Tibbi sosial media istifadəçilərinin fərdi məlumatlarının təhlükəsizliyi məsələləri

Məsumə Məmmədova[1], Zərifə Cəbrayılova[2]
[1,2]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*mmg51@mail.ru*, [2]*depart15@iit.science.az*

***Xülasə*— E-tibbin formalaşması tibbi sosial media mühitini kütlə rəyini nəzərə almaqla tibbi xidmətin keyfiyyətinin yaxşılaşdırılması, tibbi qərarların qəbulu prosesinin təkmilləşdirilməsi, bir sıra sosioloji sorğuların keçirilməsi və s. üçün əhəmiyyətli informasiya mənbəyinə çevirmişdir. Elektron pasiyentlər onları maraqlandıran problemlərin həlli üçün sosial mediaya müraciət edir, peşəkar saytlarda qeydiyyatdan keçirək kontentlərdən yararlanmağa çalışırlar. Qeydiyyatdan keçən istifadəçilər bəzən özləri haqqında açıq verilənlər ilə yanaşı şəxsi identiklik verilənlərini də qeyd etməli olurlar. Bu isə fərdi məlumatların konfidensiallıq siyasətinin zəif olduğu sosial media mühitində istifadəçilərin fərdi məlumatlarının təhlükəsizliyi üçün ciddi problemlər yaradır. Baxılan məqalədə tibbi sosial şəbəkələrdə istifadəçilərin konfidensiallıq riskləri analiz olunmuş və konfidensiallıq siyasəti ilə bağlı bir sıra təkliflər göstərilmişdir.**

Açar sözlər— tibbi sosial media; e-pasiyentlər; şəxsiyyətin identiklik verilənləri; konfidensiallıq riskləri; konfidensiallıq siyasəti

I. GİRİŞ

E-tibbin formalaşmasını əks etdirən əsas məqamlardan biri həkim və pasiyentlərin ünsiyyət qurmaq, informasiya əldə etmək üçün virtual mühitə müraciət etməsi, tibbi sosial medianın yaranmasdır. Hazırda tibbi seqmentdə əlyetərli olan çoxlu sayda sosial media vasitələri mövcuddur. Bu vasitələr peşəkar şəbəkələrin təkmilləşdirilməsinə, ictimai sağlamlıq proqramlarının inkişaf etdirilməsinə, pasiyentlərə və onların maarifləndirilməsinə xidmət edir [1, 2]. Öz sağlamlığı haqqında daha çox məlumat almaq istəyən və bunun üçün İnternet və tibbi sosial şəbəkələr vasitəsilə bilik əldə edən elektron pasiyentlər (e-pasiyentlər) şikatərləri, xəstəlik simptomları ilə bağlı məlumatı sosial şəbəkədə yerləşdirir, təyin edilmiş diaqnoz və müalicə üsullarının etibarlığını yoxlamaq üçün sağalmış pasiyentlərdən, ekspertlərdən dəstək alırlar. Hazırda krodsorsinq texnologiyalarının tətbiqi anoloji presedentlərin tapılmasında pasiyentlərə dəstək göstərir [3–5].

E-pasiyentlər üçün belə imkanlar yaradan peşəkar saytlar qeydiyyat prosesində onlardan bir sıra fərdi verilənlərini qeyd etməyi tələb edir, sonradan həmin istifadəçilərin yerləşdirdiyi məlumatlar, kontentlər bu saytlar üçün əlyetərli olur. Təbii ki, tibbi sosial media mühitində, xüsusilə peşəkar şəbəkələrdə olan fərdi məlumatların konfidensiallığı ilə bağlı siyasətin düzgün qurulmaması (hətta olmaması) həmin informasiyanın arzuolunmaz məqsədlər üçün istifadəsinə yol açır [6, 7]. Nəticədə tibbi sosial media mühiti pasiyentlər üçün dəyərli informasiya mənbəyindən onların fərdi məlumatlarının konfidensiallığı üçün təhlükə mənbəyinə çevrilir.

Təqdim edilən məqalədə sosial mediada e-pasiyentlərin fərdi məlumatları analiz olunmuş, onların tibbi saytlarda paylaşdığı məlumatların, hətta şəxsiyyətinin identikliyi verilənlərinin (ŞİV) yerləşdirməsinin fərdi məlumatların təhlükəsizliyi baxımından mümkün fəsadları göstərilmişdir. İstifadəçilərin tibbi sosial mediadan istifadəsi nəticəsində yarana biləcək konfidensiallıq riskləri göstərilmiş və konfidensiallıq siyasətinin məsələləri şərh edilmişdir.

