Rəqəmsal Səhiyyə Mühitində Fərdi Tibbi Məlumatların Kibertəhlükəsizlik Problemləri və Həlləri

Ramiz Şıxəliyev
ETN İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
shikhramiz61@gmail.com

***Xülasə*— Bu gün elektron tibbi qeydlərin, teletibb platformalarının, daşına bilən cihazların və tibbi əşyaların internetinin geniş tətbiqi effektiv tibbi xidmətlərin yaradılmasına imkan verir. Lakin, bu texnologiyalar xəstələrə daha əlçatan tibbi xidmət təqdim etsə də, fərdi tibbi məlumatların (FTM) kibertəhlükəsizliyinə çoxsaylı təhdidlər yaratymışdır və kiberhücumların riskini artırmışdır. FTM-lərə edilən kiberhücumlar onların bütövlüyünü və məxfiliyini poza bilər və nəticədə tibbi xidmətləri poza və səhiyyə təşkilatlarına inamı sarsıda bilər. Bununla yanaşı, FTM-lər tibbi tarixçələri, diaqnozları, müalicə planlarını, genetik məlumatları və sığorta məlumatlarını ehtiva etdiyinə görə, onlar şəxsiyyət oğurluğu, maliyyə fırıldaqları və sairə üçün istifadə edilə bilər. Buna görə də FTM-nin kibertəhlükəsizliyinin təmin edilməsi çox vacib məsləsdir və onun hərtərəfli təhlilinə ehtiyac vardır. Bu tədqiqat işində FTM-nin kibertəhlükəsizliyinə təsir edən müxtəlif aspektlər, o cümlədən FTM-in rəqəmsallaşması ilə bağlı risklər, müasir səhiyyə İT sistemlərinin zəifliklərı, mövcud kibertəhlükələr, təhlükəsizlik standartları və tənzimləyici tələblər, həmçinin FTM-in kibertəhlükəsizliyinin artırılması üçün perspektivli sahələr təhlil edilir.**

Açar sözlər— fərdi tibbi məlumatlar, elektron tibbi qeydlər, kibertəhlükəsizlik, kibertəhlükəsizlik təhdidləri, rəqəmsal tibb, rəqəmsal səhiyyədə riskləri

I. GIRIŞ

Bu gün səhiyyədə elektron tibbi qeydlərin (ETQ), teletibb platformalarının, daşına bilən cihazların və Tibbi Əşyaların İnternetinin (Internet of Medical Things - IoMT) geniş tətbiqi effektiv tibbi xidmətlərin yaradılmasına imkan yaratmışdır. Eyni zamanda, tibbi xidmətlərin göstərilməsi üçün bulud hesablamaları, mobil tibbi proqramlar, uzaqdan monitorinq kimi texnologiyalar geniş miqyasda istifadə olunur. Bu yeniliklər tibbi xidmətlərə geniş və asan çıxış imkanı verir və xəstələrə tibbi xidmətlərin göstərilməsini təkmilləşdirir. Bununla yanaşı, IoMT cihazlarının səhiyyə sistemlərinə inteqrasiyası fərdi tibbi məlumatlara (FTM) qarşı yeni kiber təhdidlər yaradır [1]. İnkişaf edən kiber risklər qarşısında FTM-in kibertəhlükəsizliyini təmin etmək üçün sıfır inamlı arxitekturaların qəbulu vacib hala gəlir [2]. Sıfır etibar arxitekturaları müasir rəqəmsal tibb mühitində tibbi informasiya sistemlərinin təhlükəsizliyini təmin etmək üçün çox vacibdir [3].

FTM-lər tibbi tarixçələri, diaqnozları, müalicə planlarını, genetik məlumatları və sığorta məlumatlarını ehtiva etdiyinə görə, onlar şəxsiyyət oğurluğu, maliyyə fırıldaqları və sairə qeyri-qanuni hərəkətlərə qarşı həssasdır və onlar kiberhücumların hədəfinə çevrilir [4].

Bu gün, səhiyyə təşkilatları “ransomware” hücumları, fişinq hücumları, qabaqcıl davamlı təhdidlər (Advanced Persistent Threat - APT) və sairə kimi artan hücumlarla üzləşirlər [5]. Eyni zamanda, qeyri-effektiv FTM kibertəhlükəsizlik tədbirlərindən və köhnəlmiş informasiya texnologiyaları (İT) infrastrukturundan istifadə kiberhücumların tezliyini artırır. FTM-lərə qarşı həyata keçirilən kiberhücumlar tibbi sistemlərin və tibbi xidmətlərin bütövlüyünü poza bilər, həmçinin səhiyyə təşkilatlarına inamı sarsıda bilər. Buna görə də, FTM kibertəhlükəsizliyinin təmin edilməsi tibbi xidmətlərin bütövlüyü və etibarlılığının, habelə səhiyyə təşkilatlarına inamı təmin edilməsi üçün çox vacibdir.

Qanunvericilik səviyyəsində FTM-lərin məxfiliyini tənzimləmək üçün müxtəlif ölkələr tərəfindən qanunlar və qaydalar hazırlanmışdır. Bu məqsədlə ABŞ-da Səhiyyə Sığortasının Daşınması və Hesabatlılığı Aktı (Health Insurance Portability and Accountability Act - HIPAA) və Kaliforniya İstehlakçı Məxfiliyi Aktı (California Consumer Privacy Act - CCPA), Avropa İttifaqında (Aİ) isə Ümumi Məlumatların Qorunması Qaydası (General Data Protection Regulation - GDPR) qəbul edilmişdir [6-8]. Bununla belə, bu gün onlar rəqəmsal tibb mühitində daim inkişaf edən kiber risklərin qarşısını almaq üçün kifayət deyil. Odur ki, yeni kibertəhlükələr və innovativ texnologiyalar nəzərə alınmaqla FTM-nin məxfiliyini tənzimləmək üçün yeni qaydalar və standartların yaradılması çox vacibdir.

Məqalənin məqsədi tibbi xidmətlərin rəqəmsal transformasiyası nəticəsində FTM-in kibertəhlükəsizliyində yaranan problemlərin hərtərəfli təhlil edilməsidir. Bu problemlərin həlli FTM-in məxfiliyini və bütövlüyünü təmin edən daha təhlükəsiz, davamlı və etibarlı səhiyyə sisteminin yaradılmasına imkan verər..

