

6. Про фінансові послуги та фінансові компанії: від 15 лют. 2021 р. № 1953-IX URL: <https://zakon.rada.gov.ua/laws/show/1953-20#Text>

7. Про затвердження Програми стратегічного розвитку Державної служби фінансового моніторингу України на період до 2024 року: Наказ Міністерства фінансів України від 17 січ. 2022 р. № 16. URL: <https://fiu.gov.ua/assets/userfiles/0350/strategy/16.pdf>

8. Про Національну стратегію доходів до 2030 року: Постанова Національної комісії з цінних паперів та фондового ринку від 01 трав. 2024 р. № 542. URL: https://www.mof.gov.ua/uk/news/pro_natsionalnu_strategiiu_dokhodiv_do_2030_roku-4369

DOI <https://doi.org/10.30525/978-9934-26-493-1-114>

EXERCISE OF THE RIGHT TO HEALTH IN THE FIELD OF INFORMATION TECHNOLOGIES: LEGAL AND ETHICAL ASPECTS

РЕАЛІЗАЦІЯ ПРАВА НА ЗДОРОВ'Я У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ: ПРАВОВІ ТА ЕТИЧНІ АСПЕКТИ

Shambura D. V.

*PhD in Law,
Postdoctoral Student at the Department
of Civil Law Disciplines and Statistics,
International Humanitarian University
Odesa, Ukraine*

Щамбура Д. В.

*доктор філософії в галузі права,
докторант кафедри цивільно-
правових дисциплін та статистики
Міжнародний гуманітарний
університет
м. Одеса, Україна*

Реалізація права на здоров'я у сучасному світі все більше пов'язується з розвитком інформаційних технологій (ІТ), зокрема з використанням цифрових медичних записів, телемедицини, мобільних додатків для здоров'я та аналітики великих даних. Цей процес підсилює доступ до медичної допомоги, прискорює діагностику та підвищує ефективність охорони здоров'я, проте породжує значні правові та етичні виклики – від захисту персональних даних до забезпечення якості медичної допомоги й відповідальності за помилки в цифровому середовищі. У тезах нижче проаналізовано ключові правові рамки (законодавство України та міжнародні стандарти), етичні

проблеми, судову практику та рекомендації щодо вдосконалення регулювання і практики цифрового охорони здоров'я [1].

Право на охорону здоров'я та медичну допомогу закріплено у вітчизняному законодавстві: Основи законодавства України про охорону здоров'я (Закон України № 2801-XII) закладають загальні принципи державної політики в галузі охорони здоров'я. У поєднанні з іншими нормативними актами ці положення утворюють правову базу для цифровізації медичної сфери [2].

Закон України «Про захист персональних даних» (№ 2297-VI) регулює відносини, пов'язані з обробкою персональних даних, та має особливе значення для медичної інформації як чутливого класу даних. У поєднанні з європейськими підходами (зокрема принципами GDPR, які впливають на національну практику та очікування пацієнтів) це створює обов'язки для медичних закладів і розробників ІТ-систем щодо безпеки, мінімізації збору даних і забезпечення прав суб'єктів даних. [3].

За умов воєнного стану в Україні Міністерство охорони здоров'я запровадило нормативні акти, що визначають організаційні й процедурні основи застосування телемедицини (зокрема Наказ МОЗ №1062 від 20.06.2022 та Стратегія розбудови телемедицини, схвалена розпорядженням 2023 р.). Ці документи регламентують права й обов'язки медичних працівників, порядок надання меддопомоги дистанційно, вимоги до документування й передачі даних [4,5].

Всесвітня організація охорони здоров'я (WHO) у глобальній стратегії по цифровому здоров'ю (Global strategy on digital health 2020-2025) та суміжних матеріалах підкреслює необхідність інтегрованого підходу: стандартизація, забезпечення інтероперабельності, захист даних та етичні принципи в цифровому здоров'ї. Для національної політики це є орієнтиром для розробки стратегії й операційних планів [6].

Медична інформація належить до чутливих персональних даних; її витік або несанкціонований доступ може призвести до порушення прав пацієнта. Водночас практика застосування хмарних сервісів, сторонніх платформ телемедицини та аналітики даних ускладнює застосування гарантованих законом заходів захисту (наприклад, забезпечення згоди, контролю доступу, шифрування, аудитних журналів). Закон про персональні дані та відповідні МОЗ-накази зобов'язують запроваджувати технічні та організаційні захисні заходи, але їх імплементація на практиці нерідко відстає [3].

Недостатня сумісність систем, відсутність загальних стандартів електронних медичних записів і слабкий захист мереж роблять медичні системи вразливими до кіберзагроз. Це створює ризики для цілісності

даних (відсутність довіри до даних), що у свою чергу впливає на якість медичної допомоги. WHO і національні стратегії наголошують на необхідності стандартів інтероперабельності та кібергігієни [6.]

