Elektron Fərdi Tibbi Məlumatların İnformasiya Təhlükəsizliyi Problemləri

Məsumə Məmmədova
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
masuma.huseyn@iit.ab.az

Xülasə– **Elektron tibdə fərdi məlumatların qorunması problemləri tədqiq edilmişdir. Beynəlxalq təcrübədə pasiyentlərin sağlamlıq vəziyyətləri haqqında məlumatların informasiya təhlükəsizliyinin təmin edilməsinə yanaşmalar göstərilmiş, fərdi tibbi məlumatların spesifik xüsusiyyətləri qeyd edilmiş, tibbi informasiya sistemlərində tibbi və həkim sirlərinin konfidensiallığı və təhlükəsizliynə potensial təhlükələr göstərilmişdir. Azərbaycanda fərdi tibbi məlumatların qorunmasının hüquqi əsasları nəzərdən keçirilmiş və Respublikada fərdi tibbi məlumatların qorunmasını tənzimləyən normativ-hüquqi sənədlərin işlənməsinin məqsədəmüvafiqliyi əsaslandırılmışdır.**

Açar sözlər– fərdi tibbi məlumatlar, informasiya təhlükəsizliyi, konfidensiallıq, həkim sirri, təhlükələr.

I. GİRİŞ

İctimai həyatın praktiki olaraq bütün sahələrininin informasiyalaşdırılması ildən-ilə daha da intensiv olaraq tibbi sferaya nüfuz edir.

Tibbi qeydlərə fərdi-mərkəzləşdirilmiş yanaşma və pasiyentlərin elektron tibbi kartlarının (ETK) yaradılması ilə ifadə olunan tibbin kompüterləşdirilməsinə yeni konseptual yanaşmalar, tibbi sənədlərin elektron analoqlarının işlənməsi, istənilən tibbi qeydlər çoxluğuna və tibbi məlumatların onların mənbəyindən ayrılması hesabına pasiyentin müayinəsinin ilkin nəticələrinə effektiv əlyetərlilik imkanlarının yaranması, elektron sənəd dövriyyəsinə keçid hər bir insanın sağlamlıq vəziyyəti haqqında məlumatların müxtəlif səviyyəli xüsusiləşdirilmiş informasiya emalı mərkəzlərində inteqrasiyası ilə ifadə olunan səhiyyənin modernləşdirilməsi istiqamətlərini müəyyən etmişdir.

ETK-infrastrukturunun reallaşdırılması imkanını müəyyən edən informasiya texnologiyalarının inkişaf səviyyəsi aşağıdakıların genişlənməsinə səbəb olmuşdur: a) qeydiyyata alınmış tibbi məlumatların yerləşdiyi ərazidən və vaxtdan asılı olmadan tibbi xidmətlərin əlyetərliyi; b) informasiyanın surətinin çıxarılması, təkrar istifadəsi və yayılması üzrə texniki imkanlar; c) kütləvi kommunikasiya vasitələrinə çıxış. Lakin göstərilən müsbət dəyişikliklərin fonunda fərdi tibbi məlumatların (FTM-ın) sürətli emalına və inteqrasiyasına imkan verən müasir effektiv vasitələr, şəxsiyyətin hüquqlarına və qanuni maraqlarına təhlükə yaradan bədniyyətli tərəfindən də müvəffəqiyyətlə istifadə olunur. Odur ki, elektron tibbin (e-tibb) həyata keçirilməsi şəraitində fərdi məlumatların informasiya təhlükəsizliyinin (İT) təmin edilməsi məsələsi hal-hazırda kifayət qədər aktualdır.

II. TİBBİ MƏLUMATLARIN TƏHLÜKƏSİZLİYİ VƏ KONFİDENSİALLIĞI PROBLEMLƏRİ: BEYNƏLXALQ TƏCRÜBƏ

Beynəlxalq təcrübə göstərir ki, FTM-ın konfidensiallığının və təhlükəsizliyinin lazımi səviyyədə təmin olunmaması e-tibbin effektiv inkişafı yolunda başlıca maneədir. Belə ki, insanların qapalı fərdi məlumatlarına əlçatanlığı olan tibb müəsissələri bütün tibbi məlumatların konfidensiallığı və təhlükəsizliyinə zəmanət verməlidirlər. İnformasiya daşıyıcısından asılı olmayaraq, konfidensial olan istənilən FTM, həm informasiyanın subyektləri olan pasiyentlər, həm də peşəkar tibbi xidmət göstərənlər – tibbi personal tərəfindən etibarlı formada idarə edilməlidir. Giriş hüququ olan hər bir tərəf əmin olmalıdır ki, onun əsaslandığı məlumatlar səlahiyyətli şəxslər tərəfindən daxil edilmişdir.