II. FƏRDI TIBBI MƏLUMATLARIN IDARƏ OLUNMASI TƏKAMÜLÜ

XX əsrin sonlarında ETQ-lərin meydana gəlməsi FTM-nin yaradılması, saxlanması və paylanmasında inqilab etdi. ETQ-lərin tətbiqi xəstələrə tibbi xidmətin əlçatanlığını, dəqiqliyini

DOI: 10.25045/SPCDH4.0.2025.12

və koordinasiyasını artırdı [9]. Bununla yanaşı, ETQ-lərin tətbiqi müxtəlif səhiyyə sistemlərinin qarşılıqlı əlaqəsi və standartlaşdırılması sahəsində yeni problemlər yaratdı. Bu problemləri həll etmək üçün HL7 (Health Level Seven International) və IHE (Integrating the Healthcare Enterprise) standartları yaradılmışdır. Beləliklə, tibbi məlumatların mübadiləsi (Health Information Exchange - HIE) sistemləri xəstələrə tibbi xidmətin koordinasiyasını yaxşılaşdırmaq üçün mühüm alətə çevrilmişdir. HIE platformaları müxtəlif səhiyyə təşkilatları sistemləri arasında FTM-lərin təhlükəsiz mübadiləsinə imkan yaratmışdır. Bu cür qarşılıqlı fəaliyyət tibbi xidmətin keyfiyyətini yaxşılaşdırmaqla xəstələrin vəziyyətinin yaxşılaşdırılmasına töhfə vermişdir.

Son onillikdə səhiyyə sektorundakı texnoloji irəliləyişlərə görə FTM-lərin idarə edilməsi dəyişmişdir. Şəkil arxivləşdirmə, kommunikasiya sistemləri və radioloji informasiya sistemləri kimi ixtisaslaşmış texnologiyaların yaranması diaqnostik məlumatların getdikcə daha təkmil idarə olunmasına gətirib çıxardı. Bu sistemlər rəqəmsal tibbi təsvirləri və diaqnostik məlumatları əldə etməyə, saxlamağa və paylaşmağa imkan verir və nəticədə diaqnostika prosesini sadələşdirir. Bu texnologiyalar coğrafi yerindən asılı olmayaraq tibb işçiləri arasında məsafədən məsləhətləşmələrə imkan yaratmışdır.

Teletibb və uzaqdan xəstə monitorinqi texnologiyalarının inteqrasiyası FTM-lərin idarə edilməsində növbəti mühüm addım oldu. Teletibb infrastrukturunun yaranması uzaqdan məsləhətləşmələri asanlaşdırdı və xəstələrin vəziyyətinin yaxşılaşdırılmasına imkan verdi [10, 11]. Daşına bilən cihazların və uzaqdan monitorinqin tətbiqi həkimlərə real vaxt rejimində FTM-ləri toplamağa imkan verdi. Bu məlumatlar fərdi tibb və profilaktik tədbirləri gücləndirərək xəstə qeydlərinə inteqrasiya edilmişdir. Bununla belə, bu cihazlardan əldə edilən böyük həcmli məlumatların idarə edilməsi, təhlili və düzgün şərh edilməsi əlavə problemlər yaratmışdır. Bununla yanaşı, xəstə yönümlü yanaşmanın yaranması xəstələrin öz FTM-lərinin idarə edilməsində daha fəal iştirakını tələb edir. Portallar və mobil proqramlar xəstələrə öz sağlamlıqlarına nəzarət etməyə və tibbi qərarlarda daha fəal iştirak etməyə imkan verir. Bu yanaşma FTM idarəetməsində şəffaflığın və hesabatlılığın təmin edilməsinə kömək edir.

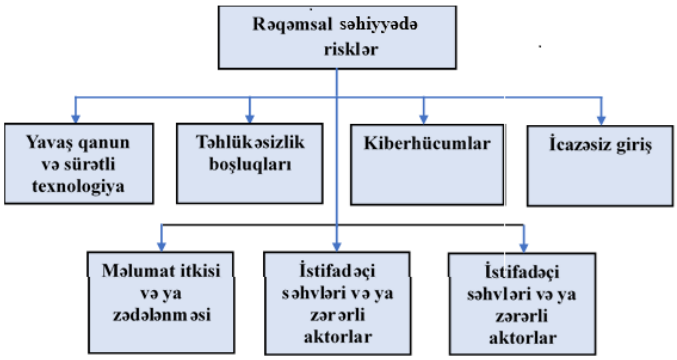
Bulud hesablamalarının inteqrasiyası FTM-lərin saxlanma və paylaşılma üsulunu əhəmiyyətli dərəcədə dəyişdi, miqyaslana bilən və çevik məlumat saxlama həlləri təklif etdi [12]. Bu texnologiyalar səhiyyə təşkilatlarına daha səmərəli fəaliyyət göstərməyə və səylərini coğrafi olaraq paylanmış sistemlər arasında əlaqələndirməyə imkan verir, eyni zamanda FTM-nin kibertəhlükəsizliyini təmin etmək problemini daha da gücləndirir.

Məlumatların emalı texnologiyalarının sürətli inkişafı səhiyyə təşkilatlarına strukturlaşdırılmış və strukturlaşdırılmamış tibbi qeydlərdən faydalı məlumat əldə etməyə imkan verdi. Faydalı məlumatın əldə edilməsi üçün böyük verilənlər analitikasından və maşın təlimindən (MT) istifadə edilir [13, 14]. Böyük verilənlər analitikasının istifadəsi klinik qərarların dəqiqliyini və müalicənin effektivliyini artırmış və fərdiləşdirilmiş tibbin inkişafını sürətləndirmişdir [15]. Böyük verilənlərin təhlili üçün süni intellekt (Sİ) və MT metodlarının tətbiqi tibbi qərarların qəbuluna dəstək sistemlərinin keyfiyyətini və diaqnozların dəqiqliyini artırmışdır [16].

Beləliklə, texnoloji innovasiya və FTM kibertəhlükəsizliyi məsələləri arasında dinamik qarşılıqlı əlaqə FTM idarəçiliyinin cari təkamülünü formalaşdırır və gələcəkdə mühüm istiqamət olaraq qalacaq.

