Elektron sağlamlıq kartlarında fərdi məlumatların təhlükəsizliyi problemləri

Aytən Əhmədova
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
ayten.adia 1996@gmail.com

***Xülasə*—Məqalədə elektron sağlamlıq kartlarında fərdi məlumatların təhlükəsizliyi məsələləri tədqiq olunmuşdur. Elektron sağlamlıq kartları haqqında qısa məlumat verilmiş, onlara olan təhlükəsizlik təhdidləri təsnifatlandırılmışdır. Elektron sağlamlıq kartlarının hansı şərtlər daxilində təhlükəsizliyinin təmin olunması qeyd olunmuş, fiziki sistemə girişə nəzarət olunması qaydaları və bir sıra şifrələmə üsulları göstərilmişdir.**

Açar sözlər– elektron sağlamlıq qeydləri; tibbi sənədlər; fərdi məlumatların təhlükəsizliyi; təhdidlər; HIPAA

I. GİRİŞ

İnformasiya cəmiyyətinin formalaşması, ictimai həyatın bütün sahələrinə informasiya texnologiyalarının (İT) tətbiq edilməsi tibb sahəsində də öz təsirini göstərmişdir. Tibbi xidmətlərə artan tələbin təmin olunması probleminin konstruktiv həlli İT-nin səhiyyəyə inteqrasiyasından qaynaqlanır. İKT-nin tibb sahəsinə tətbiqi 2000-ci ildən əsas prioritetlər sırasına daxil edilmişdir [1].

Elektron sağlamlıq kartları *(ing. Electronic Health Cards, ESK*) fərdi, sağlam və məxfi bir mühitdə sağlamlıq məlumatlarının saxlandığı elektron tətbiqdir. ESK-ya fərdin doğulduğu gündən etibarən bütün ömür boyu məlumatlar qeyd olunmağa davam edir. ESK-da hər bir xəstə üçün fərdi məlumatlar (diaqnostik təsvirlər, reseptlər, laborator testlər, aparılmış müşahidə nəticələri) yerləşir. Həkim həmin qeydlərdən istifadə etməklə kağız üzərində olan yazılı xəstəlik tarixçələrinin oxunmasına çox vaxt sərf etmir və xəstənin müalicəsi üçün lazımi müayinə üsulunun seçilməsi ilə bağlı onlara qərar qəbulunda operativ həll əldə edir [2,3].

Elektron tibbi kartların bir çox üstünlükləri vardır, lakin bu texnologiyada informasiya elektron mühitdə saxlandığı üçün fərdi məlumatlara qarşı məxfilik və təhlükəsizlik təhdidləri artmış olur. Odur ki, elektron səhiyyənin inkişaf etdiyi hazırki dövrdə fərdi məlumatların təhlükəsizliyinin təmin edilməsi kifayət qədər aktual məsələdir.

II. ELEKTRON SAĞLAMLIQ KARTLARI

ESK xəstə haqqında bütün lazımi tibbi məlumatların toplanmasına və istifadə edilməsinə imkan verən məlumatlar bazasıdır.

1960-1970-ci illərdə sürətlə inkişaf edən yeni informasiya texnologiyaları ESK-nın inkişafına zəmin yaratdı və xəstələrin tibbi məlumatlarına dünyanın hər yerindən əlçatanlığını mümkün etdi [4]. ABŞ-da Muin Rochesterdəki “Mayo” klinikası 1960-cı illərin əvvəllərində ESK-nı qəbul edən ilk böyük sistemlərdən biri idi. Aparılan tədqiqatlara görə 1965-ci ilə qədər təxminən 73 xəstəxana və klinik informasiya layihələri tibbi sənədlərin və klinik məlumatların saxlanması və alınması üçün 28 layihə işləmişdir [5].

Tibbi məlumatların elektron mühitdə saxlanmasının aşağıdakı müsbət cəhətləri var [6]:

- tibbi sənədlərin dəqiqliyi və aydınlığını artırmaqla səhvlərin azaldılması;
- təkrarlanmaları azaltmaq, müalicədə gecikmələri minimuma endirmək, həkimlər tərəfindən daha etibarlı qərar qəbul edilməni təmin etmək.