Tibb müəssisəsində (TM-də) vahid informasiya fəzasının yaradılmasını təmin edən tipik tibbi informasiya sistemi (TİS) sənəd dövriyyəsi və resursların qeydiyyatından başlamış elektron xəstəlik tarixçəsinin, pasiyent haqqında kliniki qeydlərin, tibbi avadanlıqla inteqrasiyanın yerinə yetirilməsinə qədər təşkilatın müalicə-diaqnostika proseslərinin və onun fəaliyyətinin digər sahələrinin təşkilini avtomatlaşdırır və optimallaşdırır, TM-in bütün xidmətlərinin fəaliyyətinin informasiya təminatını, intellektual dəstəklənməsini, eləcə də idarəedici və həkim qərarlarının qəbul edilməsinin dəstəklənməsini yerinə yetirir.

TM-in fəaliyyətinin dəstəklənməsi üçün nəzərdə tutulmuş TİS digər proqram məhsullarından hər şeydən əvvəl onunla fərqlənir ki, orada fərdi və konfidensial informasiya saxlanılır və emal edilir.

Hüquqi olaraq, pasiyentlər haqqında tibbi məlumatlar giriş məhdudlaşdırılmış həkim sirri hesab olunan informasiyaya aiddir və hər bir ölkədə fəaliyyət göstərən qanunvericiliklə tənzimlənir. Bununla əlaqədar olaraq, TİS-in işlənməsi zamanı informasiyanın, eləcə də bütövlükdə informasiya sisteminin təhlükəsizliyinin təmin edilməsi üçun bir sıra tədbrilər mütləq nəzərə alınmalı və yerinə yetirilməlidir, əks təqdirdə bu TİS-in istifadəsi qanunsuz hesab olunur.

TİS-ə giriş əldə edən TM-nin istənilən istifadəçisi daxil etdiyi, istifadə etdiyi və digər istigadəçilərə ötürdüyü məlumatın konfidensiallığının təmin edlməsinə görə tam (mənəvi, inzibati və cinayət) məsuliyyət daşıyır. Deməli, məlumatların təhlükəsizliyinin və konfidensiallığının təmin olunması müasir TİS-ə qoyulan əsas tələblərdən biridir və onun informasiya-kommunikasiya və hesablama sistemlərində reallaşdırılması aktual məsələ hesab olunur [1–4].

FTM-in konfidensiallığı fərdi məlumatlara giriş əldə etmiş TM-lərin pasiyentin icazəsi olmadan fərdi məlumatları açmağa və yaymağa hüququ olmaması ilə ifadə olunur. FTM-ın informasiya təhlükəsizliyi dedikdə, elektron media və istənilən digər texniki çatdırılma və kommunikasiya vasitələri ilə ötürülən və ya dəstəklənən fərdi identifikasiya olunmuş tibbi məlumatların daxili və xarici təhlükələrdən mühafizə olunması, eləcə də məlumatların sızma, oğurlanma, itirilmə, icazəsiz məhv edilmə, təhrif olunma, modifikasiya edilmə (saxtalaşdırma), surətinin çıxarılması və bloklamadan qorunma vəziyyəti nəzərdə tutulur.

Dünya təcrübəsinə əsasən, e-tibb sistemində İT aşağıdakıları təmin etməlidir: 1) konfidensiallıq (həkim sirrinə riayət olunması və fərdi məlumatların qorunması), yəni səlahiyyəti olmayan istifadəçilərin informasiyanı icazəsiz ələ keçirməsindən qorunma; 2) verilənlərin mübadiləsi zamanı informasiyanın etibarlılığı və tamlığına zəmanət və informasiyanın icazəsiz dəyişdirilməsindən qorunma ilə ifadə olunan tamlıq; 3) səlahiyyətli istifadəçilərin informasiyaya və zərurət yarandıqda onunla bağlı olan aktivlərə əlyetərliyinin mümkünlüyü, eləcə də TİS-in sistemin qırılması və ya sorğularla həddən artıq yüklənməsi zamanı davamlılıq rejiminə malik olması ilə müəyyən olunan əlyetərlik [5–7].

