



**TIBBIY MA'LUMOTLARNI OSHKOR QILISHDA MA'MURIY
JAVOBGARLIK: RAQAMLI TIBBIYOT SHAROITIDA HUQUQIY
MUAMMOLAR VA TAKLIFLAR**

Yusupova Farangiz O'ktam qizi

O'zbekiston Respublikasi IIV Akademiyasi

Ma'muriy huquq kafedrası dotsenti

<https://doi.org/10.5281/zenodo.20431898>

Annotatsiya. Mazkur tezisda raqamli sog'liqni saqlash tizimida tibbiy ma'lumotlarni himoya qilishning ma'muriy-huquqiy asoslari tahlil qilinadi. Elektron tibbiy kartalar, telemeditsina va sun'iy intellekt texnologiyalarining joriy etilishi tibbiy sir daxlsizligini ta'minlash masalasini dolzarb muammoga aylantirmoqda. Tadqiqotda tibbiy ma'lumotlarni noqonuniy oshkor qilish bilan bog'liq xavflar, amaldagi qonunchilikdagi bo'shliqlar hamda ma'muriy javobgarlikni takomillashtirish bo'yicha takliflar ishlab chiqilgan.

Kalit so'zlar. Tibbiy sir, shaxsga doir ma'lumotlar, ma'muriy javobgarlik, raqamli tibbiyot, axborot xavfsizligi, teletibbiyot.

**АДМИНИСТРАТИВНАЯ ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ
МЕДИЦИНСКОЙ ИНФОРМАЦИИ: ПРАВОВЫЕ ПРОБЛЕМЫ И
ПРЕДЛОЖЕНИЯ В УСЛОВИЯХ ЦИФРОВОЙ МЕДИЦИНЫ**

Аннотация. В данной статье анализируются административно-правовые основы защиты медицинских данных в условиях цифровизации системы здравоохранения. Внедрение электронных медицинских карт, телемедицины и технологий искусственного интеллекта усиливает необходимость обеспечения конфиденциальности медицинской тайны.

Contact: 99 826 99 56



Исследуются риски незаконного раскрытия медицинской информации, пробелы действующего законодательства, а также предлагаются меры по совершенствованию административной ответственности за нарушение безопасности медицинских данных.

Ключевые слова. Медицинская тайна, персональные данные, административная ответственность, цифровое здравоохранение, информационная безопасность, телемедицина.

ADMINISTRATIVE LIABILITY FOR THE DISCLOSURE OF MEDICAL INFORMATION: LEGAL ISSUES AND PROPOSALS IN THE CONTEXT OF DIGITAL MEDICINE

Abstract. This article analyzes the administrative and legal foundations for the protection of medical data in the context of healthcare digitalization. The implementation of electronic medical records, telemedicine, and artificial intelligence technologies increases the importance of ensuring the confidentiality of medical secrecy. The study examines the risks of unlawful disclosure of medical information, identifies gaps in current legislation, and proposes measures to improve administrative liability for violations related to medical data security.

Keywords. Medical secrecy, personal data, administrative liability, digital healthcare, information security, telemedicine.

Raqamli transformatsiya jarayonida sogʻliqni saqlash tizimida elektron axborot texnologiyalaridan foydalanish koʻlami tobora kengayib bormoqda. Bugungi kunda elektron tibbiy kartalar, laboratoriya axborot tizimlari, telemeditsina platformalari, mobil tibbiy ilovalar hamda sunʼiy intellekt texnologiyalarining amaliyotga joriy etilishi natijasida tibbiy maʼlumotlarni yigʻish, saqlash, qayta ishlash va uzatish hajmi keskin ortmoqda. Mazkur jarayon sogʻliqni saqlash tizimini





modernizatsiya qilish va tibbiy xizmatlar sifatini oshirishga xizmat qilayotgan bo'lsa-da, fuqarolarning shaxsiy hayoti daxlsizligi, tibbiy sir va maxfiy ma'lumotlarni himoya qilish bilan bog'liq huquqiy masalalarni yanada dolzarb ahamiyat kasb etishiga sabab bo'lmoqda.

Tibbiy ma'lumotlar shaxsga doir ma'lumotlarning eng nozik va kuchli huquqiy himoyaga muhtoj toifalaridan biri hisoblanadi. Chunki ushbu ma'lumotlar shaxsning sog'lig'i, tashxisi, davolanish jarayoni, biologik va genetik xususiyatlari, psixologik holati, reproduktiv salomatligi hamda boshqa maxfiy jihatlarini o'z ichiga oladi. Shu sababli bunday ma'lumotlarning noqonuniy ravishda oshkor qilinishi yoki uchinchi shaxslarga tarqatilishi fuqarolarning sha'ni, qadr-qimmati, ishchanlik obro'si va konstitutsiyaviy huquqlariga jiddiy zarar yetkazishi mumkin.