[6]-də ESK-ların arxitekturası aşağıdakı kimi qruplaşdırılmışdır:

- *mərkəzləşmiş/tam inteqrasiya olunmuş model*. Bu modeldə bütün cavabdehlik Səhiyyə Nazirliyi və ya eSəhiyyə mərkəzlərinə verilir;
- *mərkəzi-paylanmış/federallaşmış model*. Burada ESK özü Səhiyyə Nazirliyinin öhdəsinə verilir, onun blokları isə müxtəlif səhiyyə təşkilatlarında yerləşir;
- *hibrid model*. Əvvəlki iki modelin birləşməsidir.

Arxitekturaya uyğun olaraq ESK-nın təhlükəsizliyi üçün müvafiq tədbirlər görülür.

III. ELEKTRON SAĞLAMLIQ KARTLARINDA TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

Dünya səhiyyə provayderləri təhlükəsiz, effektiv, əlçatan və paylaşılan tibb xidmətləri göstərmək üçün ESK sistemlərinə böyük axınla miqrasiya edir. ESK fərdi tibbi məlumatların təhlükəsizliyinin təmin olunması üçün sistemin işlənməsi və təhlükəsizlik üçün optimal rejimin seçilməsini kifayət qədər aktuallaşdırır. İnsanların qapalı məlumatlarının yerləşdiyi ESK-ya girişi olan tibb müəssələri tibbi məlumatların konfidensiallığına və təhlükəsizliyinə zəmanət verməlidir. Konfidensiallıq dedikdə, həmin məlumatlara giriş əldə etmiş şəxslərin xəstənin icazəsi olmadan onun fərdi məlumatlarını açmağa və yaymağa hüququnun olmaması başa düşülür.

DOI: 10.25045/NCInfoSec.2019.55

Hüquqi baxımdan pasientin tibbi məlumatları əlçatanlığı məhdudlaşdırılmış, həkim sirri hesab olunan informasiyalara aid edilir və hər bir ölkədə fəaliyyət göstərən müəyyən qanunvericiliklə idarə olunur.

Elektron fərdi tibbi məlumatlarla işləyərkən aşağıdakı təhlükə və təhdidlər meydana çıxa bilər [2,3]:

- *təşkilati təhdidlər*. Bədniyyətlə, icazəsi olmadan ESK-ya giriş edən şəxslər, hakerlər, insayderlər tərəfindən yaranan təhdidlər;
- *texniki təhdidlər*. Məlumatların itirilməsi, saxtalaşdırılması, fiziki daşıyıcıların məhv olması nəticəsində yaranan təhdidlər.

Məlumatın təhlükəsizliyi ilə bağlı təhdidlər adətən informasiyanın üç xüsusiyyətinə qarşı yönəlir [8]:

- konfidensiallıq;
- tamlıq;
- əlyetənlik.

Bütün bu xüsusiyyətlərin qorunması ESK-lar üçün vacibdir.

Bu xüsusiyyətlərdən hər hansı biri ilə bağlı təhlükəsizlik tədbiri lazımi səviyyədə olmazsa, pasiyentlər haqqında olan fərdi tibbi məlumatların təhlükəsizliyini təmin etmək çətinləşir.

Hazırda səhiyyə infrastrukturuna zərərli proqramlar, botnetlər kimi vasitələrlə kiberhücumların edilməsi halları çoxluq təşkil edir [7]. Kibertəhlükəsizlik insidentlərinin səhiyyə sistemlərinə göstərdiyi təsir böyük problemlərə gətirib çıxara bilər. Kibertəhlükəsizliyə qarşı dayanıqlı e-tibb sistemində aşağıdakı şərtlər təmin olunmalıdır:

1) fərdin müayinə və müalicəsində ciddi fəsadlar yarada biləcək verilənlərin tamlığının təmin olunması;

2) e-səhiyyəni təşkil edən sistemlər arasında interaprobelliyin qorunması;

3) şəxsə aid olan fərdi tibbi məlumatların gizliliyinin təmin olunması;

4) fərdi tibbi məlumatlara ancaq səlahiyyətli şəxslərin istənilən vaxt girişinin təmin olunması üçün sistemdə əlçatanlığın mümkünlüyü.

Sistemdə insan səhvləri nəticəsində baş verən pozulmalara, insidentlərə tab gətirə bilən davamlı mexanizm işlənməlidir. Əks halda, yəni girişə nəzarət və autentifikasiya üsulları kifayət qədər olmazsa, fərdi məlumatların üçüncü şəxs tərəfindən ələ keçirilməsi baş verə bilər. Fərdi məlumatlara icazəsiz daxilolmalar nəticəsində klinik verilənlərin pozulması halları müşahidə olunur.