III. FƏRDI TIBBI MƏLUMATLARIN RƏQƏMSALLAŞDIRILMASI ILƏ BAĞLI RISKLƏR

Səhiyyənin rəqəmsallaşdırılması FTM-ə çıxışı və səhiyyə xidmətinin göstərilməsinin koordinasiyasını və səmərəliliyini əhəmiyyətli dərəcədə artırıb. O, səhiyyə təminatçılarına real vaxt rejimində məlumat mübadiləsini asanlaşdırmağa və qərar qəbuletmə proseslərini təkmilləşdirməyə imkan verir. Bunun nəticəsində xəstələrə qulluq və müalicənin keyfiyyətində əhəmiyyətli irəliləyişlər əldə oldu. Bununla belə, FTM üçün bir sıra risklərlər meydana gəlir və bu risklər rəqəmsal sistemlərin geniş istifadəsinə əsas maneə yaradır (Şəkil 1). FTM-ə icazəsiz giriş şəxsi məlumatların oğurlanmasına, maliyyə fırıldaqlığına və digər zərərli fəaliyyətlərə gətirib çıxara bilər ki, bu da güclü kibertəhlükəsizlik tədbirlərinin həyata keçirilməsinə ehtiyac olduğunu göstərir [5]. Oğurlanmış FTM müxtəlif zərərli məqsədlər üçün, o cümlədən şəxsiyyət oğurluğu, səhiyyə xidmətlərindən icazəsiz istifadə, saxta reseptlərin yaradılması və maliyyə fırıldaqları istifadə edilə bilər [4].



Şəkil 1. Rəqəmsal səhiyyədə risklər.

FTM-nin icazəsiz yayılması və ya açıqlanması şəxsi həyatın məxfiliyinin ciddi şəkildə pozulmasına və xəstələrlə səhiyyə işçiləri arasında etimadın sarsıdılmasına gətib çıxara bilər. Bu riskləri azaltmaq üçün səhiyyə təşkilatları güclü şifrələmə, girişə nəzarət mexanizmləri və müntəzəm kibertəhlükəsizlik auditləri daxil olmaqla hərtərəfli təhlükəsizlik tədbirləri tətbiq etməlidir [5]. HIPAA sənədinin qəbulu məlumatların qorunması qaydalarına uyğun məxfilik problemlərini həll etmək və FTM idarəçiliyi üçün təhlükəsiz mühitin yaradılması üçün çox vacibdir. Bundan əlavə, effektiv autentifikasiya və avtorizasiya protokollarının istifadəsi şəxsiyyətlə bağlı riskləri azaltmaq və FTM-ə icazəli girişi təmin etmək üçün vacibdir.

Rəqəmsal FTM-nin idarə edilməsində digər əsas problem qarşılıqlı fəaliyyət məsələləridir. Qarşılıqlı qarşılıqlı fəaliyyət problemləri və məlumatların parçalanması tibbi xidmətin davamlılığını və keyfiyyətini poza bilər. Bunun üçün standartlaşdırılmış məlumat formatları və kommunikasiya protokollarının istifadəsi tələb olunur. FTM məlumatlarını

təhlükəsiz şəkildə paylaşmaq üçün müxtəlif səhiyyə sistemləri arasında vahid standartlar istifadə edilməli və qarşılıqlı fəaliyyət təşkil olunmalıdır. Əks halda, FTM-nin parçalanması tibbi xidmətin davamlılığını və keyfiyyətini poza bilər, çünki səhiyyə mütəxəssislərinin bütün FTM-lərə çıxışı olmaya bilər. Bu problemlərin həlli standartlaşdırılmış məlumat formatlarının və HL7 və IHE standartları tərəfindən dəstəklənən əlaqə protokollarının qəbulunu tələb edir.

Etik və məxfilik məsələləri FTM-in rəqəmsallaşdırılması ilə bağlı risklərin həllində mühüm əhəmiyyət kəsb edir [17]. Xəstələrin məlumatsızlığı və öz FTM-lərinin idarə edilməsində iştirak etmək istəməməsi kibertəhlükəsizlik zəifliklərini daha da artırır. Bir çox xəstələr FTM-lərinin rəqəmsallaşdırılması ilə bağlı risklərdən və ya məxfiliklərini qorumaq üçün atacaqları addımlardan xəbərsizdirlər. Xəstələri məlumatların kibertəhlükəsizliyi haqqında maarifləndirmək və onları öz FTM-lərinin idarə edilməsində daha çox iştirak etməyə təşviq etmək bu zəifliklərin azaldılması üçün çox vacibdir.

Səhiyyə sistemlərində rəqəmsal texnologiyaların geniş istifadəsi sistem nasazlığı ilə bağlı risklər yaradır. Texniki nasazlıqlar, səhiyyə sistemindəki nasazlıqlar və ya kiberhücumlar FTM-nin əlçatanlığını poza bilər ki, bu da kritik tibbi müdaxilələri (əməloyyatları) gecikdirə və xəstələrin həyatını riskə ata bilər. Səhiyyə sistemlərinin nasazlıqdan sonra bərpası və işin davamlılığı planlarının hazırlanması səhiyyə təşkilatlarına bu riskləri həll etməyə və xəstə məlumatlarına fasiləsiz girişi təmin etməyə kömək edə bilər.

FTM-in məxfiliyinin, bütövlüyünün və əlçatanlığının təmin edilməsi çoxşaxəli yanaşma tələb edir. Bunun üçün qabaqcıl təhlükəsizlik texnologiyaların tətbiq edilməli, standartlaşdırılmış çərçivələr yaradılmalı, pasiyentlərin marifləndirilməsi və sairə həyata keçirilməlidir. Bu problemləri həll etməklə, səhiyyə sistemləri xəstələrin məxfiliyini təmin edər və tibbi xidməti təkmilləşdirmək üçün rəqəmsallaşdırılmış FTM-dən istifadə edə bilər.

IV. MÖVCUD SƏHIYYƏ SISTEMLƏRININ ZƏIFLIKLƏRI

Səhiyyə İT sistemləri müasir səhiyyə xidmətlərinin göstərilməsi, həmçinin FTM məlumatlarının saxlanması, idarə edilməsi və mübadiləsi üçün çox vacibdir. Bununla belə, bu sistemlərdə FTM-in kibertəhlükəsizliyinə əhəmiyyətli təhlükə yaradan bir neçə zəifliklər var. Kibertəhlükələr getdikcə təkmilləşdikcə, səhiyyə İT sisteminin zəifliklərinin hərtərəfli təhlili və güclü təsir strategiyalarının həyata keçirilməsi zəruridir. İSO/IEC 27001-də qeyd edildiyi kimi tibbi informasiya təhlükəsizliyi idarəetmə sistemlərinin tətbiqi səhiyyə İT sistemlərində zəifliklərin aradan qaldırılması üçün çox vacibdir [18].