Avropa ölkələri, ABŞ, Kanada, Avstraliya və digər ölkələrdə səhiyyənin modernləşdirilməsində əsas cərəyan olan fərdi-mərkəzləşdirilmiş yanaşma konsepsiyası “tibbi məlumatlara giriş nə qədər asandısa, tibbi xidmətin keyfiyyəti bir o qədər yüksəkdir” prinsipinə əsaslanır. Bu prinsip, bir tərəfdən, pasiyentə (xəstəyə) operativ, ixtisaslı tibbi yardım göstərmək üçün onun FTM-na girişin sadələşdirilməsini nəzərdə tutur, digər tərəfdən isə, bu ölkələrdə İT rejiminə qanunvericiliklə tənzimlənən standartlarla təmin olunmuş ciddi tələblər irəli sürür. Belə ki, informasiyanın qorunması haqqında Avropa direktivinə (EU Data Protection Directive 1995) əsasən, Avropa Şurasına üzv ölkələr səviyyəsində vahid Avropa məkanında qanunvericiliyin harmonizasiyası təmin olunub və hal-hazırda bir çox müalicə müəssisələri xəstənin fərdi tibbi məlumatlarına giriş hüququna malikdirlər [8]. TİS də daxil olmaqla, informasiya sistemlərində (İS) İT rejiminin təmin olunması təcrübəsi Beynəlxalq Standartlaşdırma Təşkilatının Azərbaycanda da qəbul edilmiş ISO 27001 standartının əsasını təşkil edir [9].

1996-cı ildə ABŞ-da qəbul edilmiş tibbi sığortanın vərəsəliliyi və hesabatlılığı haqqında Qanun (Health Insurance Portability and Accountability Act - HIPAA) şəxsi tibbi məlumatın konfidensiallığı və təhlükəsiz mübadiləsi, onun icazəsiz istifadədən mühafizəsi qaydalarını müəyyən edən ABŞ Federal Qanunudur. Qanun kağız, eləcə də elektron daşıyıcılarda saxlanan FTM-a aiddir [10]. HIPAA pasiyentə qulluq göstərilməsində iki vacib ideyaya əsaslanır: şəxsi həyatın toxunulmazlığı və konfidensiallıq. Şəxsi həyatın toxunulmazlığına pasiyentin aşağıdakı hüquqları daxildir: a) onun tibbi vəziyyəti haqqında kimin və nəyi bilməsinin məhdudlaşdırması; b) pasiyent haqqında məlumatlara girişi olanlar və onların məqsədləri haqqında məlumatın əldə edilməsi (şəffaflıq prinsipi).

III. ELEKTRON FƏRDİ TİBBİ MƏLUMATLARIN SPESİFİK XÜSUSİYYƏTLƏRİ

FTM-ın təhlükəsizliyi sisteminin işlənməsi və TİS-nin informasiya təhlükəsizliyinin optimal rejiminin seçilməsi zamanı təhlükəsizlik xarakteristikalarının pozulması şərtlərinin və təhdidlərin uçotunun aparılmasının vacibliyi ilə yanaşı, həm də pasiyent haqqında məlumatın xüsusiyyətlərini, tərkibini, eləcə də məlumatı emal edən insanları nəzərə almaq lazımdır. Ədəbiyyat mənbələrinin [11–14] analizi pasiyentin FTM-nın aşağıdakı spesifik xüsusiyyətlərini müəyyən etməyə imkan verir:

1. Pasiyentin fərdi tibbi məlumatları onun haqqında qapalı şəxsi (konfidensial) məlumatlardır, həm də bu məlumatların hüquqi sahibi və sərəncamçısı tibb müəssisəsi və ya tibb işçisi deyil, pasiyentin özüdür. Bu, məlumatların subyekti kimi pasiyentlər və onların şəxsi məlumatlarını istifadə edənlər arasında münasibətlərin xüsusi formasının yaranmasını şərtləndirir. Beləliklə, məlumatların subyektinin fərdi qeydlərini və şəxsi həyati maraqlarını, həkim sirrini, peşəkar tibb işçilərinin məsuliyyət və maraqlarını, tədqiqatçıların və digər üçüncü şəxslərin qanuni maraqlarını eyni zamanda qorumaq lazımdır. Bu zaman bəzi FTM-lər yalnız tibbi xarakterli məlumatlardan deyil, eləcə də həkimin pasiyentlə ünsiyyəti nəticəsində yaranan müxtəlif xarakterli məlumatları ehtiva edən həkim sirrindən ibarət ola bilər.

2. Vaxtında tibbi yardım göstərilməsinin vacibliyi ilə əlaqədar olaraq tibbi sənədlərlə işləmək üçün ciddi vaxt reqlamentinin mövcudluğu. Məlumatın konfidensiallığı rejiminin gücləndirilməsi səbəbindən həkim üçün məlumatların əlçatan olmasının məhdudlaşdırılması nəticəsində bu göstəricinin pisləşməsi xəstənin sağlamlığı üçün, bəzi hallarda isə həyatı üçün təhlükə yarada bilər. Buna görə də İT-nin təmin olunmasının üç tərkib hissəsi arasında məntiqli kompromisin təmin edilməsi vacibdir: məlumatların konfidensiallığı, tamlığı və əlyetərliyi.