O'zbekiston Respublikasi Ma'muriy javobgarlik to'g'risidagi kodeksining 46-moddasi fuqarolarning shaxsiy hayoti daxlsizligini himoya qilishga qaratilgan muhim huquqiy norma sifatida alohida ahamiyatga ega. Mazkur moddada tibbiy sirlarni oshkor qilishning alohida ko'rsatilgani sog'liqni saqlash tizimida tibbiy ma'lumotlarning maxfiyligi davlat tomonidan huquqiy himoya ostiga olinganligini anglatadi. Ushbu norma orqali bemorning roziligisiz uning sog'lig'iga oid ma'lumotlarni oshkor qilish ma'muriy javobgarlikka sabab bo'lishi belgilangan.

Ayniqsa, raqamli tibbiyot va elektron sog'liqni saqlash tizimlari rivojlanayotgan hozirgi sharoitda tibbiy ma'lumotlarni noqonuniy oshkor qilish xavfi yanada ortib bormoqda. Elektron tibbiy kartalar, laboratoriya natijalari, telemeditsina yozuvlari, diagnostika ma'lumotlari, biometrik va genetik ma'lumotlarning internet tarmoqlari orqali uzatilishi yoki bulutli texnologiyalarda saqlanishi axborot xavfsizligi bilan bog'liq yangi tahdidlarni yuzaga keltirmoqda. Bemorning roziligisiz uning tibbiy ma'lumotlarini ijtimoiy tarmoqlarda tarqatish, messengerlar orqali yuborish yoki uchinchi shaxslarga taqdim etish fuqaroga nafaqat ma'naviy, balki moddiy zarar ham yetkazishi mumkin.





Mazkur modda asosida:

- shifokorlar;
- hamshiralar;
- laboratoriya xodimlari;
- klinika ma'muriyati;
- tibbiy axborot tizimi operatorlari;
- telemeditsina platformalari administratorlari

tomonidan tibbiy ma'lumotlarni noqonuniy oshkor qilish ma'muriy javobgarlikni keltirib chiqaradi.

Xorijiy davlatlar tajribasida tibbiy ma'lumotlarni himoya qilish va ularni noqonuniy oshkor qilganlik uchun javobgarlik masalasiga alohida e'tibor qaratilgan. Ayniqsa, raqamli sog'liqni saqlash tizimlari rivojlangan davlatlarda tibbiy ma'lumotlar "maxsus toifadagi shaxsiy ma'lumotlar" sifatida kuchaytirilgan huquqiy himoya ostiga olingan.

Jumladan, European Union GDPR (General Data Protection Regulation) qoidalariga ko'ra, tibbiy ma'lumotlar eng yuqori darajada himoyalaniishi lozim bo'lgan maxsus ma'lumotlar toifasiga kiradi. Mazkur reglamentga asosan, bemorning aniq rozilgisiz uning sog'lig'iga oid ma'lumotlarni qayta ishlash, uchinchi shaxslarga uzatish yoki oshkor qilish taqiqlanadi. Tibbiy ma'lumotlarni noqonuniy oshkor qilgan tashkilotlarga yillik daromadining katta foizigacha miqdorda jarimalar qo'llanishi mumkin. Shuningdek, GDPR ma'lumotlarni minimallashtirish, anonimlashtirish va "privacy by design" prinsiplarini majburiy tartibda belgilaydi.

AQSh tajribasida esa United States Department of Health and Human Services tomonidan qabul qilingan HIPAA (Health Insurance Portability and





Accountability Act) tibbiy ma'lumotlarni himoya qilishning asosiy huquqiy mexanizmlaridan biri hisoblanadi. Ushbu tizimga ko'ra, shifoxonalar, sug'urta kompaniyalari va tibbiy platformalar bemorning ma'lumotlarini maxsus himoya choralarisiz saqlashi yoki tarqatishi mumkin emas. HIPAA talablarini buzganlik uchun katta miqdordagi moliyaviy jarimalar, faoliyatni cheklash va ayrim hollarda jinoiy javobgarlik ham qo'llaniladi.

Germany tajribasida tibbiy ma'lumotlarni himoya qilish federal ma'lumotlarni himoya qilish qonunchiligi orqali amalga oshiriladi. Germaniya qonunchiligida shifokorlar va tibbiyot xodimlari uchun "professional maxfiylik majburiyati" juda qat'iy belgilangan bo'lib, bemor ma'lumotlarini oshkor qilish nafaqat ma'muriy, balki kasbiy javobgarlikka ham sabab bo'ladi. Bundan tashqari, elektron tibbiy kartalar bilan ishlovchi axborot tizimlari majburiy kiberxavfsizlik auditidan o'tkaziladi.

South Korea sog'liqni saqlashni raqamlashtirish bo'yicha eng ilg'or davlatlardan biri hisoblanadi. Ushbu davlatda tibbiy ma'lumotlarni noqonuniy tarqatish yoki internetda joylashtirish uchun ma'muriy va jinoiy javobgarlik choralarining qat'iy tizimi mavjud. Ayniqsa, telemeditsina va mobil sog'liqni saqlash platformalari uchun alohida axborot xavfsizligi standartlari ishlab chiqilgan.