Səhiyyə İT sistemləri FTM-in məxfiliyi, bütövlüyü və əlçatanlığına təhlükə yarada biləcək müxtəlif zəifliklərə malikdir. Səhiyyə İT sisteminin ən çox rast gəlinən zəifliklərinə qeyri-adekvat məlumat şifrələməsi, zəif autentifikasiya mexanizmləri, köhnəlmiş proqram təminatı, təhlükəsiz proqram təminatı, məlumatların qeyri-adekvat ehtiyat nüsxəsinin çıxarılması və bərpa mexanizmlərinin istifadəsi, həmçinin daxili təhdidlər, şəbəkə zəifliklər, cihaz zəifliklər, üçüncü tərəf riskləri, insidentlərə qarşı dəqiq marifləndirmə planının olmaması [4] daxildir.

Həm ötürmə, həm də saxlanılma zamanı FTM-nin qeyri-adekvat şifrələnməsi səhiyyə İT sistemlərində ən ciddi zəifliklərdən biridir [5]. Qeyri-adekvat şifrələnmiş məlumatlar ələ keçirilməyə və icazəsiz girişə qarşı çox həssasdır. FTM-lərin icazəsiz giriş üçün əlçatmaz qalmasını təmin etmək üçün onları qorumaq üçün müvafiq şifrələmə standartlarından istifadə edilməlidir.

Zəif autentifikasiya sistemlərinə asanlıqla təxmin edilən parollar və ya çoxfaktorlu autentifikasiyanın olmaması daxildir ki, bu da səhiyyə sistemlərinə icazəsiz giriş riskini son dərəcədə artırır. Güclü autentifikasiya sistemlərinin, o cümlədən biometrik eyniləşmə və çoxfaktorlu autentifikasiyanın tətbiqi FTM-i qorumaq və onların təhrif riskini azaltmaq üçün vacibdir.

Çox vaxt səhiyyə təşkilatları bədəməlçilər tərəfindən istifadə edilə bilən zəifliklərə malik köhnə sistemlərdən və ya köhnəlmiş proqram təminatından istifadə edir. Müntəzəm proqram yeniləmələri və təhlükəsizlik yeniləmələrinin vaxtında tətbiqi bu riskləri aradan qaldırmaq üçün vacibdir.

Təhlükəsiz məsələləri nəzərə alınmadan kodlaşdırılmış proqramlarda kodlaşdırma səhvləri və zəif dizayn kimi zəifliklər ola bilər. Səhiyyə təşkilatlarında proqram tıminatı tətbiq edilməzdən əvvəl riskləri müəyyən etmək və azaltmaq üçün onlar hərtərəfli sınaqdan keçirməli və zəifliklər qiymətləndirilməlidir.

FTM-lər üçün qeyri-adekvat ehtiyat nüsxəsinin çıxarılması və bərpa mexanizmlərindən istifadə, onları kiberhücumlar və ya sistem uğursuzluqları halında əhəmiyyətli risklərə məruz qoyur. Müntəzəm sınaq və saxlama həlləri daxil olmaqla effektiv ehtiyat strategiyası FTM-lərin mövcudluğunu və bütövlüyünü təmin etmək üçün çox vacibdir.

Zərərli niyyət, səhlənkarlıq və ya təsadüfi açıqlama nəticəsində yaranan daxili təhlükələr səhiyyə İT sistemləri üçün böyük risk yaradır. Səhiyyə İT sistemlərinə girişi olan istifadəçilər təhlükəsizliyi poza bilər. Girişə ciddi nəzarət, davamlı monitorinq və səhiyyə İT sistemlərinin idarə olunması ilə bağlı aydın siyasətin həyata keçirilməsi bu riskləri azalda bilər.

Açıq portların olması, müdaxilənin aşkarlanması sistemlərinin olmaması və qeyri-adekvat şəbəkələrarası mühafizə səhiyyə İT sistemlərini kiberhücumlara qarşı həssas edir. Şəbəkə təhlükəsizliyi tədbirləri, o cümlədən müdaxilələrin qarşısının alınması sistemlərinin tətbiqi və müntəzəm nüfuz testi səhiyyə şəbəkələrinin kibertəhlükəsizliyinin gücləndirilməsi üçün çox vacibdir.

Tibbi cihazların, o cümlədən IoMT cihazlarının səhiyyə İT sistemlərinə inteqrasiyası əlavə zəifliklər yaradır. Bu cihazlar lazımi şəkildə qorunmazsa təcavüzkarlar üçün giriş nöqtəsi ola bilər. Müntəzəm cihaz təhlükəsizlik yeniləmələrinin təmin edilməsi, zəifliklərin qiymətləndirilməsi və cihazın təhlükəsizlik standartlarına riayət edilməsi səhiyyə sistemlərinin bütövlüyünü qorumaq üçün çox vacibdir.

Çox vaxt səhiyyə təşkilatları üçüncü tərəf xidmət təminatçıları ilə inteqrasiya olur ki, bu da əlavə zəifliklər yaradır. FTM-in kibertəhlükəsizliyinin təmin edilməsi, xarici

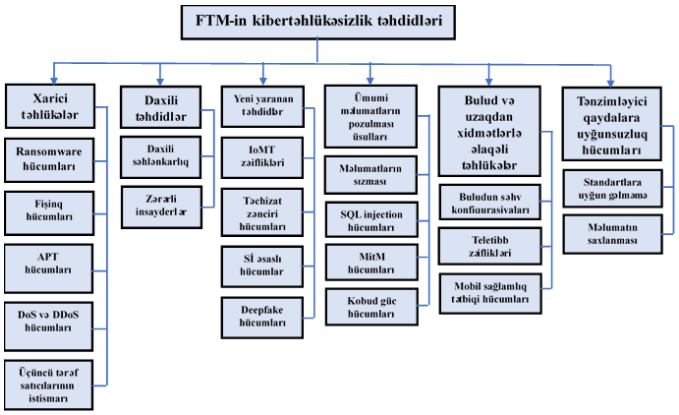
əlaqələrdən yaranan riskləri minimuma endirmək üçün sistem təhlükəsizliyinin müntəzəm qiymətləndirilməsini tələb edir.

