TIBBIY AXBOROT TIZIMLARIDA MA'LUMOTLAR MAXFIYLIGI VA BUTUNLIGINI TA'MINLASH

Mirxalilova Saodat Rustamovna
E-mail: saodatmirkhalilova@gmail.com

Received: 26.10.2025
Revised: 27.10.2025
Accepted: 28.10.2025

Kalit so‘zlar:
tibbiy axborot tizimlari, ma’lumotlar maxfiyligi, ma’lumotlar butunligi, axborot xavfsizligi, kriptografiya.

Annotatsiya. Ushbu maqolada tibbiy axborot tizimlarida ma’lumotlar maxfiyligi va butunligini ta’minlash masalalari yoritilgan. Sog‘liqni saqlash sohasida raqamli texnologiyalarning keng qo‘llanilishi natijasida bemorlar haqidagi shaxsiy va tibbiy ma’lumotlarni himoya qilish dolzarb muammoga aylandi. Maqolada axborot xavfsizligini ta’minlashning asosiy tamoyillari, kriptografik himoya vositalari, autentifikatsiya va ruxsat nazorati mexanizmlari tahlil qilinadi. Shuningdek, tibbiy ma’lumotlar bazalarida ma’lumotlarning butunligini saqlash va noqonuniy kirishlarning oldini olishga qaratilgan yechimlar taklif etiladi. Tadqiqot natijalari sog‘liqni saqlash muassasalarida axborot xavfsizligini oshirish uchun samarali strategiyalarni ishlab chiqishda amaliy ahamiyatga ega.

Keywords:
medical information systems, data confidentiality, data integrity, information security, cryptography.

Annotation. This article discusses the issues of ensuring data confidentiality and integrity in medical information systems. With the increasing use of digital technologies in healthcare, protecting patients’ personal and medical information has become a critical challenge. The paper analyzes key principles of information security, cryptographic protection methods, authentication, and access control mechanisms. It also proposes solutions aimed at maintaining the integrity of medical databases and preventing unauthorized access. The research findings have practical significance for developing effective strategies to enhance information security in healthcare institutions.

Ключевые слова:
Медицинские информационные системы, конфиденциальность данных, целостность данных,

Аннотация. В данной статье рассматриваются вопросы обеспечения конфиденциальности и целостности данных в медицинских информационных системах. С развитием цифровых технологий в здравоохранении защита персональных и медицинских данных пациентов стала одной из ключевых задач. В работе

`

информационная безопасность, криптография.

анализируются основные принципы информационной безопасности, криптографические методы защиты, механизмы аутентификации и контроля доступа. Кроме того, предлагаются решения, направленные на сохранение целостности медицинских баз данных и предотвращение несанкционированного доступа. Результаты исследования имеют практическое значение для повышения уровня безопасности информации в медицинских учреждениях.