II. TİBBİ SOSIAL ŞƏBƏKƏLƏRDƏ PASIYENTLƏRIN FƏRDI MƏLUMATLARI

Sosial şəbəkələrdən kütləvi surətdə istifadə olunması İnternet mühitində peşəkar tibbi sosial cəmiyyətlərin meydana gəlməsinə səbəb olmuşdur. Məsələn, *Doc2Doc, Ozmosis, Healtheva* kimi tibbi sosial şəbəkələri həkim və pasiyentlər arasında kommunikasiya qurmaq üçün ən nümunəvi platformalar hesab olunurlar. *The Medical Directors Forum, QuantiaMD, Doctors Hangaut, Doc2Doc* kimi şəbəkələr isə həkimlərin bir-birilə və pasiyentlərlə kommunikasiya yaratmaları və əməkdaşlıq etmələri üçün mühüm platformalardır [8, 9]. *Medihost.ru, adam.com, DoctorSpring, likar.info, health.mail.ru* şəbəkələrində e-pasiyentlər ödənişsiz olaraq qeydiyyatdan keçməklə həkim xidmətlərindən yararlana bilərlər. Bu şəbəkələrdə qeydiyyatdan keçən e-pasiyentlərdən adı, yaşı, e-mail ünvanı, *qapsula.com_doslovno.com*-da isə həm də yaşadığı ərazi ilə bağlı məlumatı göstərməsi tələb olunur.

E-pasiyentlərin əksəriyyəti *Smart Patients, Stupidcancering, e-patients.net, Woman Heart Support Community, babycenter, Daily Strength* sosial şəbəkələrdən və sosial cəmiyyətlərin platformalarından istifadə edirlər. *PatientsLikeMe* [10] və *Treato* [11] sırf e-pasiyent cəmiyyətlərini dəstəkləyən sosial media resurslarıdır. *PatientsLikeMe* müxtəlif xəstəliklərin müalicəsindəki təcrübəyə əsaslanaraq terapiya (preparatlar da daxil olmaqla) növlərinin, simptomların, mümkün fəsadların və digər aspektlərin analizi üçün nəzərdə tutulmuşdur. Resursun əsas

DOI: 10.25045/NCInfoSec.2019.03

məsələlərindən biri analoji diaqnozlu e-pasiyentləri tapmaq, müəyyən xəstəliyin müalicəsində istifadəçilərə uğurlu təcrübədən yararlanmaq imkanının yaradılmasıdır.

Azərbaycanda tibbin müxtəlif sahələri üzrə ixtisaslaşmış həkimləri bir portalda cəmləyən peşəkar sosial cəmiyyətlər fəaliyyət göstərir. Bunlara misal olaraq “*Həkim.tap*”, “*həkimsənaz.az*”, “*sağlamolun.az*” , “*doctormap.az*” kimi sosial cəmiyyətləri göstərmək olar. E-pasiyentlər bu şəbəkələrin “həkim-axtarış” bölməsindən istifadə etməklə onları maraqlandıran həkimlər haqqında ətraflı məlumatlar əldə edə bilir, müəyən suallarla həmin həkimlərə müraciət edə bilirlər.

Bir çox açıq cəmiyyətlərdə olduğu kimi, tibbi saytların əksəriyyətində istifadəçilər çox vaxt öz sağlamlıqları ilə bağlı məlumtları azad şəkildə yerləşdirməkdən çəkinmirlər. Saytlarda istifadəçilər haqqında iki cür verilənlər toplanılır: ümumi verilənlər və məhdud (identik) verilənlər. Ümumi verilənlərə istifadəçilərin tərcümeyi-halı, yaşam tərzi, aldığı müalicələr, xəstəliyinin simptomları, laboratoriya nəticələri, genetik informasiyalar, sorğulara cavabları və digər istifadəçilərlə əlaqəsi aiddir. Əgər istifadəçi şəxsi identifikasiya informasiyası kimi adını və şəklini göstərirsə, bu ümumi məlumat hesab edilə bilər. Amma istifadəçi şəxsi informasiya kimi, məsələn, elektron poçt ünvanını, parolunu göstərirsə, bu artıq məhdud əlyetərli veriləndir. Məhdud əlyetərli verilənlərdən başqa saytda yerləşdirilən bütün verilənlər sayt tərəfindən digər istifadəçilərə və ya partnyorlarla mübadilə oluna bilər. Məsələn, *PatientsLikeMe* veb-saytının siyasətinə görə, istifadəçinin yerləşdirdiyi, məhdud əlyetərli verilənlərdən başqa informasiyanın istənilən bir hissəsi digər istifadəçilərə və ya partnyorlara ötürülə bilər [10]. İstifadəçi “M*ənim profilim”*-də “kütləvi” variantını seçmədikdə, onun profilində yerləşdirdiyi informasiya nə satıla bilər, nə də digər partnyorlara ötürülə bilər.