İnsan faktoru səhiyyə İT sisteminin zəifliyinə əhəmiyyətli təsir göstərir. Fişinqi müəyyən edilməsi, güclü parolların təyin edilməsi və s. kimi kibertəhlükəsizlik praktikalarına dair kifayət qədər məlumatın olmaması FTM kibertəhlükəsizlik pozuntularına səbəb ola bilər. Davamlı təhsil və maarifləndirmə kampaniyaları səhiyyə işçilərinə potensial FTM risklərini müəyyən etmək və minimuma endirmək üçün lazım olan bilikləri təmin etmək üçün çox vacibdir.

Səhiyyə İT sisteminin kibertəhlükəsizliyinə qarşı mümkün insidentlərə cavab planının olması çox vacibdir. Əks halda, insidentlərin aşkarlanması və həllində əhəmiyyətli problemlər yarana bilər və səhiyyə sahəsində İT kibertəhlükəsizliyinin pozulmasının nəticələri daha da ağırlaşa bilər. Proaktiv insident cavablandırma üsullarından istifadə səhiyyə İT kibertəhlükəsizlik insidentlərinin təsirini əhəmiyyətli dərəcədə azalda bilər. Müəyyən edilmiş zəifliklərin aradan qaldırılması üçün texnoloji həllər, işçilərin təlimi və kibertəhlükəsizlik üzrə ən yaxşı təcrübələrdən istifadəni birləşdirən hərtərəfli yanaşma tələb olunur. Səhiyyə İT sisteminin kibertəhlükəsizliyinin müntəzəm monitorinqi və auditi səhiyyə təşkilatlarına potensial riskləri müəyyən etməyə və azaltmağa kömək edə bilər.

V. FƏRDI TIBBI MƏLUMATLARI HƏDƏF ALAN ÜMUMI KIBERTƏHLÜKƏSIZLIK TƏHDIDLƏRI

Rəqəmsal tibbi cihazların geniş istifadəsi həm istifadəçiləri, həm də səhiyyə təşkilatlarını hədəf alan müxtəlif kiber təhlükələrə səbəb olur. Səhiyyə təşkilatları üçün ümumi kibertəhlükəsizlik təhdidlərinə "ransomware" hücumları, fişinq hücumları, məlumatların pozulması, daxili təhdidlər, APT hücumları, zərərli proqramlar, casus proqramlar, ortada adam (MitM) hücumları, bir-biri ilə əlaqəli tibbi cihaz zəifliklərı və digərləri daxildir (Şəkil 2). Rəqəmsal tibbi cihazları bu təhdidlərin qoruması kompleks tədbirlər tələb edir.



Şəkil 2. FTM-ə ümumi kibertəhlükəsizlik təhdidləri.

Ransomware hücumları rəqəmsal tibbi cihazların təhlükəsizliyi üçün ən ciddi təhdidlərdən biridir və çox vaxt həssas məlumatların tamamilə itirilməsinə səbəb olur [5]. Bu cür hücumlar zamanı kibercinayətkarlar xəstələrin mühüm məlumatlarını şifrələyir və girişi bərpa etmək üçün səhiyyə təşkilatlarından ödəniş tələb edirlər. Bu hücumlar səhiyyə sistemlərini və xəstələrə göstərilən tibbi xidmətləri ciddi şəkildə poza bilər və etibarlı məlumat ehtiyat nüsxələri olmadıqda, həssas məlumatların tamamilə itirilməsinə səbəb ola bilər. Bununla yanaşı, bu cür hücumlar səhiyyə sistemlərinə inamı sarsıda bilər.

Fişinq hücumları insanların psixoloji zəifliklərindən istifadə edir və qurbanları aldadaraq giriş məlumatlarını əldə edir və ya zərərli proqram quraşdırır [5]. Fişinq tibb işçilərinə, inzibati heyətə və xəstələrə qarşı istifadə edilən ümumi üsuldur. Bu halda, kibercinayətkarlar qurbanları aldatmaq üçün fişinq e-poçtları, veb-saytlar və ya mətn mesajları kimi aldadıcı üsullardan istifadə edirlər.

Məlumatların məxfiliyinin pozulması səhiyyə məlumat bazalarına və ya sistemlərinə icazəsiz giriş nəticəsində baş verə bilər. Bunun nəticəsində şəxsi məlumatlar açıla və zərərli məqsədlər üçün istifadə edilə bilər. Məlumatların konfidiensallığının pozulmasının əsas səbəbləri qeyri-adekvat təhlükəsizlik protokollarının və zəifliklərə malik köhnəlmiş proqram təminatının istifadəsi, həmçinin girişə nəzarət sisteminin düzgün konfiqurasiya edilməmsidir..

Çox vaxt səhiyyə İT sisteminə giriş hüququ olan şəxslər tərəfindən həyata keçirilən *daxili təhdidlər* FTM-in kibertəhlükəsizliyi üçün risklər yaradır [4]. Girişə zəif nəzarətin olması və qeyri-effektiv monitorinq nəticəsində bu təhlükələrin nəticələri daha təsirli ola bilər. Daxili təhdidlərin əsas məqsədləri maliyyə mənfəəti, şəxsi mənfəət və s. ola bilər. Girişə nəzarətin gücləndirilməsi və davamlı monitorinqin həyata keçorolməsi bu təhlükələrin riskini azalda bilər.

APT hücumları FTM üçün ciddi risklər yaradan və uzun müddət aşkarlanmayan mürəkkəb kiberhücumlardır. Bu hücumlar səhiyyə İT sistemlərinə icazəsiz giriş əldə edə və uzun müddət aşkarlanmaya bilər. Çox vaxt, bu hücumların məqsədi məlumatları tədricən silməkdir ki, bu da FTM-in həm məxfiliyinə, həm də bütövlüyünə ciddi təhlükə yaradır.

Zərərli proqramlar və casus proqramları, adətən yenilənməyən proqram təminatı, mühafizə edilməyən cihazlar və təhlükəsizliyi pozulmuş şəbəkələr vasitəsilə səhiyyə İT sistemlərinə nüfuz edir. Bu zərərli proqramlar FTM-in əldə edilməsinə, səhiyyə xidmətlərinin pozulmasına və ya daha mürəkkəb hücumlar üçün istifadə edilə bilər.