3. Pasiyentin FTM-ı müxtəlif TM-ləri arasında paylanmışdır ki, bu da sonuncuları aşağıdakı kimi fraqmentləşdirməyə imkan verir: a) pasiyenti birmənalı olaraq tanımağa imkan verən anket məlumatlarına əsasən; б) tibbi məlumatların tipi və xarakterinə görə (diaqnoz, sağlamlıq vəziyyəti haqqında məlumatlar, tövsiyələr və təyinatlar, aparılmış müalicə haqqında məlumat, laborator analizlərin nəticələri, statistik verilənlər və s.); c) saxlanma yerinə əsasən (qeydiyyat şöbəsi, doğum evi, USM, laboratoriya və s.), informasiya daşıyıcılarına görə (kağız, video, elektron fayllar) və FTM-ın müəllifinə görə (həkimlər və müxtəlif profilli müalicə müəssisələri, tibb bacısı, laborant və s.).

4. Pasiyentlərin müxtəlif coğrafi və funksional cəhətdən uzaq TM-lərindən alınmış FTM-ı, bir qayda olaraq, bir yerdə saxlanılmır. Bu o deməkdir ki, bir TM-də göstərilmiş tibbi xidmət haqqında məlumat avtomatik olaraq digər TM-də əlyetər deyil. Paylanmış məlumat fraqmentlərinin hamısı və ya böyük bir hissəsi birlikdə konfidensial məlumat hesab edilir və tibbi mılumatların ayrı-ayrı bölmələri sirr hesab olunmur. Buna görə də, İT-ni təmin etmək üçün tibb mütəxəssislərinin çoxsəviyyəli vəzifələri, səlahiyyətləri və prioritetləri nəzərə alınmaqla girişin idarə edilməsini təşkil etmək və onlara funksional təyinata müvafiq və identifikasiya olunma şərti ilə

informasiyanın bu və ya digər hissəsinə giriş imkanı vermək məqsədəuyğundur. Hal-hazırda TİS-i inkişaf etmiş ölkələrdə istifadə edilən bu yanaşma, hər bir istifadəçiyə onun səlahiyyətlərinə uyğun ETK-nın müəyyən fraqmentlərinə giriş hüququ verir.

IV. TİS-DƏ FƏRDİ MƏLUMATLARIN KONFİDENSİALLIĞI VƏ TƏHLÜKƏSİZLİYİNƏ POTENSİAL TƏHDİDLƏR

[11,14–17]-yə əsasən, fərdi tibbi məlumatlarla işləyərkən İT-nin müxtəlif təhlükələri yarana bilər. Bu, hər şeydən əvvəl, informasiyanın təhlükəsizliyi və konfidensiallığı təhlükələridir ki, onları da iki əsas kateqoriyaya bölmək olar:

I. Aşağıda göstərilənlər tərəfindən pasiyentlər haqqında məlumatlara icazəsiz girişə nəticəsində yaranan təşkilati təhdidlər: a) insayder – TM-nin işçisi; b) sistemi istismar edən autsayder və ya haker; c) TİS-nin həssaslığı; bu zaman qaydaları pozan şəbəkə resurslarına səhvən, təsadüfən və ya bəd niyyətlə (hakerlər, keçmiş əməkdaşlar, pasiyentlər və s.) icazəsiz giriş əldə edə bilər.

Hazırda informasiyanın konfidensiallığı və təhlükəsizliyi üçün ən böyük təhlükə yaradanlar daxili pozucular – insayderlərdir [18]. Bədniyyətli TM-nin adi tibb bacısından tutmuş yüksək ranqlı rəhbərinə kimi istənilən əməkdaşı ola bilər.

II. Verilənlər bazasına qanunsuz və ya təsadüfi giriş, məlumatın icazəsiz təhrif olunması, silinməsi, fiziki daşıyıcıların məhv edilməsi, faylların və ya zədələnmiş verilənlərin silinməsi zamanı avadanlıqların işində meydana gələn kəsilmələr, eləcə də məsafədən ehtiyat surətin çıxarılmasının gözlənilməz nəticələri, məlumatların icazəsiz dəyişdirilməsi (saxtalaşdırılması) və s. səbəbindən informasiya axını zəncirində pozulmalar nəticəsində yaranan texniki (sistem və fiziki) təhdidlər.

İT anlayışı hər bir konkret vəziyyət üçün xüsusiləşdirildiyinə görə, başqa sözlə, proqram əlavəsinin obyektinin xüsusiyyətlərini nəzərə aldığına görə, TM-lərində fərdi məlumatların qorunması sisteminin texniki tərkibinin formalaşdırılması üçün tipik TİS-nə ümumi və özəl təhdidlərin tərkibini müəyyən edən idarəedici və metodiki sənədlər işlənilir, eləcə də FTM-ın emalı zamanı məlumatın mühafizəsi üçün müvafiq tədbirlər görülür.