Məxfilik fərdi məlumatlar üzərində icazəli şəxslər tərəfindən nəzarəti ehtiva edir. Fərdi məlumatların digər şəxslər tərəfindən idarə olunması nəticəsində xəstənin fərdi tibbi məlumatları oğurlanır. Təhlükəsizlik təmin edildikdə həmin məlumatlara giriş məhdudlaşdırılır [9]. ESK sistemlərinin təhlükəsizliyi aşağıdakı üsullarla həyata keçirilir [10]:

- fiziki təhlükəsizlik – ESK-ya girişlərə nəzarət olunması;
- texniki təminatlar – şifrələmə və ya şəbəkələrarası ekran üsullarından istifadə olunması.

A. Fiziki sistemlərdə girişə nəzarət edilməsi mexanizmi

Fiziki sistemlərdə girişə nəzarət edilməsi mexanizmi aşağıdakıları ehtiva edir [11]:

1) məlumatlara daxilolma icazəsi olmayan şəxslər üçün əlçatmaz sistemin yaradılması;

2) sistemə daxil olmaq istəyən bütün şəxslər üçün şəxsiyyəti təsdiqləmə bölməsinin olması;

3) şifrə və fərdi identifikasiya nömrələrinin (FİN) təmin olunması;

4) proqramın avtomatik bağlanması prosedurunun yerinə yetirilməsi.

B. Şifrələmə üsulları

Şifrələmə proseslərində müxtəlif alqoritmlərdən ən uyğun olanı seçmək vacibdir. Aşağıda şifrələmə üsullarına nümunələr verilmişdir [12]:

–*CryptDB*. Proksi əsaslı şifrələmə sistemidir. CryptDB verilənlər bazasının şifrələnməsi üsulu ilə təhlükəsizliyi mümkün edir. Massaçuset Texnologiyalar İnstitutu tərəfindən yaradılmışdır və proksi şifrələməyə əsaslanan verilənlər bazası şifrələmə üsullarının əksəriyyəti CryptDB-nin formasına uyğun qurulmuşdur.

–*T-SQL* şifrələmə - tranzaktiv quruluşlu sorğu dili T-SQL Microsoft SQL server 2005-dən bəri tətbiq olunan bir şifrələmə üsuludur. Şifrələmə əsasən bir-birindən fərqli iki üsulla aparıla bilər:

Şəffaf şifrələmə (ing. Tansparent data encryption). Bütövlükdə verilənlər bazasına tətbiq olunur. Bu şifrələmə üsulunda əməliyyatlar səhifələr üzrə aparılır.

Sütun şifrələmə (ing. Column level encryption)- Şəffaf şifrələmə üsulundan fərqli olaraq istənilən sütunun şifrələnməsi ilə həyata keçirilir və Encrypt Key, Decrypt Key funksiyaları tətbiq olunana qədər işləmir.

VI. HIPAA TƏHLÜKƏSİZLİK STANDARTI

1996-cı ildə ABŞ-da qəbul edilmiş Tibbi Konfidensiallıq və Mobilliyin Sığortalanması haqqında Qanun (*ing. The Health Insurance Portability and Accountability Act, HIPAA)* bütün e-tibb sistemində xəstə məlumatlarını qorumaq üçün məxfilik, təhlükəsizlik və elektron əməliyyat standartlarını tələb edən və mühafizə üsullarını təyin edən federal qanundur [13]. HIPAA standartında fərdi məlumatların təhlükəsizliyi şəxsi həyatın toxunulmazlığı və konfidensiallığı kimi iki vacib ideyaya əsaslanır. Şəxsi həyatın toxunulmazlığı dedikdə, xəstənin tibbi vəziyyəti haqqında kimin və nəyə əlçatanlığının olmasının

məhdudlaşdırılması, məlumatlara girişi olan şəxslərin məqsədləri barədə qaydaların olması kimi hüquqlar daxildir.

Təhlükəsizlik standartında tədbirlər üç başlıq altında (inzibati, fiziki, texniki) qruplaşdırılır [14].

– *İnzibati tədbirlər*: fövqəladə hallar və görüləcək tədbirlər, riayət ediləcək prosedurlar;

– *Fiziki tədbirlər*: sağlamlıq haqqında məlumat mühitinə fiziki girişə nəzarət tədbirləri;

–*Texniki tədbirlər*: hücumlardan qorunma, monitorinq və qeyd üsulları, məlumat ötürülməsində istifadə edilə bilən şifrələmə metodları, daimi risk təhlili və risklərin idarə edilməsi.