MitM hücumları zamanı kibercinayətkarlar şifrələnmiş və ya şifrələnməmiş şəbəkə əlaqələri üzərindən iki tərəf arasında göndərilən məlumatları ələ keçirir. Bu cür hücumlar ötürmə zamanı FTM-nin icazəsiz tutulması və ya manipulyasiyası ilə nəticələnə bilər. Təhlükəsiz şəbəkə protokollarının və şifrələmə alqoritmlərinin istifadəsi bu təhlükələri azalda bilər.

Bir-biri ilə əlaqəli tibbi cihazların və IoMT-lərin geniş istifadəsi ciddi zəifliklər yaradır [1, 19]. Bu cihazların bir çoxunda güclü təhlükəsizlik tədbirləri yoxdur, bu da onları hücuma həssas edir. Təhlükə yarandığı halda, bu cihazlar FTM-ni sızdıraraq, xəstənin təhlükəsizliyinə təhlükə yarada bilər.

VI. FƏRDI TIBBI MƏLUMATLAR ÜÇÜN TƏHLÜKƏSIZLIK VƏ TƏNZIMLƏYICI ÇƏRÇIVƏLƏR

FTM-i icazəsiz girişdən, məlumat sızmasından və sui-istifadədən mühafizə etmək üçün möhkəm təhlükəsizlik və tənzimləyici çərçivə vacibdir. Bu çərçivələr FTM-nin məxfiliyini, bütövlüyünü və əlçatanlığını təmin etmək üçün səhiyyə təşkilatlarının əməl etməli olduğu təlimatları və

standartları təmin edir. FTM-in kibertəhlükəsizliyi bir sıra milli və beynəlxalq qanunlar, qaydalar və standartlarla tənzimlənir.

CƏDVƏL 1. FƏRDI TIBBI MƏLUMATLARIN TƏHLÜKƏSIZLIYI VƏ TƏNZIMLƏYICI ÇƏRÇIVƏLƏRI

Qanun/ standart	Kategoriya	Ölkə/region	Əsas tələblər/Prinsiplər	Tətbiq sahəsi
HIPAA (Səhiyyə Sığortası Portativliyi və Məsuliyyət Aktı)	Qanuni çərçivə	ABŞ	– Məxfilik və təhlükəsizlik standartları – İnzibati, fiziki, texniki tədbirlər – Məlumatın mühafizəsi və hesabatlılıq	Səhiyyə qurumları, tibbi məlumat-ları emal edən şirkətlər
GDPR (Ümumi Məlumat Qorunma Qaydası)	Qanuni çərçivə	Avropa İttifaqı	– Açıq razılıq və məlumat minimumu – Məlumatlara daxil olma, düzəliş və silmə hüququ – Davamlı monitorinq	AB-də fəaliyyət göstərən və ya AB vətəndaş-larının məlumat-larını emal edən təşkilatlar
CCPA (Kaliforniya İstehlakçı Məxfilik Aktı)	Qanuni çərçivə	ABŞ (Kaliforniya)	– Şəffaflıq və məlumat nəzarəti – İstehlakçıların məlumatlarına nəzarət hüququ – Sərt məlumat idarəetmə siyasəti	Kaliforniyada fəaliyyət göstərən və müəyyən həcmi ötən şirkətlər
Kanada Fərdi Məlumatların Mühafizəsi Aktı	Qanuni çərçivə	Kanada	– Şifrələmə, rol əsaslı giriş – İşçi təlimi və insident protokolları – Dövri təhlükəsizlik qiymətləndirmələri	Kanada qanunlarına tabe olan təşkilatlar
Avstraliya Məxfilik Aktı	Qanuni çərçivə	Avstraliya	– Məlumatların toplanması, istifadəsi və açıqlanması qaydaları – Risk idarəetmə tədbirləri	Avstraliyada fəaliyyət göstərən təşkilatlar
ISO/IEC 27001	Beynəl-xalq standart	Beynəlxalq	– İnformasiya təhlükəsizliyi idarəetmə sistemi (ISMS) – Risk əsaslı yanaşma – Davamlı yaxşılaşdırma	İnformasiya təhlükəsizliyini təmin etmək istəyən istənilən təşkilat
ISO/IEC 27701	Beynəl-xalq standart	Beynəlxalq	– Məxfi məlumatların idarə edilməsi	Xüsusilə məxfilik tələbləri yüksək olan sektorlar (səhiyyə, maliyyə və s.)

HIPAA ABŞ-da səhiyyə məlumatlarının qorunması üçün əsas qanundur. O, FTM-in məxfiliyi və təhlükəsizliyi üçün ciddi inzibati, fiziki və texniki tədbirlər tələb edən milli standartları müəyyən edir [6]. CCPA kimi yeni qaydalar, FTM daxil olmaqla, fərdi məlumatların məxfiliyinin təmin edilməsi məsələsini genişləndirir [7]. Bu qaydalar fərdlərə öz məlumatları üzərində tam nəzarət imkanı verməklə yanaşı, şəffaflıq və hesabatlılıq üçün geniş öhdəliklər qoyur və təşkilatlardan məlumatların daha sərt idarə edilməsi siyasətinin qəbul edilməsini tələb edir.

Aİ-də GDPR fərdi məlumatların, o cümlədən FTM-nin qorunması üçün hərtərəfli hüquqi baza təqdim edir və məlumatların minimuma endirilməsini və açıq-aşkar razılığı təmin edir [8, 20]. Bundan əlavə, GDPR fərdlərə öz məlumatlarına daxil olmaq, düzəlişlər etmək və silmək hüququ verir. Bu tələblər Aİ-də fəaliyyət göstərən və ya onunla qarşılıqlı əlaqədə olan səhiyyə təşkilatlarını təhlükəsiz məlumat idarəçiliyi və davamlı monitorinq təcrübələrini həyata keçirməyə məcbur edir.

Eynilə, Kanada, Avstraliya və bəzi Asiya ölkələri FTM-i tənzimləmək üçün xüsusi məxfilik qanunları yaratmışlar. Kanada Fərdi Məlumatların Mühafizəsi və Elektron Sənədlər Aktı və Avstraliya Məxfilik Aktı FTM-nin toplanması, istifadəsi və açıqlanması üçün tələbləri müəyyən edir. Bu aktlar riskləri azaltmaq üçün şifrələmə, rol əsaslı girişə nəzarət, hərtərəfli işçi təlimi, insidentlərə cavab protokolları və dövri FTM təhlükəsizlik qiymətləndirmələrini təşviq edən beynəlxalq təcrübəyə uyğundur.