Beynəlxalq təcrübə göstərir ki, ETK infrastrukturunda şəxsi həyat üçün ən böyük təhlükə FTM-ın ikinci dəfə istifadə olunması ilə bağlıdır. Bu o hallara aiddir ki, müəyyən məqsədlər üçün açılan informasiya sonradan informasiya subyektinin icazəsi olmadan başqa məqsədlər üçün istifadə oluna bilər [14].

Tibb təşkilatlarında yaranan və saxlanılan böyük həcmli strukturlaşdırılmamış məlumatlar massivinin (Big Data) emalı unikal biliklərin əldə edilməsinə imkan verə bilər [15]. Belə ki, pasiyentlərin FTM-ı haqqında məlumat müxtəlif xəstəliklərin müalicəsi üçün yeni metodların işlənməsinə, statistikanın toplanıb analiz edilməsinə, yeni dərman preparatlarının farmakoloji təsirlərinin yoxlanılmasına, səhiyyənin keyfiyyətinin yaxşılaşdırılmasına, müxtəlif xəstəliklərin mümkün ola bilən yayılmasını proqnozlaşdırmağa və s. imkan verən kliniki, epidemioloji, ekoloji və digər elmi-tədqiqat işlərinin aparılmasında mühüm rol oynayır .

Sağlamlıq vəziyyəti haqqında məlumata giriş reqlamentə dövlət və özəl TM-ləri, sığorta şirkətləri, adminstratorlar, həkimlər, apteklər, işəgötürənlər, təhsil müəssisələri, elmi-tədqiqat institutları, data-mərkəzlər, akkreditasiya və standartlaşdırma üzrə təşkilatlar, laboratoriyalar, əczaçılıq şirkətləri, maliyyə agentləri və s. daxil edilir. Pasiyent haqqında məlumatın alınmasında maraqlı olan digər üçüncü qrup şəxslər qohumlar, tibb işçiləri, marketoloqlar, müxtəlif ictimai yardım proqramlarının nümayəndələri, kredit büroları və hüquq-mühafizə orqanlarıdır.

Bu zaman tibbi məlumatların istifadə edilməsi üçün vacib şərt fərdi məlumatların sahiblərinin göstərilməməsidir (fərdisizləşdirilməsidir). Lakin pasiyentlərin fərdisizləşdirilmiş FTM-nın sonrakı xoşniyyətli istifadəsi ilə yanaşı, bu məlumatlardan sui-istifadə edilməsi ehtimalı da mövcuddur. İnternetdə sosial şəbəkələrdən, geolokasiya servislərindən açıq informasiyanın, əczaçılıq şirkətlərindən və digər mənbələrdən alınmış verilənlərin mövcudluğu müxtəlif mənbələrdə olan məlumatların tutuşdurması yolu ilə ETK-ın anonimliyinə təhlükənin yaranmasına səbəb olur.

FTM-ın İT-nin pozulması: 1) özəl həyatın toxunulmazlığı, 2) şəxsi sağlamlıq və təhlükəsizlik, 3) maliyyə və kommersiya konfidensiallığı, 4) işəgötürənlər, sığorta şirkətləri tərəfindən əsassız ayrıseçkilik, 5) siyasi və karyera yüksəlişi üçün maneələr və s. toxunan kifayət qədər ciddi mənəvi, fiziki və maddi təsirlərə səbəb ola bilər.

V. FƏRDİ MƏLUMATLARIN MÜHAFİZƏSİ TƏDBİRLƏRİ

İnformasiya təhlükəsizliyi müvafiq hüquqi bazanın, təşkilati tədbilərin, proqram və texniki mühafizə vasitələrinin qarşılıqlı şəkildə əlaqələndirilmiş, kompleks istifadəsi hesabına təmin edilir: 1) Təşkilati (inzibati və prosedur) səviyyədə – təşkilatın təhlükəsizlik siyasəti ilə, bu siyasətdə təhlükəsizliyin məqsədi və ona çatmaq yolları formalaşdırılmışdır, prosedur səviyyədə - personal üçün İT üzrə təlimatların işlənməsi və yerinə yetirilməsi yolu ilə, eləcə də fiziki mühafizə tədbirləri ilə; 2) texniki (avadanlıq-proqram) səviyyədə – sınaqdan keçirilmiş və sertifikatlaşdırılmış həllər, standart əks-tədbirlər dəsti: ehtiyat surətlərin çıxarılması, antivirus və parol vasitəsi ilə mühafizə, şəbəkələrarası ekranlar, məlumatların şifrələnməsi və s. tətbiqi ilə təmin edilir.