Lakin bir tərəfdən fərdi məlumatların konfidensiallığı ilə bağlı istifadəçilərin kifayət qədər təlimatlı olmaması, digər tərəfdən, toplanan kontentin həddən artıq alıcısının olması konfidensiallığın qorunmasında çox böyük problemlər yaradır. Odur ki, saytlar xüsusilə ŞİV göstərilən informasiyaların təhlükəsizliyi üçün təhlükələrə yol açır.

Hazırda saytların biznes-modeli onlarda toplanan informasiyanın formaseptik kompaniyalara və digər maraqlı partnyorlara satılmasına yönəlmişdir. İstifadəçilərin kontenti belə partnyorlara müalicə metodlarının seçilməsi, dərman və tibbi avadanlıqların istehsalı üçün qərarlar qəbulunda dəstək olur. İstifadəçilərin sağlamlıq vəziyyəti haqqında verilənlər tədqiqatların keçirilməsi, hesabatların hazırlanmasında çox istifadə olunur. Beləliklə, istifadəçilər peşəkar virtual cəmiyyət daxilində verilənlərin mübadiləsinə praktiki olaraq nəzarət etmirlər. Onlar belə saytdan istədiyini “aldığına” görə şəxsi verilənlərini qeyd etməklə sanki ona qarşı bir “inam” nümayiş etdirirlər və nəticədə konfidensiallıqla bağlı istifadə şərtlərini, siyasətini bəzən unudurlar.

1996-cı ildə ABŞ-da elektron tibbi kartlarda olan məlumatların qorunması üçün tibbi konfidensiallıq və mobilliyin sığortalanması haqqında qanun (*ing. Health Insurance Portability and Accountability Act of 1996 (HIPAA)*) və daha sonra onu təkmilləşdirərək iqtisadi və kliniki sağlamlıq üçün tibbi informasiya texnologiyaları haqqında qanun (*ing. Health Information Technology for Economic and Clinical Health HITECH*) qəbul edilmişdir [6, 12]. Lakin insanlar özləri könüllü surətdə veb saytlarda, virtual cəmiyyətlərdə şəxsi məlumatlarını yerləşdirirlərsə, burada HIPAA / HITECH onlar üçün “işləmir”. Beləliklə, tibbi sosial şəbəkələr e-pasiyentlər üçün geniş müzakirə meydanı yaratmaqla yanaşı, həm də bu mühitdə paylanmış məlumtaların nəzərdə tutulmayan məqsədlər üçün istifadəsinə yol açmış olur, fərdi məlumatların konfidensiallığı üçün bir sıra risklər yaradır.

III. TİBBİ SOSİAL ŞƏBƏKƏLƏRDƏ KONFİDENSİALLIQ RİSKLƏRİ

Tibbi sosial şəbəkələr e-pasiyentlərin fərdi məlumatlarının təhlükəsizliyi və konfidensiallığına yönəlmiş aşağıdakı risklərin yaranmasına imkan verir.