Müxtəlif sənaye standartları da FTM-in kibertəhlükəsizliyinin formalaşmasında əsas rol oynayır. Məsələn, ISO/IEC 27001informasiya təhlükəsizliyinin idarə edilməsinə [18], ISO/IEC 27701 isə FTM-nin məxfiliyinin və bütövlüyünün təmin edilməsi üçün təlimatlar təqdim edərək, məxfi məlumatların idarə edilməsinə tələblər qoyur [21]. Bu standartlar səhiyyə təşkilatlarına effektiv kibertəhlükəsizlik tədbirlərinin işlənib hazırlanması, həyata keçirilməsi və saxlanılması üçün strukturlaşdırılmış yanaşma təqdim edir. Onlar həmçinin riskə əsaslanan metodologiyanı dəstəkləyərək, təşkilatları davamlı olaraq zəiflikləri qiymətləndirməyə, potensial təhdidləri izləməyə və yaranan riskləri həll etmək üçün kibertəhlükəsizliyə nəzarəti artırmağı çağırırlar. Hüquqi, texniki və təşkilati təhlükəsizlik tədbirlərini birləşdirərək, səhiyyə təşkilatları normativlərə uyğunluğu təmin edə, yaranan kibertəhlükələrə qarşı FTM-in dayanıqlığını yaxşılaşdıra və nəticədə xəstələrin etibarını və təhlükəsizliyini təmin edə bilər.

VII. GƏLƏCƏK TENDENSIYALAR

Qabaqcıl texnologiyaların istifadəsi, normativ-hüquqi bazanın təkmilləşdirilməsi və risklərin kompleks idarə edilməsi strategiyalarının həyata keçirilməsi FTM-in kibertəhlükəsizliyində yeni tendensiyalar yaradır. Bu, əsasən FTM-in təhlükəsizliyini, məxfiliyini və bütövlüyünü təmin etməklə yanaşı, mövcud və yaranan zəifliklərı aradan qaldırmağa yönəlib.

Sİ və MT texnologiyalarının istifadəsi FTM-in kibertəhlükəsizliyinin təmin edilməsində mühüm rol oynayır. Bu texnologiyalar proqnozlaşdırıcı analitika, anomaliyaların aşkarlanması və kibertəhlükələrə cavab mexanizmlərinin

avtomatlaşdırılmasına imkan verir. Sİ-yə əsaslanan sistemlər kibertəhlükəsizlik pozuntularını göstərə bilən qeyri-adi nümunələri açkar etmək üçün böyük həcmdə FTM-i emal etməyə qadirdir. Sİ real vaxtda təhdidləri aşkar etmək və onlara cavab vermək üçün kibertəhlükəsizlik tədbirlərinin effektivliyini artıra bilər. MT modellərinin istifadəsi yanlış pozitivlərin sayını azalda və FTM-in kibertəhlükələrinin daha dəqiq qiymətləndirilməsini təmin edə bilər.

Blockchain texnologiyası FTM-in kibertəhlükəsizliyini və məxfiliyini artırmaq üçün çox böyük potensiala malikdir. Mərkəzləşdirilməmiş və müdaxiləyə qarşı davamlı infrastruktura malik olan blokçeyn texnologiyası FTM-in bütövlüyünə və məxfiliyinə zəmanət verə bilər [22, 23]. Bu, məlumatların şəffaf idarə edilməsini təmin edə və nəticədə xəstələr və tibb işçiləri arasında etimadı artıra bilər. Bundan əlavə, blokçeyn texnologiyası müxtəlif səhiyyə sistemləri arasında təhlükəsiz məlumat mübadiləsini dəstəkləyə bilər. Blockchain əsaslı təhlükəsiz məlumat mübadiləsi və müxtəlif səhiyyə sistemlərinin inteqrasiyası FTM-in idarə edilməsinin şəffaflığını və etibarlılığını artıra bilər.

Kvant hesablamanın meydana gəlməsi FTM-nin kibertəhlükəsizliyinə həm imkanlar, həm də risklər gətirir. Kvant texnologiyaları hesablama imkanlarını təkmilləşdirmək potensialına malikdir, lakin onlar mövcud kriptoqrafik alqoritmlər üçün ciddi problemlər yaradır. Buna görə də, FTM-ni post-kvant təhlükələrindən qorumaq üçün kvant hesablamalarına davamlı olan kriptoqrafik alqoritmlərin işlənilməsi və həyata keçirilməsi vacibdir [24].

VIII. NƏTICƏ

Dayanıqlı, çevik və çox səviyyəli FTM kibertəhlükəsizlik sistemlərinin yaradılması səhiyyənin sürətli rəqəmsal transformasiyası kontekstində getdikcə daha çox əhəmiyyət kəsb edir. Bu zaman, FTM-in məxfiliyini təhdid edən kibertəhlükələrin artan mürəkkəbliyinin və müxtəlifliyinin nəzərə alınması xüsusilə vacibdir. FTM-in məxfiliyinin pozulması səhiyyə sistemlərinə ictimai inamı sarsıda və xəstələrə tibbi xidmətlərin effektiv şəkildə çatdırılmasına mane ola bilər. FTM-in kibertəhlükəsizliyi həm texnoloji, həm də daimi diqqət və fəal tədbirlər tələb edən etik və hüquqi məsələdir. Beləliklə, FTM-in kibertəhlükəsizliyi səhiyyə sistemlərinə ictimai inamın təmin edilməsində, xəstələrin məxfiliyinin qorunmasında və səhiyyənin təhlükəsiz və effektiv çatdırılmasında əsas rol oynayır. Bu tədqiqat işində FTM-in kibertəhlükəsizliyinin əsas aspektləri, o cümlədən FTM-in rəqəmsallaşması ilə bağlı risklər, müasir səhiyyə İT sistemlərinin zəifliklərı, mövcud kibertəhlükələr, təhlükəsizlik standartları və tənzimləyici tələblər, həmçinin FTM-in kibertəhlükəsizliyinin artırılması üçün perspektivli sahələr təhlil edilmişdir. Beləliklə, insanları, sistemləri və texnologiyanı birləşdirən hərtərəfli strategiyadan istifadə etməklə səhiyyə təşkilatları FTM-in məxfiliyini və kibertəhlükəsizliyini təmin edə bilər.