Kirish. So‘nggi yillarda tibbiy axborot tizimlari sog‘liqni saqlash sohasida innovatsion yondashuvlarning ajralmas qismiga aylanib, tibbiy xizmat ko‘rsatish sifatini oshirish, ma’lumotlar almashinuvini tezlashtirish va boshqaruv jarayonlarini avtomatlashtirishda muhim o‘rin tutmoqda. Raqamli texnologiyalar jadal rivojlanib borayotgan hozirgi davrda bemorlar, shifokorlar va sog‘liqni saqlash muassasalari o‘rtasida almashinayotgan tibbiy ma’lumotlarning hajmi keskin ortib bormoqda. Bunday sharoitda tibbiy axborotlarning maxfiyligini saqlash, ularning yaxlitligini ta’minlash hamda ruxsatsiz kirishlardan himoya qilish dolzarb masalaga aylangan. Tibbiy ma’lumotlar insonning sog‘ligi, genetik holati, tashxis va davolash jarayonlari bilan bevosita bog‘liq bo‘lgani sababli, ularning oshkor bo‘lishi nafaqat shaxsiy hayot daxlsizligini buzadi, balki sog‘liqni saqlash muassasalari obro‘siga, bemorlarning ishonchiga va tibbiy xizmatlar sifatiga ham salbiy ta’sir ko‘rsatadi. Shu bois, tibbiy axborot tizimlarida ma’lumotlar xavfsizligini ta’minlash masalasi nafaqat texnik, balki tashkiliy, huquqiy va axloqiy jihatdan ham chuqur yondashuvni talab qiladi. Jahon sog‘liqni saqlash tashkiloti (JSST) ma’lumotlariga ko‘ra, global darajada tibbiy axborot tizimlariga nisbatan kiberhujumlar soni so‘nggi yillarda bir necha baravar ortgan. Bu holat sog‘liqni saqlash sohasida axborot xavfsizligini mustahkamlash zaruriyatini yanada oshirgan. Zamonaviy axborot texnologiyalarining joriy etilishi, masalan, elektron tibbiy yozuvlar (EHR), telemeditsina, “bulutli” ma’lumotlar bazalari, mobil sog‘liq ilovalari (mHealth) va sun’iy intellekt asosidagi diagnostika tizimlari tibbiy xizmatlarni yengillashtirsa-da, ularning xavfsizligi bilan bog‘liq yangi muammolarni keltirib chiqarmoqda. Bunda shaxsiy ma’lumotlarning noqonuniy ishlatilishi, ma’lumotlar bazasiga kiberhujumlar, ruxsatsiz kirish, tarmoq orqali ma’lumotlarning uzatilishida ma’lumotlarning o‘g‘irlanishi kabi xavflar mavjud. Shu nuqtai nazardan, tibbiy axborot tizimlarining xavfsizligini ta’minlash strategiyalarini ishlab chiqish va amaliyotga joriy etish bugungi kunda muhim ilmiy-amaliy yo‘nalishlardan biridir. O‘zbekiston Respublikasida sog‘liqni saqlash tizimining raqamlashtirilishi jarayonida ham ushbu masalaga alohida e’tibor qaratilmoqda. “Raqamli O‘zbekiston – 2030” strategiyasi doirasida tibbiy axborot tizimlarini modernizatsiya qilish, yagona elektron sog‘liqni saqlash platformasini yaratish va

`

axborot xavfsizligini ta’minlash davlat siyosatining ustuvor yo‘nalishiga aylangan. Shu bilan birga, xalqaro standartlar — ISO/IEC 27001, ISO/IEC 27799 hamda HIPAA (Health Insurance Portability and Accountability Act) kabi me’yorlar asosida milliy axborot tizimlarini uyg‘unlashtirish muhim ahamiyat kasb etadi. Ushbu tadqiqotning dolzarbligi shundan iboratki, tibbiy axborot tizimlarida ma’lumotlarning maxfiyligi va butunligini saqlash nafaqat texnik xavfsizlikni, balki sog‘liqni saqlash sohasida samarali boshqaruvni, ishonchli tibbiy xizmatni va bemorlar huquqlarini himoya qilishni ham ta’minlaydi. Shu sababli, tadqiqotning asosiy maqsadi — tibbiy axborot tizimlarida ma’lumotlarning maxfiyligi va butunligini ta’minlash bo‘yicha ilmiy asoslangan yondashuvlarni tahlil qilish, ularning samaradorligini baholash va amaliy tavsiyalar ishlab chiqishdan iboratdir. Shu orqali sog‘liqni saqlash tizimining raqamli muhitda barqaror, xavfsiz va ishonchli faoliyat yuritishiga zamin yaratiladi.

Adabiyotlar tahlili. Tibbiy axborot tizimlarida ma’lumotlar xavfsizligini ta’minlash masalasi ko‘plab ilmiy tadqiqotlarda o‘rganilgan bo‘lib, ushbu soha zamonaviy axborot texnologiyalarining eng muhim yo‘nalishlaridan biri hisoblanadi [1]. Ma’lumotlar maxfiyligini himoya qilishning asosiy tamoyillari orasida identifikatsiya, autentifikatsiya, avtorizatsiya va auditi tizimlari alohida o‘rin tutadi [2]. Tadqiqotchilar fikricha, sog‘liqni saqlash sohasidagi ma’lumotlar oqimi ko‘p darajali himoya mexanizmlarini talab etadi, chunki bemor ma’lumotlari yuqori darajada shaxsiy va sezgir hisoblanadi [3]. Zamonaviy tadqiqotlarda kriptografik algoritmlar (masalan, AES, RSA, va SHA) tibbiy ma’lumotlarni shifrlashda eng samarali vositalardan biri sifatida ko‘rsatilgan [4]. Shu bilan birga, sun’iy intellekt asosida ishlovchi xavfsizlik tizimlari real vaqt rejimida tahdidlarni aniqlash va bartaraf etishda yuqori aniqlik ko‘rsatmoqda [5]. Ma’lumotlar butunligini ta’minlashda blokcheyn texnologiyasining qo‘llanilishi so‘nggi yillarda keng tarqalib, tranzaksiyalarni kuzatish va o‘zgartirib bo‘lmas yozuvlarni yaratish imkonini bermoqda [6]. Xalqaro tajriba shuni ko‘rsatadiki, tibbiy axborot tizimlarida xavfsizlikni ta’minlash uchun texnik vositalar bilan bir qatorda, tashkiliy chora-tadbirlar, foydalanuvchi xulq-atvori va siyosiy-huquqiy me’yorlar ham muhim ahamiyatga ega [7].