Birincisi, saytlar, adətən, istifadəçi profillərinin nəhəng saxlancına malik olurlar və onları daimi olaraq saxlaya bilirlər. Belə saytlarda istifadəçilər vaxtaşırı olaraq öz fərdi məlumatlarını bölüşürlər, sağlamlığı ilə bağlı yaranmış vəziyyəti idarə etmək, səhhətini yaxşılaşdırmaq üçün öz problemini daha məzmunlu ifadə etməyə çalışırr və konfidensiallıq məsələsini unudurlar [7]. Bəziləri isə əksinə, digərlərinə dəstək olmaq, özünün keçdiyi müalicə yolunda qarşılaşdığı problemlərlə digərlərinin üzləşməməsi üçün öz sağlamlığı ilə bağlı verilənləri saytda açıqlayır. Digər tərəfdən, tibb işçiləri də müəyyən cəmiyyətlərdə və təşkilatlarda hər hansı bir kliniki vəziyyətin müzakirəsi, yaranmış kritiki situsiyanın idarə olunması ilə bağlı iştirak etdikdə pasiyentlərinin konfidensial verilənlərinə istinad edirlər [13, 14]. Bir sıra peşəkarlar isə hətta sayt tərəfindən göstərilən xidmətin təkmilləşdirilməsi və təsadüfi mükafatlara görə pasiyentlərinin bütün fərdi məlumatlarını verməyə hazırdırlar [15]. Beləliklə, istifadəçilər haqqında ayrı-ayrı vaxtlarda açıqlanan verilənlər və əlaqəli (meta-) verilənlərin toplanması onların elektron sağlamlıq portretinin formalaşdırılmasına, konfidensiallıq riskinin yaranmasına zəmin yaradır.

İkincisi, istifadəçilər tərəfindən yaradılan kontent həm məqsədli, həm də nəzərdə tutulmayan auditoriya tərəfindən istifadə oluna bilər. Məsələn, istənilən fiziki və ya hüquqi şəxs qeydiyyatdan keçməklə saytın digər istifadəçilərinin verilənlərini əldə edə bilər, yəni veb-sayt istifadəçinin razılığı olmadan onun verilənlərini üçüncü tərəfə ötürə bilər [16]. Məsələn, checkMD (http://www.checkMD.com) saytı kimi saytlar öz işgüzar partnyorlarına və ya digər üçüncü tərəfə istifadəçilərinin şəxsi məlumatlarını açaqlaya bilir [17]. Belə

saytlar bəzən istifadəçilərinin bir sıra profil verilənlərinə istinad etməklə onların digər saytlarda olan qorunan məlumatlarına əlyetərlikdə üçüncü tərəfə dəstək göstərirlər. Beləliklə, istifadəçilərin istəyindən asılı olmayaraq onların verilənləri müxtəlif maraqlı tərəflərin əlinə keçə bilir.

Üçüncüsü, sağlamlıq vəziyyəti ilə bağlı toplanmış verilənlər qeyr-tibbi məqsədlər üçün istifadə oluna bilər. Bir sıra tibbi sosial şəbəkələr kommersiya və şəxsi məqsədlər üçün sağlamlıqla bağlı verilənləri toplamağa əsaslanan biznes modellərə malikdirlər. Onlar sağlamlıq vəziyyəti ilə bağlı verilənləri həkimlərə, formasept və tibbi kompaniyalara, tədqiqatçılara, qeyri-kommersiya təşkiltlarına və s. ötürə bilərlər. Dərman istehsalı və tibbi avadanlıqların istehsalı ilə bağlı olaraq sağlamlıq vəziyyəti ilə bağlı aqreqatlaşdırılmış verilənlər kommersiya təşkilatları üçün çox qiymətli məlumatdır. Verilənlərin toplanması üzrə innovasiya texnologiyaları və tibbi informatika müxtəlif mənbələrdən alınan məlumatları əlaqələndirməyə qadirdir, bu da rəqəmsal dosyenin yaranmasına zəmin yaradır. Təbii ki, ayrılıqa götürülmüş verilənlər şəxs haqqında o qədər də çox məlumat vermir, lakin onlar bir yerə toplandıqda şəxs haqqında çox şeyi “söyləyə” bilər. Odur ki, sığorta şirkətləri, işəgötürənlər, müştəri axtaran kompaniyalar üçün belə rəqamsal dosye çox fövqaladə qiymətli mənbə ola bilər. Digər tərəfdən lazımi nəzarət olmadan saxlanılan belə dosyelər haker və oğrular üçün də çox cəlbedicidir.