Elektron sənədi göndərənin (müəllifin) identifikasiyası və sənədin məzmununun qorunması (informasiyanın təhrif olunmaması) üçün elektron imzadan istifadə olunur ki, o da elektron sənəddə dəyişikliklər edərkən öz qüvvəsini itirmiş olur. Məlumatların nəzərdən keçirilməsindən fərqli olaraq, onların düzəliş edilməsinə münasibətdə tələblər daha sərtdir, pasiyentin ETK-ı ilə iş seansı başa çatdıqdan sonra düzəlişlərin aparılması istisna olunur. Əks təqdirdə, əvvəllər yaradılmış və elektron imza vasitələri ilə imzalanmış mətnə düzəlişlər edən zaman əvvəlki qeydlər, sonradan ETK-ı nəzərdən keçirən TM-lərinin əməkdaşları üçün əlçatmaz olmaq şərti ilə saxlanılmalıdır, başqa sözlə, əməliyyatların protokollaşdırılması və auditdən ibarət olan hesabatlılıq mexanizmi reallaşdırılmalıdır [5–9]. Bu zaman, eləcə də, FTM-ın yayılmasının mənəvi-etik aspektlərinə və konfidensiallığın pozulması və vətəndaşa dəymiş ziyana görə hüquqi cəhətdən təsbit edilmiş məsuliyyətə diqqət etmək lazımdır [19].

VI. AZƏRBAYCANDA FTM-IN QORUNMASININ HÜQUQİ ƏSASLARI

Son iki onillik ərzində Azərbaycan Respublikasında (AR) informasiyalaşdırma proseslərinə əhəmiyyətli diqqət yetirilir. Lakin digər fəaliyyət sahələrinin fonunda səhiyyə milli iqtisadiyyatın digər sahələri ilə müqayisədə ən az informasiyalaşdırılmış sahə olaraq qalır, bu sahədə TİS-nin işlənməsi və tətbiqi isə, hələ ki, inkişafın başlanğıc mərhələsindədir [20, 21]. Buna baxmayaraq, ölkədə fərdi məlumatların qorunmasının hüquqi əsası mövcuddur. Hazırda AR-da fərdi tibbi məlumatların informasiya təhlükəsizliyi, əsasən aşağıdakı siyasi sənədlərlə tənzimlənir:

1. Ümumdünya insan hüquqları bəyannaməsi, Birləşmiş Millətlər Təşkilatı (BMT), 10 dekabr 1948-ci il.
2. «Fərdi məlumatların avtomatlaşdırılmış qaydada işlənməsi ilə əlaqədar şəxsiyyətin qorunması haqqında» Avropa Şurasının Konvensiyası, 28 yanvar 1981-ci il.
3. Azərbaycan Respublikasının Konstitusiyası, 3 avqust 2003-cü il.
4. «Fərdi məlumatlar haqqında» AR-nın Qanunu, 11 may 2010-cu il.
5. “Əhalinin sağlamlığının qorunması haqqında” AR-nın Qanunu, 25 iyun 1997-ci il.
6. "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" AR-nın Qanunu, 3aprel 1998-ci il.
7. “Elektron imza və elektron sənəd haqqında” AR-nın Qanunu, 9 mart 2004-cü il.

Fərdi verilənlərin İT sahəsində AR qanunvericiliyinin məqsədi vətəndaşlara aid məlumatların emalı zamanı onların hüquq və azadlıqlarının qorunmasının təmin edilməsi, eləcə də şəxsi həyatın, şəxsi və ailə sirlərinin qorunmasıdır. Lakin beynəlxalq təcrübədən məlum olduğu kimi, e-tibbin formalaşması şəraitində FTM nöqteyi-nəzərindən qanunun şərhi pasiyentlərin sağlamlıqları haqqında məlumatların xüsusiyyətlərindən irəli gələn çoxlu sayda mübahisələr və fikir ayrılıqları yaradır. Məsələn, «Fərdi məlumatlar haqqında» Qanun AR-nın ümumi fərdi verilənlərlə (S.A.A., pasport məlumatları, ünvan və s.) yanaşı, həm də xüsusi kateqoriya fərdi verilənlər adlanan məlumatları – pasiyentlərin sağlamlıqları haqqında həkim sirrini təşkil edən məlumatları emal edən TM-nə tətbiq edilir. Digər tərəfdən, tibbi xidmətlər göstərən zaman həkim sirrinin bir forması kimi tibb müəsisəsi işçilərinə məlum olan fərdi məlumatların mühafizəsi “Əhalinin sağlamlığının qorunması haqqında” Qanunla tənzimlənir. Bu kontekstdə “Fərdi məlumatlar haqqında” AR Qanununun FTM prizmasından interpretasiyası müəyyən anlaşılmazlıqlar və ziddiyyətlər yaradır. Belə ki, “Əhalinin sağlamlığının qorunması haqqında” AR-nın Qanununa müvafiq olaraq həkim sirrini təşkil edən məlumatlar eyni zamanda həm “xidməti sirlər”, eləcə də “fərdi məlumatlar” anlayışlarına aid edilir. Özəl həyat, şəxsi və ailə sirri faktları, hadisə və vəziyyətləri əhatə edən bu məlumatlar da vətəndaşın şəxsiyyətini identifikasiya etməyə kömək edir. Daha sonra, pasiyentlərin TİS-də emal olunan şəxsi məlumatlarının əksəriyyəti (sağlamlıq vəziyyəti, laborator tədqiqatların nəticələri haqqında və s. məlumatlar) “fərdi məlumatların xüsusi kateqoriyasına”, bəzi hallarda isə “biometrik fərdi məlumatlar” kateqoriyasına aiddir ki, bu da mühafizə sisteminə olan tələbləri artırır[22]. Buna görə də dünyanın bir çox ölkələrində FTM-ın İT-ni tənzimləyən spesifik normativ-hüquqi aktlar işlənmişdir [8–10, 16].