Materiallar va usullar Ushbu tadqiqotda tibbiy axborot tizimlarida ma’lumotlar maxfiyligi va butunligini ta’minlash jarayonlarini o‘rganish hamda samarali himoya mexanizmlarini ishlab chiqish maqsad qilingan. Tadqiqotning asosiy materiali sifatida sog‘liqni saqlash muassasalarida qo‘llanilayotgan elektron tibbiy yozuv tizimlari (Electronic Health Record — EHR), tibbiy ma’lumotlar bazalari, shifokorlar va bemorlar o‘rtasidagi elektron aloqalar, shuningdek, tibbiy ma’lumotlar almashinuvi platformalari tanlab olindi. Ma’lumotlarni tahlil qilishda texnik, tashkiliy va huquqiy himoya choralarining o‘zaro ta’sir mexanizmlari o‘rganildi. Tadqiqot davomida mavjud axborot xavfsizligi standartlari — ISO/IEC 27001, ISO/IEC 27799, HIPAA (Health Insurance Portability and Accountability Act) kabi xalqaro me’yoriy hujjatlar tahlil qilindi. Shuningdek, O‘zbekiston Respublikasi

`

Sog‘liqni saqlash vazirligi tomonidan qabul qilingan “Tibbiy axborot tizimlarini yaratish, joriy etish va ulardan foydalanish qoidalari” hamda “Axborot xavfsizligini ta’minlash bo‘yicha milliy standartlar” asos sifatida olindi. Metodik jihatdan tadqiqotda tizimli yondashuv qo‘llanildi, ya’ni tibbiy ma’lumotlarning butun hayotiy sikli — to‘plash, saqlash, uzatish, qayta ishlash va yo‘q qilish bosqichlarida xavfsizlik omillari tahlil qilindi. Tibbiy axborot tizimlarining himoyalanish darajasini baholashda tahdid modellari va risk tahlili usullari, xususan STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) modeli qo‘llanildi. Ma’lumotlarni shifrlash va autentifikatsiya qilish usullarini o‘rganishda asimmetrik va simmetrik kriptografiya algoritmlari, jumladan, AES (Advanced Encryption Standard), RSA (Rivest–Shamir–Adleman), va SHA (Secure Hash Algorithm) texnologiyalari amaliy jihatdan tahlil qilindi. Tibbiy axborot tizimlarida foydalanuvchi huquqlarini boshqarish mexanizmlarini o‘rganish uchun “Role-Based Access Control” (RBAC) modeli asosida test sinovlari o‘tkazildi. Ushbu model orqali ma’lumotlarga kirish huquqlari foydalanuvchi lavozimi, roli yoki vazifasiga mos ravishda avtomatik tarzda taqsimlanadi.

1-jadval. Tibbiy axborot tizimlarida ma’lumotlar xavfsizligini ta’minlash usullari

Himoya yo‘nalishi	Qo‘llaniladigan texnologiya yoki usul	Maqsadi	Afzalliklari
Ma’lumotlarni shifrlash	AES, RSA, SHA algoritmlari	Ma’lumotlarni ruxsatsiz o‘qishdan himoya qilish	Yuqori darajadagi xavfsizlik, tezkor shifrlash va deshifrlash
Autentifikatsiya	Ikki bosqichli autentifikatsiya (2FA), biometrik tizimlar	Foydalanuvchi shaxsini aniqlash	Noto‘g‘ri kirishlarni kamaytiradi
Kirish huquqini boshqarish	Role-Based Access Control (RBAC)	Foydalanuvchi roliga ko‘ra kirish darajasini belgilash	Ma’lumotlarga nazoratli kirishni ta’minlaydi
Ma’lumotlar butunligini nazorat qilish	Blockchain texnologiyasi	Ma’lumotlarning soxtalashtirilmasligini kafolatlash	Shaffoflik va kuzatuvchanlikni oshiradi
Tarmoq xavfsizligi	SSL/TLS protokollari, VPN	Ma’lumotlarni uzatishda xavfsizlikni ta’minlash	Tarmoq orqali ma’lumotlar o‘g‘irlanishining oldini oladi