Kazakhstan qonunchiligida ham tibbiy ma'lumotlar shaxsiy ma'lumotlarning maxsus turi sifatida e'tirof etiladi. Qozog'iston Respublikasining sog'liqni saqlash kodeksida bemorning rozilgisiz uning sog'lig'iga oid ma'lumotlarni oshkor qilish taqiqlangan hamda bunday holatlar uchun ma'muriy javobgarlik nazarda tutilgan.

Mazkur xorijiy tajribalar shuni ko'rsatadiki, raqamli tibbiyot rivojlangan sari tibbiy ma'lumotlarni himoya qilishning maxsus huquqiy mexanizmlarini yaratish, elektron tibbiy ma'lumotlarning huquqiy maqomini aniq belgilash hamda ularni noqonuniy oshkor qilganlik uchun qat'iy ma'muriy javobgarlik choralarini joriy etish zarur hisoblanadi.





Shu bilan birga, amaldagi normada “tibbiy sir” tushunchasi umumiy ko‘rinishda nazarda tutilgan bo‘lib, elektron tibbiy ma’lumotlar, raqamli platformalar, bulutli texnologiyalar, sun’iy intellekt orqali qayta ishlanadigan ma’lumotlar hamda telemeditsina xizmatlari doirasidagi axborotlarning huquqiy maqomi yetarlicha aniq belgilanmagan. Bu esa amaliyotda turli huquqiy kolliziyalar va javobgarlikni qo‘llashda murakkabliklarni yuzaga keltirmoqda.

Shu sababli Ma’muriy javobgarlik to‘g‘risidagi kodeksning 46-moddasini zamonaviy raqamli sog‘liqni saqlash tizimi talablaridan kelib chiqib takomillashtirish maqsadga muvofiq hisoblanadi. Xususan:

- elektron tibbiy ma’lumotlarni noqonuniy tarqatish;
- tibbiy axborot tizimlariga ruxsatsiz kirish;
- himoyalangan messenjerlar va platformalar orqali yuborish;
- bemorning roziligisiz internet tarmoqlarida joylashtirish;
- sun’iy intellekt tizimlari orqali noqonuniy qayta ishlash

uchun alohida ma’muriy javobgarlik choralari belgilash zarur.

Mazkur yondashuv fuqarolarning tibbiy sir daxlsizligini ta’minlash, sog‘liqni saqlash tizimida axborot xavfsizligini mustahkamlash, raqamli tibbiyotga bo‘lgan ishonchni oshirish hamda zamonaviy raqamli huquqiy munosabatlarni samarali tartibga solishga xizmat qiladi.

Foydalanilgan adabiyotlar ro‘yxati

1. O‘zbekiston Respublikasining Konstitutsiyasi. – Toshkent: O‘zbekiston, 2023.





2. O‘zbekiston Respublikasining Ma‘muriy javobgarlik to‘g‘risidagi kodeksi. – Toshkent: Adolat, 2025.
3. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni // Qonunchilik ma’lumotlari milliy bazasi.
4. O‘zbekiston Respublikasining “Fuqarolar sog‘lig‘ini saqlash to‘g‘risida”gi Qonuni // Qonunchilik ma’lumotlari milliy bazasi.
5. O‘zbekiston Respublikasi Prezidentining sog‘liqni saqlash tizimini raqamlashtirish va axborot texnologiyalarini joriy etishga oid farmon va qarorlari.
6. O‘zbekiston Respublikasi Vazirlar Mahkamasining sog‘liqni saqlash tizimida axborot texnologiyalarini joriy etish bo‘yicha qarorlari.
7. European Union. General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
8. United States Department of Health and Human Services. Health Insurance Portability and Accountability Act (HIPAA), 1996.
9. World Health Organization. Global Strategy on Digital Health 2020–2025. Geneva, 2021.
10. United Nations. Universal Declaration of Human Rights. New York, 1948.
11. Soliyev N., Axmedov B. Axborot xavfsizligi va shaxsga doir ma’lumotlarni himoya qilish. – Toshkent: TDYU nashriyoti, 2022.
12. Yuldashev A. Raqamli huquq va kiberxavfsizlik masalalari. – Toshkent: Yuridik adabiyotlar publish, 2023.





13. Kuner C. Transborder Data Flows and Data Privacy Law. – Oxford University Press, 2013.
14. Bygrave L.A. Data Privacy Law: An International Perspective. – Oxford University Press, 2014.
15. Warren S., Brandeis L. The Right to Privacy // Harvard Law Review. – 1890. – Vol. 4. – № 5.
16. Tavani H. Ethics and Technology: Controversies, Questions and Strategies for Ethical Computing. – Wiley, 2016.
17. Richards N., King J. Big Data Ethics // Wake Forest Law Review. – 2014. – Vol. 49.
18. OECD Health Data Governance Principles. Paris, 2017.
19. European Health Data Space (EHDS) Regulation materials. Brussels, 2024.
20. Qozog‘iston Respublikasining “Xalq salomatligi va sog‘liqni saqlash tizimi to‘g‘risida”gi Kodeksi.