VII. FTM-IN İNFORMASİYA TƏHLÜKƏSİZLİYİNİN İNKİŞAF PERSPEKTİVLƏRİ

E-tibbin inkişafı, FTM-ın emalının kompüter texnologiyalarının geniş tətbiqi və onların trans-sərhəd mübadiləsi, TİS-nin inkişafı şəraitində tibbi, eləcə də həkim sirrini təşkil edən informasiyanın icazəsiz girişlərdən mühafizəsinin hüquqi, təşkilati və texnoloji təminatının işlənməsinə kompleks innovativ yanaşma tələb olunur. Bunun üçün FTM-ın mühafizəsi sahəsində real vəziyyətin aşağıdakı xüsusiyyətlərini nəzərə almaq tələb olunur: 1) bədniyyətlilərin informasiyanın köçürülməsi, ələ keçirilməsi və yayılması üzrə texniki imkanlarının artması, məlumatların təhlükəsiz ötürülməsi probleminin operativ həlli, tipik təhlükələr modeli və konkret bir təşkilatın FTM-nın mühafizə səviyyəsi və s. nəzərə alınmaqla, İT sistemini daim aktual vəziyyətdə saxlamaq lazımdır; 2) hal-hazırda bir çox TM-də FTM-ın qorunmasına lazımi diqqət yetirilmir; pasiyentlərin FTM-nın elektron bazalarının mühafizəsinə ayrılmış vəsait kifayət qədər deyil; məlumatın texniki mühafizəsi məsələlərində səriştəli, eləcə də müvafiq qanunvericiliyə bələd olan ixtisaslı kadrlar çatışmır, bir çox hallarda yox dərəcəsindədir [22].

Yaranmış vəziyyətdə effektiv yanaşmalardan biri yüksək ixtisaslı ekspert-mütəxəssislərin biliklərinin toplanması hesabına TM-də FTM-ın İT üzrə səlahiyyətli şəxslər tərəfindən qəbul edilmiş qərarların dəstəklənməsi üçün tövsiyələrin işlənməsinə imkan verən qərar qəbul edilməsini dəstəkləyən sistemlərin (QQDS) yaradılması ola bilər [23, 24].

VIII. NƏTİCƏ

1. TM-lərində FTM-ın mühafizəsinin təmin olunması probleminin spesifik xüsusiyyətləri vardır və e-tibb sistemi inkişaf etmiş ölkələrdə bu xüsusiyyətlərə uyğun, FTM-ın İT, şəxsi həyatın konfidensiallığı və toxunulmazlığı, şəxsi verilənlərə əlçatanlıq və onlardan istifadə zamanı məsuliyyət məsələlərini tənzimləyən ayrıca qanunverici baza işlənmişdir;

2. FTM-ın mühafizəsi sahəsində beynəlxalq təcrübə Azərbaycanda e-tibb şəraitində TM-ləri işçilərinin fəaliyyəti, hüquq və vəzifələrini, həkim və tibbi sirlərdən ibarət olan məlumatların mühafizəsi və təhlükəsizliyinin təmin olunması qaydalarını, ölkə daxilində, eləcə də onun sərhədlərindən kənarda informasiya mübadiləsi zamanı FTM-ın İT-ni və s. tənzimləyən normativ-metodiki sənədlərin işlənməsinin məqsədəuyğunluğunu aktuallaşdırır;

3. Səhiyyənin informasiyalaşdırılması şəraitində TM-lərində FTM-ın İT-nin təmin olunması məqsədi ilə səlahiyyətli şəxslər tərəfindən qəbul edilmiş qərarların dəstəklənməsinə yeni konseptual yanaşmaların işlənməsi məqsədəuyğundur.