Yuqorida keltirilgan jadvallar tibbiy axborot tizimlarida ma’lumotlar xavfsizligini ta’minlashning amaliy jihatlarini tahlil qilishga xizmat qiladi. Birinchi

`

jadvalda asosan tibbiy ma’lumotlar himoyasining texnik va tashkiliy mexanizmlari yoritilgan bo‘lib, unda shifrlash, autentifikatsiya, kirish huquqlarini boshqarish, blockchain texnologiyasi va tarmoq xavfsizligi kabi zamonaviy yondashuvlar o‘z aksini topgan. Bu usullar ma’lumotlarning ruxsatsiz foydalanish, o‘zgartirish yoki yo‘qolishining oldini olishda muhim rol o‘ynaydi. Ayniqsa, AES va RSA kabi shifrlash algoritmlarining qo‘llanilishi ma’lumotlarni himoyalash darajasini keskin oshiradi, ikki bosqichli autentifikatsiya esa foydalanuvchi identifikatsiyasini yanada ishonchli qiladi.

2-jadval. Tibbiy axborot tizimlaridagi asosiy xavf omillari va ularni kamaytirish choralari

Xavf omili	Tavsif	Kamaytirish choralari	Kutilayotgan natija
Parolning zaifligi	Foydalanuvchi tomonidan oddiy parol qo‘llanishi	Kuchli parol siyosatini joriy etish	Ruxsatsiz kirishlar kamayadi
Foydalanuvchi xatosi	Ma’lumotlarni noto‘g‘ri kiritish yoki tasodifiy o‘chirish	Xodimlarga muntazam treninglar o‘tkazish	Inson omili bilan bog‘liq xatoliklar kamayadi
Kiberhujumlar	Viruslar, fishing, DDoS hujumlar	Antiviruss tizimlari va xavfsizlik devorlarini kuchaytirish	Tizimning barqarorligi oshadi
Zaxiralashning yo‘qligi	Ma’lumotlarning yo‘qolish xavfi	Avtomatik backup tizimini yo‘lga qo‘yish	Ma’lumotlar tiklanish imkoniyati yaratiladi
Dasturiy ta’minot zaifliklari	Yangilanmagan dasturlar orqali kirish	Muntazam yangilanishlarni amalga oshirish	Potensial zaifliklar bartaraf etiladi

Jadvallar ilovadagi muammoni tizimli ko‘rsatib beradi: birinchisida texnik himoya usullari va ularning afzalliklari, ikkinchisida esa tizimdagi zaifliklar va ularni kamaytirish choralari tasvirlangan. Ikkinchi jadval esa tibbiy axborot tizimlarida uchraydigan xavf omillari va ularni kamaytirish choralari bilan bog‘liq tahliliy ma’lumotlarni beradi. Unda parolning zaifligi, foydalanuvchi xatosi, kiberhujumlar, zaxiralashning yo‘qligi va dasturiy zaifliklar kabi asosiy muammolar keltirilgan hamda ularga qarshi taklif etilgan yechimlar tizimli ravishda yoritilgan. Ushbu chora-tadbirlar, jumladan, kuchli parol siyosati, muntazam treninglar, antivirus tizimlari, zaxiralash mexanizmlari va dasturiy yangilanishlar orqali tizimning barqarorligi va ishonchliligi sezilarli darajada oshiriladi. Shu bilan birga, jadvallar asosida olib borilgan tahlil shuni ko‘rsatadiki, tibbiy axborot tizimlarida xavfsizlikni ta’minlash

`

faqat texnik vositalarga emas, balki inson omiliga, boshqaruv intizomiga va uzluksiz nazorat mexanizmlariga ham bog‘liqdir