Nəhayət, daha bir məlum problem təhlüksizlik təhdidinin miqyasıdır. Təbii ki, yuxarıdakıların həlli istiqamətində şifrlənmiş ötürmə, autidentifikasiya və nəzarətin təmin edilməsi konfidensiallığın artırılmasına, ünvanlanmamış əlyetərliyin aradan qaldırılmasına imkan verir. Lakin saytın “sındırılması” və ya saytın operatorunun bircə səhvi saytın çoxsaylı istifadəçilərinin rəqəmsal anketlərini təhlükə altına alır.

IV. TİBBİ SOSİAL ŞƏBƏKƏLƏRDƏ KONFİDENSİALLIQ SİYASƏTİ

İstifadəçilərin konfidensiallığa münasibəti fərqli ola bilər, xüsusilə xroniki xəstəlikləri olanlar üçün konfidensiallıq çox vacib məqamdır. Bəzən istifadəçilərin rəqəmsal savadsızlığı, veb-saytlardan düzgün istifadə etməməsi və öz şəxsi verilənlərini açıqlaması onlayn-praktikada tez-tez rast gəlinən hallardandır [18]. Təbii ki, tibbi sosial şəbəkə mühiti hamı tərəfindən dərk edilən konfidensiallıq strukturu ilə təmin olunmalıdır və burada aşağıdakılar nəzərə alınmalıdır.

Birincisi, belə strukturda mübadilə olunan verilənlər ilə risklər arasında qarşılıqlı əlaqə olduğunu nəzərə almaq lazımdır. İstifadəçilər nə qədər çox verilənlərlə mübadilə edərlərsə, bir o qədər çox risk etmiş olurlar. Sosial şəbəkələrdə konfidensiallıq probleminin vahid yoxlanılmış və real həlli – qeyd olunan verilənlərə məhdudiyyət qoyulmasıdır. Yəni risk faktorunu azaltmaq üçün istifadəçilər ən minimum həcmdə şəxsi verilənlərini təqdim etməlidirlər (hətta bunlar fərdin açıq veilənləri olsa da). Məsələn, istifadəçilər əsil adlarını və milli identifikasiya nömrələrini bildirməməlidirlər. Buna baxmayaraq, istifadəçilər bir sıra tibbi sosial mənbələrdə onlara effektiv tibbi xidmət göstərilməsi üçün hətta belə verilənləri də göstərməli olurlar. Bir sıra istifadəçilər sayt tərəfindən təqdim olunan “konfidensiallıq siyasətini” qəbul etməklə (və hətta bu siyasətin “açıq” olduğunu bilsələr belə), elə hesab edirlər ki, saytda onların bütün şəxsi verilənləri qorunacaq [19].

İkincisi, istifadəçiləri öz şəxsi verilənlərinin konfidensiallığını təmin etməyə yönəltməkdir. Bu saytlarda informasiya mübadiləsi tibbi xidmətin keyfiyyətinin yaxşılaşdırılmasına yönəlsə də, verilənləri qərəzli auditoriyalarla mübadilədən qorumaq lazımdır. Konkret istifadəçinin verilənləri ya bütün geniş kütləyə açıq ola bilər, ya da istifadəçi konfidensiallıq problemindən xəbərdardırsa, veb-saytın yaratdığı imkandan istifadə etməklə öz verilənlərini yalnız seçilmiş “inamlı qruplar” üçün açıq edə bilər. Bu baxımdan saytlar bir neçə konfidensiallıq səviyyəsinə malik ola bilərlər.

Saytlarda istifadəçilərin fərdi məlumatlarının qərəzli açılması təhlükəsi ilə bağlı informasiyalara geniş yer verilməlidir. Məsələn, konfidensiallıq siyasətində göstərilməlidir ki, fərd kütlə tərəfindən görünən fərdi məlumatlarının silinməsini tələb etmək hüququna malikdir. Sayt öz konfidensiallıq siyasətində, fərdi məlumatların toplanması, istifadəsi və açıqlanması ilə bağlı bir dəyişiklik edirsə, bu haqda istifadəçilərini məlumatlandırmalıdır və s.