ƏDƏBİYYAT

[1] Chao, H., Twu, S., and Hsu, C. A Patient-Identity Security Mechanism for Electronic Medical Records During Transit and At Rest,II Medical Informatics and the Internet in Medicine, vol. 30, no. 3, pp. 227–240, 2005.

[2] А. А. Абдуманонов, М. К. Карабаев, «Алгоритмы и технологии обеспечения безопасности информации в медицинской информационной системе Externet», Программные продукты и системы, №1, с. 150–155, 2013.

[3] J. Wang, Z. Zhang, X. Yang., L. Zuo, J. Kim, «Data Security and Privacy of e-Healthcare in Electronic Medical Environment», Proc. of the 2nd

International Conference on Sensor and its Applications, 2013, pp. 92–98.

[4] W. Wilkowska, M. Ziefle, “Privacy and data security in e-health: Requirements from the user’s perspective. Aachen University, Communication Science, Germany”, Health Informatics Journal, vol.18, no.3, pp.191–201, 2012.

[5] Б. А. Кобринский, Конфиденциальность и защита персональных медицинских данных в системе электронного здравоохранения. http://federalbook.ru/files/FSZ/soderghanie/Tom%2015/Kobrinskiy.pdf

[6] M. A. Ameen, J. W. Liu and K. Kwak, “Security and privacy issues in wireless sensor net-works for healthcare applications”, Journal of Medical System, vol.36, no.1, pp.93–101, 2012.

[7] D.B. Baker, “Privacy and Security in Public Health: Maintaining the Deli-cate Balance between Personal Privacy and Population Safety”, The 22nd Annual Computer Security Applications Conference, 2006, pp.3–22.

[8] European Parliament and Council Directive 95/46/ EC of 24 October 1995.http://europa.eu/legislation_summaries

[9] ISO 27001: 2013 Information technology. Security technigues. Information Security management systems. Requiremets.

[10] Y. B Choi, K. E. Capitan, J. S. Krause, and M. M. Streeper, “Challenges Associated with Privacy in Healthcare Industry: Implementation of HIPAA and Security Rules”, Journal of Medical Systems, vol. 30, no. 1, pp.57–64, 2006.

[11] Г. И. Назаренко, А. Е., Михеев, П. А. Горбунов, Я. И. Гулиев, И. А. Фохт, О. А. Фохт, Особенности решения проблем информационной безопасности в медицинских информационных системах. www.interin.ru/datas/documents/pib.pdf

[12] R. Agrawal, and C. Johnson, “Securing Electronic Health Records Without Impeding the Flow of Information”, International Journal of Medical Informatics, vol. 76, no. 5-6, pp 471– 479, 2007.

[13] L. O. Gostin, J. G. Hodge, “Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule”, Minnesota Law Review, vol.86, pp 1439–1449, 2002.

[14] Stefan Brands. Privacy and Security in Electronic Health www.credentica.com/ehealth.pdf

[15] A. Alyass, M.Turcotte, D. Meyre, From big data analysis to personalized medicine for all: challenges and opportunities. BMC Medical Genomics *2015*, www.biomedcentral.com/1755-8794/8/33

[16] Ajit Appari, M.Eric Johnson (2008).Information Security and Privacy in Healthcare: Current State of Research www.ists.dartmouth.edu/library/416.pdf.

[17] М. Г. Мамедова, «Информационная безопасность персональных медицинских данных в электронной среде», Проблемы информационных технологий, №2, с.16–30, 2015. http://jpit.az/index.php?mod=9&view=art&id=142

[18] McAfee Labs Threats Report – February 2015. www.mcafee.com/ru/security.

[19] L. B. Harman, C. A. Flite, Kesa Bond, “Electronic Health Records: Privacy, Confidentiality, and Security, AMA”, Journal of Ethics, vol. 14, no. 9, pp, 712–719, 2012. http://journalofethics.ama-assn.org/2012/09/stas1-1209.html

[20] M. H. Məmmədova, Ə. Q. Əliyev, “E-səhiyyə sisteminin formalaşması və inkişaf etdirilməsi problemləri”, Elektron dövlət quruculuğu problemləri” üzrə I Respublika elmi-praktiki konf. əsərləri, Bakı, 2014, səh.160–162.

[21] E-health. www.health.gov.az

[22] Р. М. Алгулиев, Я. Н. Имамвердиев, В. Я. Мусаев "Методы обнаружения живучести в биометрических системах," Вопросы защиты информации, №3, стр.16–21, 2009.

[23] М. Г. Мамедова, Принятие решений на основе баз знаний с нечеткой реляционной структурой. Ба ку, ЭЛМ, 1997, 296 с.

[24] E. S. Berner. Clinical decision support systems. Theory and practice. Springer Science+Business Media LLC, 2007, 278 p.