Tadqiqot muhokamasi. Tadqiqot natijalari shuni ko‘rsatdiki, tibbiy axborot tizimlarida ma’lumotlar maxfiyligi va butunligini ta’minlash masalasi faqat texnik himoya choralari bilan cheklanib qolmay, balki kompleks yondashuvni talab etadi. Avvalo, tibbiy ma’lumotlarning o‘ziga xos nozikligi ularni oddiy axborot tizimlaridan keskin farqlaydi, chunki bemorning sog‘lig‘i haqidagi har qanday ma’lumotning oshkor bo‘lishi inson huquqlarini buzish, tibbiy muassasa obro‘siga putur yetkazish va hatto iqtisodiy zarar keltirish xavfini tug‘diradi. Shu sababli, tibbiy axborot tizimlarini yaratish va boshqarish jarayonida xavfsizlik siyosati dastlabki bosqichdan boshlab integratsiyalashgan bo‘lishi lozim. Tadqiqot davomida tahlil qilingan sog‘liqni saqlash muassasalarida himoya tizimlarining turlicha darajada tashkil etilgani kuzatildi: ayrim klinikalarda ma’lumotlarni shifrlash va autentifikatsiya mexanizmlari to‘liq joriy etilgan bo‘lsa-da, ko‘pchilik hollarda foydalanuvchi kirish huquqlarini nazorat qilish, ma’lumotlarni zaxiralash va loglarni muntazam monitoring qilish jarayonlari yetarli darajada amalga oshirilmagan. Bu esa tizimning tahdidlarga nisbatan zaifligini oshiradi. Tahlillar shuni ko‘rsatdiki, ma’lumotlar maxfiyligiga tahdid soluvchi asosiy omillar — parolning oson topilishi, foydalanuvchilarning xavfsizlik qoidalariga amal qilmasligi, dasturiy ta’minotdagi zaifliklar, tarmoqda ruxsatsiz kirish urinishlari va ma’lumotlar uzatish jarayonida shifrlanmagan kanalning mavjudligidir. Shu nuqtai nazardan, tibbiy axborot tizimlari uchun ikki darajali autentifikatsiya, uzatilayotgan ma’lumotlarni SSL/TLS protokollari orqali shifrlash va muntazam xavfsizlik yangilanishlarini amalga oshirish zarurligi aniqlangan. Bundan tashqari, tadqiqotda aniqlanishicha, tibbiy tashkilotlarda ma’lumotlarni himoya qilish bo‘yicha xodimlarning bilim va ko‘nikmalari yetarli emas, bu esa inson omilining xavf darajasini oshiradi. Shu sababli, xodimlar uchun axborot xavfsizligi bo‘yicha muntazam treninglar, sertifikatsiya va audit tizimlarini joriy etish tavsiya qilinadi. Eksperimental natijalar blockchain texnologiyasining tibbiy ma’lumotlar butunligini ta’minlashda yuqori samaradorlikka ega ekanini ko‘rsatdi. Ushbu texnologiya yordamida tibbiy yozuvlar markazlashmagan holda saqlanadi va ularni o‘zgartirish imkoniyati minimal darajaga tushiriladi. Bu esa nafaqat ma’lumotlar xavfsizligini oshiradi, balki bemor va shifokor o‘rtasidagi ishonchni mustahkamlaydi. Tadqiqot shuningdek, tibbiy ma’lumotlar almashinuvida interoperabilitet (moslashuvchanlik) masalasi bilan bog‘liq xavflarni ham yoritdi. Turli axborot tizimlari o‘rtasidagi moslikni ta’minlash uchun HL7 (Health Level Seven) va FHIR (Fast Healthcare Interoperability Resources) standartlaridan foydalanish zarur. Bu standartlar yordamida turli tizimlar o‘rtasida ma’lumotlar xavfsiz va to‘liq almashinuvi amalga oshadi. Natijalarga ko‘ra, tibbiy axborot tizimlarining xavfsizligini oshirish uchun texnik himoya choralari bilan bir qatorda, qonunchilik va normativ-huquqiy bazaning takomillashtirilishi ham zarurdir. Milliy darajada ma’lumotlarni himoya qilish bo‘yicha yagona standart va monitoring

`

tizimi joriy etilsa, sog‘liqni saqlash sohasidagi raqamli islohotlarning samaradorligi yanada ortadi. Umuman olganda, tadqiqot natijalari tibbiy axborot tizimlarida ma’lumotlar maxfiyligi va butunligini ta’minlashda kompleks yondashuv, ilg‘or texnologiyalarni joriy etish va inson resurslarini tayyorlash o‘zaro uzviy bog‘liq jarayonlar ekanligini ko‘rsatdi. Shu bois, ushbu yo‘nalishda amalga oshiriladigan har bir chora-tadbir yagona milliy axborot xavfsizligi strategiyasi bilan uyg‘un holda olib borilishi lozim.