Üçüncü, konfidensiallıq və təhlükəsizlik platforması elə qurulmalıdır ki, həm də kontent üçün yararlı olsun. Lakin bəzi tibbi sosial şəbəkələr yalnız istifadəçilərin ŞİV-in konfidensiallığına zəmanət verir, onların biznes modeli məhz yaranan kontentin kommersiya məqsədləri üçün istifadəsinə yönəlir. Odur ki, bu saytlar belə geniş miqyaslı konfidensiallığa zəmanət vermirlər, bu istifadəçilərin özlərinə oxşarların tapılmasına, problemlərinin həlli istiamətində digərlərinin təcrübəsindən yararlanmağa imkan verməz. Bu problemin həlli üçün “layihələndirilmə yolu ilə konfidensiallıq” saytın arxitektur komponenti olmalıdır [20]. Bu prinsipin mahiyyəti odur ki, istifadəçidən heç bir hərəkət tələb etmədən, saytın özündə istifadəçilərin fərdi məlumatlarının nəzərdə tutulmayan əlyetərlikdən, istifadədən və yayılmaqdan qoruyan elementlər, modullar nəzərdə tutulmalıdır. Bu baxımdan **verilənlərin ananimliyi metodları** fərdi həyat üçün minimum risk yaratmaqla sağlamlıq vəziyyəti ilə bağlı veilənlərin geniş miqyaslı məqsədlər üçün istifadəsinə imkan verir.

Dördüncüsü, tibbi verilənlərin qeyri-tibbi məqsədlərlə istifadəsinə görə fiziki və hüquqi şəxslərin məsuliyyətə cəlb edilməsidir. Son dövrlərdə tibbi verilənlərin kommersiya və şəxsi məqsədlər üçün istifadəsi verilənlərin konfidensiallığı ilə bağlı cəmiyyətin siyasi dialoqa cəlb edilməsinin zəruriliyini gündəmə gətirmişdir. Fiziki və hüquqi şəxslər istifadəçilərin konfidensiallığını pozarlarsa və bu HIPAA/HITECH çərçivəsindən kənardadırsa, bu halda İnternetdə tibbi

verilənlərin konfidensiallığının qorunması üçün yeni qanunvericiliyin işlənilməsi tələb olunur.

Qanunvericilikdə istifadəçilərin məlumatlarını qeyri-tibbi məqsədlər üçün təqdim edənlərə nəzarət edilməsi ilə bağlı bölmə nəzərdə tutulmalıdır. Qanunvericilik həm də şəxsi razılıq olmadan məlumatların kommersiya məqsədləri üçün istifadəsinə qadağa qoymalıdır. Qanunvericilər konfidensiallıq prinsiplərini qəbul edən provayderlərdən saytın konfidensiallığının təmini üçün qaydalara daima əməl olunmasını tələb etməlidirlər.

NƏTİCƏ

Məqalədə göstərilmişdir ki, lazımi tibbi dəstək almaq üçün sosial tibbi mediaya müraciət edən e-pasiyentlər peşəkar saytlarda qeydiyyatdan keçərkən bir sıra şəxsi verilənlərini qeyd etməli olurlar, sağlamlıq vəziyyəti ilə bağlı müxtəlif məlumatları paylaşmalı olurlar. Saytlarda istifadəçilərin müxtəlif vaxtlarda göstərdiyi informasiyanın bir yerə toplanması, bəzən ümumi verilənlərlə yanaşı ŞİV-in də sayta ötürülməsi fərdi məlumatların arzu olunmaz məqsədlər üçün istifadəsinə yol açır. Bu baxımdan fərdi məlumatların təhlükəsizliyinin təmin olunması üçün e-pasiyentlərin qarşılaşa biləcəyi konfidensiallıq riskləri analiz olunmuş, konfidensiallıq siyasəti məsələləri göstərilmişdir. Qeyd olunmuşdur ki, tibbi sosial media mühitində istifadəçilər nəinki ŞİV-in, hətta ümumi məlumatlarının mübadiləsində ehtiyatlı olmalı, mümkün qədər az verilənlə mübadilə etməyə çalışmalıdırlar. Bu baxımdan təqdim olunan məqalə tibbi sosial şəbəkə istifadəçilərinin fərdi məlumatlarının konfidensiallığı istiqamətində maarifləndirilməsi üçün zəruri materialdır. Digər tərəfdən, məqalədə göstərilən tibbi sosial şəbəkələrdə konfidensiallıq siyasəti məsələləri istifadəçilərin bu saytlara göstərdiyi “inam”ın doğruldulmasında müvafiq sayt layihələndiriciləri üçün əhəmiyyətli informasiya kimi istifadə oluna bilər.

İSTİNADLAR

[1] M. Mammadova and A. Isayeva, “E-health activity in social media environment”, Problems of information society, 2018, no.1, pp.52–62.