Bununla yanaşı, FTM kibertəhlükəsizliyinin dinamik və çoxşaxəli bir sahə oldiğunu, həmçinin texnoloji inkişafı və yeni təhdidləri nəzərə alınaraq gələcək tədqiqatlar daha çevik və proaktiv mühafizə strategiyalarına yönəlməlidir. Əsas gələcək tədqiqat istiqamətləri süni intellekt, maşın təlimi, blokçeyn, fərdi məlumatların anonimləşdirilməsi, real-zamanda kibertəhlükəsizlik monitorinqinin texnologiyalarının FTM-in kibertəhlükəsizliyinin təmin edilməsinə tətbiqi məsələlərindən ibarətdir.. Bu istiqamətlərdə aparılacaq işlər, nəinki FTM-in kibertəhlükəsizliyini artıracaq, həm də səhiyyə sistemlərinin ümumi etibarlılığını gücləndirəcəkdir.

MINNƏTDARLIQ

Bu iş Azərbaycan Elm Fondu tərəfindən dəstəklənib – Qrant № AEF-MCG-2023-1(43)-13/04/1-M-04.

ƏDƏBIYYAT

[1] Thomasian N.M., Adashi E.Y. (2021). Cybersecurity in the Internet of Medical Things. Health Policy Technol., 10(3), 100549. https://doi.org/10.1016/j.hlpt.2021.100549.

[2] NIST. Implementing a Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology; 2020. https://doi.org/10.6028/NIST.SP.800-207.

[3] Edo O.C., Ang D., Billakota P., Ho J.C. (2023). A Zero Trust Architecture for Health Information Systems. J Med Syst., 4,189-199. https://doi.org/10.1007/s12553-023-00809-4.

[4] Newaz A.I., Sikder A.K., Rahman M.A., Uluagac A.S. (2021). A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. ACM Trans Comput Healthc., 2(3), 27. https://doi.org/10.1145/3453176.

[5] Al-Qarni E.A. (2023). Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies. Int J Adv Comput Sci Appl., 14(5), 135-140. https://doi.org/10.14569/IJACSA.2023.0140513.

[6] Cohen I.G,, Mello M.M. (2018). HIPAA and protecting health information in the 21st century. JAMA, 320(3), 231-232. https://doi.org/10.1001/jama.2018.5630.

[7] California Legislative Information. California Consumer Privacy Act (CCPA). https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

[8] European Union General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[9] Adeniyi A.O., Arowoogun J.O., Chidi R, Okolo C.A, Babawarun O. (2024). The impact of electronic health records on patient care and outcomes: A comprehensive review. World J Adv Res Rev. 21(2), 1446-1455. http://dx.doi.org/10.30574/wjarr.2024.21.2.0592.

[10] Mehta N., Chaudhary A. (2022). Infrastructure and System of Telemedicine and Remote Health Monitoring. In: Choudhury T, Katal A, Um JS, Rana A, Al-Akaidi M, editors. Telemedicine: The Computer Transformation of Healthcare. Springer, 13-28. https://doi.org/10.1007/978-3-030-99457-0_2.

[11] Caracciolo A.L., Marino M.M., Caracciolo G. (2022). Patient-Physician Relationship in Telemedicine. In: Choudhury T., Katal A., Um J.S., Rana A., Al-Akaidi M., editors. Telemedicine: The Computer Transformation of Healthcare. Springer, 123-138. https://doi.org/10.1007/978-3-030-99457-0_4.

[12] Griebel L., Prokosch H.U., Köpcke F., Toddenroth D., Christoph J., Leb I., Engel I., Sedlmayr M. (2015). A scoping review of cloud computing in healthcare. BMC Med Inform Decis Mak., 15(1), 1-16. https://doi.org/10.1186/s12911-015-0145-7.

[13] Ganie S.M., Malik M.B., Arif T. (2022). Machine Learning Techniques for Big Data Analytics in Healthcare: Current Scenario and Future Prospects. In: Choudhury T., Katal A., Um J.S., Rana A., Al-Akaidi M,. editors. Telemedicine: The Computer Transformation of Healthcare. Springer, 157-177. https://doi.org/10.1007/978-3-030-99457-0_6.

[14] Al Mudawi N., Alazeb A., Alshehri M.S., Almakdi S. (2023). Machine Learning Algorithms for Health Data Security: A Systematic Review. In: T. Choudhury, A. Katal, J. S. Um, A. Rana, and M. Al-Akaidi, editors. Cloud Computing in Medical Imaging. CRC Press, 53-78. https://doi.org/10.1201/9781003145189-3.

[15] Raghupathi W. and Raghupathi V. (2014). Big data analytics in healthcare: Promise and potential. Health Inform Sci Syst., 2(1), 3. https://doi.org/10.1186/2047-2501-2-3.

[16] De Aguiar E.J., Traina C Jr, Traina AJM. (2023). Security and Privacy in Machine Learning for Health Systems: Strategies and Challenges. Yearb Med Inform. 32(1):269-281. https://doi.org/10.1055/s-0043-1768731.

[17] Peterson R., DeCew J. (2020). Ethical and Privacy Considerations in Healthcare Cybersecurity. Ethics Med Public Health., 15, 100564. https://doi.org/10.1016/j.jemep.2020.100564.

[18] ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements. International Organization for Standardization and International Electrotechnical Commission.

[19] Sun Y., Lo F.P-W., Lo B. (2019). Security and privacy for the internet of medical things-enabled healthcare systems: A survey. IEEE Access.,7, 102580-102588. https://doi.org/10.1109/ACCESS.2019.2960617

[20] .Voigt P., von dem Bussche A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer. https://www.springer.com/gp/book/9783319579597.

[21] ISO/IEC 27701:2019 Privacy information management - Requirements and guidelines. International Organization for Standardization and International Electrotechnical Commission.

[22] Huang L., Lee H.H. (2020). A Medical Data Privacy Protection Scheme Based on Blockchain and Cloud Computing. Wirel Commun Mobile Comput., 8859961. https://doi.org/10.1155/2020/8859961.

[23] Jin H., Xu C., Luo Y., Li P. (2020). Blockchain-Based Secure and Privacy-Preserving Clinical Data Sharing and Integration. In: Qiu M, editor. Algorithms and Architectures for Parallel Processing. Springer, 123-139. https://doi.org/10.1007/978-3-030-60248-2_7.

[24] SaberiKamarposhti M., Ng K.-W., Chua F.-F., Abdullah J., Yadollahi M., Moradi M., Ahmadpour S. (2024). Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data, Heliyon, 10(10), e31406. https://doi.org/10.1016/j.heliyon.2024.e31406.