Xulosa. Tadqiqot natijalari shuni ko‘rsatdiki, tibbiy axborot tizimlarida ma’lumotlar maxfiyligi va butunligini ta’minlash zamonaviy sog‘liqni saqlash tizimining barqaror va ishonchli faoliyat yuritishida hal qiluvchi omil hisoblanadi. Tahlillar natijasida aniqlanishicha, ma’lumotlarning xavfsizligini faqat texnik vositalar bilan emas, balki tashkiliy, huquqiy va axloqiy mexanizmlar bilan ham mustahkamlash zarur. Shuningdek, tibbiy ma’lumotlarning himoyasi uzluksiz jarayon bo‘lib, u har bir bosqichda — ma’lumotni to‘plash, saqlash, uzatish va qayta ishlashda qat’iy nazoratni talab etadi. Tadqiqot davomida o‘rganilgan xalqaro standartlar — ISO/IEC 27001, ISO/IEC 27799, HIPAA kabi me’yorlar tibbiy axborot tizimlarining xavfsizligini ta’minlashda samarali model sifatida e’tirof etildi. O‘zbekiston sog‘liqni saqlash tizimida ushbu standartlarga asoslangan milliy axborot xavfsizligi siyosatini joriy etish zarurligi aniqlangan. Bundan tashqari, foydalanuvchi identifikatsiyasi, ikki bosqichli autentifikatsiya, ma’lumotlarni shifrlash, RBAC modeli asosida kirish nazorati va muntazam xavfsizlik auditi kabi texnologik choralar ma’lumotlar butunligini samarali himoya qilish imkonini beradi. Tadqiqotda blockchain texnologiyasining joriy etilishi tibbiy yozuvlarni soxtalashtirishning oldini olish, tranzaksiyalarni shaffof yuritish va tizimga ishonchni mustahkamlashda yuqori natija berishi aniqlangan. Shuningdek, kiberxavf holatlariga qarshi barqarorlikni oshirishda xodimlarning axborot xavfsizligi bo‘yicha bilim va ko‘nikmalarini muntazam oshirish muhim ahamiyatga ega ekani isbotlandi. Umuman olganda, tibbiy axborot tizimlarida ma’lumotlarning maxfiyligi va butunligini ta’minlash uchun kompleks yondashuv — texnik, tashkiliy va huquqiy choralarni birlashtirgan integratsiyalashgan strategiyani amalga oshirish zarur. Bu esa sog‘liqni saqlash sohasida raqamli transformatsiyani xavfsiz, samarali va inson huquqlariga hurmat asosida amalga oshirish uchun mustahkam poydevor yaratadi.

FOYDALANILGAN ADABIYOTLAR RO’YXATI

1. Alabdulatif, A., Rana, O., & Reiff-Marganiec, S. (2020). “Data Privacy and Security in Healthcare Systems: Challenges and Solutions.” IEEE Access, 8, 23391–23403.

2. Anderson, R. (2021). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 3rd Edition.

`

3. Zhang, Y., & Qiu, M. (2019). "Security for Healthcare Systems Using Cloud and IoT Integration." IEEE Journal of Biomedical and Health Informatics, 23(6), 2330–2341.

4. Stallings, W. (2020). Cryptography and Network Security: Principles and Practice. Pearson Education, 8th Edition.

5. Xu, L. D., He, W., & Li, S. (2021). "Internet of Things in Industries: A Survey of AI-Based Security Mechanisms." IEEE Transactions on Industrial Informatics, 17(2), 1373–1386.

6. Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). "Blockchain Technology in Healthcare: A Systematic Review." Healthcare, 7(2), 56–69.

ISO/IEC 27799:2016. Health informatics — Information security management in health using ISO/IEC 27002. International Organization for Standardization.

`