NƏTİCƏ

Hazırda insanların elektron saxlanılan tibbi məlumatları sistemləşdirilmiş şəkildə ESK-da saxlanılır. Texnologiyanın inkişafı ilə e-tibbin formalaşması və onun əsas göstəricilərindən biri olan ESK-ların daha geniş vüsətlə artmasına zəmin yaradır. Digər tərəfdən bu yüksəliş onlarda olan fərdi tibbi məlumatların təhlükəsizliyinə yönəlmiş təhdidlərin ortaya çıxmasına səbəb olur. Məqalədə ESK-da olan fərdi tibbi məlumatların təhlükəsizliyi sahəsində bir sıra tədqiqatlar nəzərdən keçirilmiş, təhlükəsizlik üsullarının təsnifatı verilmiş, HIPAA standartı haqqında məlumat təqdim edilmişdir.

İSTİNADLAR

[1] M. Məmmədova, Z. Cəbrayılova “Elektron tibb: formalaşması və elmi nəzəri problemləri,” Bakı, pp. 86-105, 2019.

[2] M.Mammadova "The information security of personal medical data in an electronic environment,"Problems of Information Technology, no.2, pp.15-25, 2015.

[3] M.Məmmədova "Elektron fərdi tibbi məlumatların informasiya təhlükəsizliyi problemləri," “Elektron tibbin multidissiplinar problemləri” I respublika elmi-praktiki konfransı, s. 192-196, 2016.

[4] R.S.Evans, “Electronic health records: Then now and future”, IMIA Yearbook of Medical Informatics, pp. 48-61, 2016.

[5] A history of EHRs: 10 things to know, 2015. https://www.beckershospitalreview.com/healthcare-information-technology/a-history-of-ehrs-10-things-to-know.html

[6] Electronic health records, https://www.cms.gov/Medicare/E-Health/EHealthRecords/index.html#:~:targetText=An%20Electronic%20Health%20Record%20(EHR,to%20streamline%20the%20clinician's%20workflow.

[7] R. Əliquliyev, F. Abdullayeva "Fərdi tibbi məlumatların on-line mühitdə təhlükəsizliyi problemləri," Elektron tibbin multidissiplinar problemləri I respublika elmi-praktiki konfransı, s. 104-109, 2016.

[8] T. Sahama, B. Lane “Security and privacy in ehealth: Is it possible?”, IEEE 15th international conference on eHealth networking, applications and services, pp. 249-253, 2013.

[9] P. Mehndiratta, S. Sachdeva, S. Kulshrestha “A model of privacy and security for electronic health records,” Databases in network information system, pp. 202-213, 2014.

[10] V. Liu, M. A. Musen, T. Chou, “Data breaches of protected health information in the United States”, JAMA, 313(14), pp. 1471-1473, 2015. doi:10.1001/jama.2015.2252.

[11] Electronic health records security and privacy concerns, General articles. https://www.ironmountain.com/resources/general-articles/e/electronic-health-records-security-and-privacy-concerns

[12] G. Dalkılıç, E. Karaarslan, “Elektronik sağlık kayıtlarının veri tabanında T-SQL ile şifrelenmesi ve başarım deneyleri”, Dokuz eylül üniversitesi mühendislik fakültesi fen ve mühendislik dergisi, cilt 20, sayı 58, s. 52-63, 2018.

[13] V. M. Paksoy, “Security and privacy practices of electronic health records in terms of HIPAA standards: A case study in Turkey”, Sağlıq akademisyenleri dergisi, 2019, cilt6, sayı 1, pp.63-69.

[14] E. Karaarslan, “Elektronik sağlık kayıtlarının gizlilik ve mahremiyyeti ", inet-tr, İstanbul december 2015.

SECURITY PROBLEMS OF PERSONAL DATA ON ELECTRONIC HEALTH CARDS

Aytan Ahmadova
Institute of Information Technology of ANAS, Baku, Azerbaijan
ayten.adia1996@gmail.com

Abstract – The article has been investigated security problems of personal data on electron health records. Brief information about electron health cards has been shown, the security threats to them have been classified. Conditions providing security of personal data on electron health cards have been analyzed, rules for access to the physical system and methods of encryption have been shown.

Keywords – *electronic health cards; medical documents; security of personal data; threats; HIPAA.*