[2] M. Mammadova and Z. Jabrayilova, “Electronic medicine: formation and scientific-theoretical problems”, Baku: “Information Technologies” publishing house, 2019, 319 p.

[3] G. Paul. The e-patient: empowered, enabled and electronic, http://www.slideshare.net/

[4] M. Swan. “Crowdsourced Health Research Studies: An Important Emerging Complement to Clinical Trials in the Public Health Research Ecosystem”, Journal of Medical Internet Research, 2012, vol.14, no.2, e46.

[5] Big data in the healthcare industry: Growing Need for Computerized Decision Support, http://www.healthcare.siemens.com/magazine/mso-big-data-and-healthcare-1.html

[6] L. Jingquan, “Privacy policies for health social networking sites”, Journal of the American Medical Informatics Association, vol.20, no.4, pp.704-707, https://doi.org/10.1136/amiajnl-2012-001500

[7] L. Jingquan, “Improving chronic diseases self-management through social networks”, Popul Health Manag., 2013, vol.16, no5, pp.285-291. doi: 10.1089/pop.2012.0110

[8] Top social networking sites for healthcare medical professionals, http://www.medicallabtechnicianschool.org/2009/top-25-social-networking-sites-for-healthcare-medical-professionals

[9] Report “Issue Brief: Social Networks in Health Care Communication, collaboration and insights”. Produced by the Deloitte Center for Health Solutions, 2010, p.2, http://www.healthinformationandcommunicationsystems.pbworks.com/w/file/fetch/93972338/SM%204b%20Full.pdf

[10] The future of health is here, www.patientslikeme.com

[11] See what millions of patients are saying, https://treato.com

[12] M. H. Mammadova, “The information security of personal medical data in an electronic environment”, Problems of information technology, 2015, no.2, pp.15-25.

[13] G. Moubarak, A. Guiot, Y. Benhamou, et al. “Facebook activity of residents and fellows and its impact on the doctor-patient relationship”, J Med Ethics, 2011, vol.37, pp.101-104.

[14] L. Thompson, E. Black, W. Duff et al. “Protecting health information on social networking sites: Ethical and legal considerations”, J Med Internet Res, 2011,vol.13. e8. http://www.jmir.org/2011/1/e8/

[15] A. Acquisti, J. Grossklags, “Privacy and rationality in individual decision making”, IEEE Secur Privacy, 2005, vol. 3, pp.26-33.

[16] J. Williams, “Social networking applications in health care: threats to the privacy and security of health information”, Conf Proc SEHC, 2010, no.2, pp.39-49.

[17] Terillion Privacy Policy. http://www.terillion.com/privacy-policy/ (accessed 25 Mar 2013).

[18] S. Livingstone, D. Brake, “. On the rapid rise of social networking sites: new findings and policy implications”, Children Soc, 2010, no.24. pp.75-83.

[19] D. McGraw, J. Dempsey, L. Harris et al., “Privacy as an enabler, not an impediment: building trust into health information exchange”, Health Aff, 2009, no.28., pp.416-427.

[20] S. Collins, D. Vawdrey, R. Kukafka R et al. “Policies for patient access to clinical data via PHRs: current state and recommendations”, J Am Med Inform Assoc, 2011, vol.18, pp12-17.

SECURITY ISSUES OF PERSONAL DATA OF MEDICAL SOCIAL MEDIA USERS

Masuma Mammadova[1], Zarif Jabrayilova[2]

[1,2]Institute of Information Technology of ANAS, Baku, Azerbaijan

[1]mmg51@mail.ru, [2]depart15@iit.science.az

Abstract – Taking into account the opinion of the mass in the medical social media environment, the formation of e-medicine becomes an important source of information for the improvement of the quality of medical services, the perfection of the medical decision-making process, implementation of numerous sociological surveys, etc. E-patients use social media to address the issues they concern about and attempt to benefit from the content professional sites registering in these sites. When registering, the users are often required to fill in their personally identifiable data along with their public information. However, this poses a serious problem for the privacy of user data in the social media environment where the privacy policy is vulnerable. This article analyzes the privacy risks of the users in medical social networks and provides a number of recommendations regarding the privacy policy.

Keywords *– medical social media environment, e-patients, personally identifiable information, privacy risks, privacy policies.*