin (ing. *certified EHR*) istifadəsi daha çox üstünlük təşkil edir [20] (şəkil 4).

ABŞ-da İnsan Hüquqları İdarəsi HIPAA aktında tibbi məlumatların qorunmasını gücləndirmək məqsədi ilə bir sıra dəyişikliklər etmişdir.

ABŞ-da tibbi qeydlərin gizliliyinin təmin olunması üzrə şəxsin hüquqlarını qoruyan konstitusion hüququ nəzərdə tutulmamışdır.



Şəkil 4.

Azərbaycan. Azərbaycan Respublikasında şəxsin fərdi tibbi məlumatları Vətəndaşların Elektron Sağlamlıq Kartı sistemində toplanır (VESKS). VESKS sistemi Səhiyyə Nazirliyi tərəfindən tətbiq olunan elektron informasiya sistemidir. Sağlamlıq Kartı sisteminə daxil edilən məlumatlar Səhiyyə Nazirliyinin İnformasiya Mərkəzində cəmləşdirilir.

Sağlamlıq kartı sistemində olan məlumatlar (xəstəlik tarixi, müayinə, müalicə, cari istifadə edilən dərman preparatları, peyvəndlər, gələcəkdə tibbi sığorta və s.) şəxsə operativ və dəqiq müayinə olunmaq imkanı yaradır. Azərbaycanda şəxsin fərdi tibbi məlumatlarının gizliliyinin qorunması fərdi məlumatların qorunması üzrə mövcud qanunvericilik aktları ilə təmin olunur.

Ölkədə şəxsin fərdi tibbi məlumatlarının qorunması üçün xüsusi bir qanunvericilik aktı qəbul olunmamışdır.

VII. TƏKLİFLƏR

- İstifadəçilərin fərdi tibbi məlumatlarının gizliliyini təmin etmək üçün xüsusi mexanizmlərdən istifadə olunmalıdır.
- Pasiyentin sağlamlıq vəziyyəti haqqında dolğun informasiya formalaşdırmaq üçün ayrı-ayrı sistemlər arasında qarşılıqlı uzlaşma (interoperabellik) təmin olunmalıdır.
- İnteroperabelliyi təmin etmək üçün təhlükəsizlik standartlarının səhiyyə sistemlərində geniş tətbiqi təmin olunmalıdır.
- Fərdi məlumatların qorunması üzrə qanunvericilik aktları tibbi məlumatları xüsusi kateqoriyalı verilənlər qrupuna aid edir və onların toplanmasını və emalını qadağan edir. Məsələn, “Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data” direktivasının 8-ci maddəsi. Lakin şəxsin fərdi tibbi məlumatlarının toplanması eSəhiyyənin başlıca tələbidir.

Bu tələb direktivanın 8-ci maddəsinin pozulmasına gətirib çıxarır, bu isə öz növbəsində insan hüquqlarının pozulması deməkdir. 8-ci maddəsində boşluğun olduğunu nəzərə alaraq bu maddədə dəyişikliklərin edilməsi zəruri olardı.

NƏTİCƏ

Dünyada qurulmuş eSəhiyyə sistemlərində pasiyentin bir tibb müəssisəsində saxlanan elektron tibbi məlumatlarını digər hospitallardan əldə etmək böyük problemlər yaradır. Bu gün bu problem Azərbaycan Respublikasında da qabarıq şəkildə öz

əksini tapır. Burada hər bir səhiyyə provayderinin özünün şəxsi quraşdırılmış sistemi vardır və bu sistemlə digər provayderlərin təqdim etdiyi sistemlər arasında interoperabellik təmin edilməmişdir.

Ayrı-ayrı fraqmentlərlə olan və bir-biri ilə qarşılıqlı uzlaşmayan şəkildə mövcud olan pasiyent məlumatları, pasiyenti öz tibbi məlumatlarını izləməsində çətinliklərlə qarşılaşdırır. Bu məlumatlara anlaşıqlı formatda birbaşa girişi təmin etmək üçün standartların işlənməsi zəruri olardı.

ƏDƏBİYYAT

[1] eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century, European Commission, 2012, 14 p.

[2] Azərbaycan Respublikasında rabitə və informasiya texnologiyalarının inkişafı üzrə 2010-2012-ci illər üçün Dövlət Proqramı (Elektron Azərbaycan), 2010, 13 s.

[3] Azərbaycan 2020: Gələcəyə baxiş” inkişaf konsepsiyası, 2012, 39 s.

[4] Elektron sağlamlıq kartı” sisteminin tətbiqi Qaydaları” nın təsdiq edilməsi haqqında Azərbaycan Respublikasi Nazirlər Kabinetinin qərar, 2005, 13 s.

[5] Security and Resilience in eHealth Security Challenges and Risks, ENISA, 2015, 48 p.

[6] ISO/TR 20514:2005. Health informatics -- Electronic health record -- Definition, scope and context, 2005, Edition 1, 27 p.

[7] Standards and eHealth, ITU-T technology watch report, 2011, 20 p.

[8] Electronic Health Records: Manual for Developing Countries, World Health Organization, 2006, 78 p.

[9] Federal Health Information Technology Strategic Plan 2011 – 2015, Office of the National Coordinator for Health Information Technology (ONC), 2011, 80 p.

[10] E-health standards and interoperability, ITU-T technology watch report, 2012, 24 p.

[11] Health care and cyber security: Increasing threats require increased capabilities, KPMG, 2015, 8 p.

[12] Methodologies for the identification of Critical Information Infrastructure assets and services Guidelines for charting electronic data communication networks, ENISA, 2014, 35 p.

[13] Security and Resilience in eHealth Security Challenges and Risks, ENISA, 2015, 48 p.

[14] Universal Declaration of Human Rights, United Nations General Assembly, 1948, 8 p.

[15] European Convention on Human Rights, 1950, Council of Europe, 55 p.

[16] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981, No. 108, 9 p.

[17] Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, European Parliament and Council, 1995, 33 p.

[18] Recommendation No. R (97) 5 on the Protection of Medical Data, Council of Europe, Committee of Ministers, 1997, 13 p.

[19] Briefing note on ITU: Consumer protections, ITU, 2012, 32 p.

[20] Adoption of electronic health record systems among U.S. NonFederal Acute Care Hospitals: 2008-2014, ONC Data Brief, no. 23, 2015, 10 p.