Телемедицина змінює формат взаємодії пацієнт – лікар: що робити в разі помилкової діагностики на відстані, які критерії стандартів надання допомоги й яка відповідальність лікаря та платформи? Український Наказ МОЗ №1062 містить правила організації телемедичної допомоги, але питання професійної відповідальності, стандартів доказовості та лікарської етики залишаються предметом судових спорів та наукових дискусій [4].

Цифрові інструменти змінюють механіку отримання інформованої згоди (наприклад, «згоди» при реєстрації в мобільному додатку), що створює етичні ризики щодо реальної обізнаності пацієнта. Також необхідно враховувати цифрове розриви (digital divide): доступ до інтернету і технічної грамотності залишається нерівномірним, що може посилювати нерівність у доступі до медичної допомоги [7].

Використання алгоритмів машинного навчання у діагностиці та прийнятті клінічних рішень ставить етичну проблему пояснюваності (explainability). Пацієнт і лікар мають розуміти підґрунтя клінічної рекомендації; відсутність прозорості ускладнює встановлення відповідальності й довіри. WHO та наукові публікації наполягають на контролі якості алгоритмів і впровадженні принципів «етичного ШІ» у сфері охорони здоров'я [6].

Агреговані дані про стан здоров'я можуть бути цінними для громадського здоров'я (епіднагляд, планування ресурсів), але використання таких даних повинно бути етично виправданим та легітимним, з обов'язковим знеособленням та правовими гарантіями. Європейські стандарти захисту здоров'я підкреслюють обережність при зберіганні й обробці біометричних та медичних даних [8].

Українська судова практика щодо телемедицини та цифрових медичних записів ще формується. Окремі наукові огляди й аналітичні матеріали вказують на наявні спори щодо доступу до медичної інформації, відповідальності медзакладу за обробку даних та наслідків порушень конфіденційності (аналіз практики Єдиного державного реєстру судових рішень і тематичних досліджень). Загальноєвропейська практика (ECHR) підкреслює конституційні гарантії конфіденційності медичної інформації та право на життя/якість медичної допомоги, що формує орієнтири для національних судів.

Рішення Ірпінського міського суду (справа № 367/9129/19) – 01.06.2022. Коротко: справа, у якій суд послався на ст.39-1 Закону №2801-ХІІ та визнав порушення права на таємницю про стан здоров'я;

наведено відшкодування моральної шкоди (приклад практики щодо лікарської таємниці) [9].

Постанова (апеляція) у справі № 490/7421/20 – 08.11.2021 (приклад: розголошення медичної інформації). Коротко: суд апеляційної інстанції та/або касація розглядали питання поширення медичної інформації та відшкодування моральної шкоди. [10].

Оглядова позиція/дайджест Верховного Суду (щодо права на таємницю стану здоров'я; з прикладами практики). Коротко: офіційні матеріали ВС/дайджести констатують, що стаття 286 ЦК і ст.39-1 Закону про охорону здоров'я забезпечують захист лікарської таємниці; у практиці — відшкодування моральної шкоди за розголошення. [11].

Європейський суд з прав людини – справа «М.К. v. Ukraine» (щодо розголошення медичних записів і права на приватне життя). Коротко: прецедент ЄСПЛ, який розглядав розголошення медичної інформації іншими державними органами і констатував втручання у приватне життя; корисний для інтерпретації національної практики. [12]

На підставі аналізу законодавства, міжнародних рекомендацій та наукових оглядів пропонується ключові напрямки вдосконалення: уніфікація стандартів для електронних медичних записів (ЕМЗ) – створити обов'язкові технічні та семантичні стандарти інтероперабельності (формати, API, структури метаданих). Це підвищить якість передачі інформації й зменшить ризики клінічних помилок.

Посилення вимог до захисту медичних даних – запровадити мінімально необхідні технічні заходи (шифрування, багатофакторна автентифікація, аудитні логи) й регулярні незалежні аудити безпеки, особливо для комерційних телемедичних платформ. Законодавчі норми про персональні дані повинні мати конкретні імплементаційні стандарти у медичній сфері.

Регуляція застосування ШІ в медицині – встановити вимоги до валідації алгоритмів, прозорості та моніторингу ефективності в клінічній практиці; обов'язкова клінічна оцінка й сертифікація перед впровадженням у масове використання.

Підвищення цифрової грамотності пацієнтів і медпрацівників – програми навчання для лікарів щодо стандартів телемедицини й кібергієни; інформаційні кампанії для пацієнтів про права та ризики цифрових сервісів.

Чітка модель відповідальності – законодавче уточнення відповідальності платформ, розробників і медичного персоналу у випадку шкоди внаслідок цифрових технологій; судова практика повинна розвиватися з урахуванням нових технологічних реалій.

Інформаційні технології створюють унікальні можливості для реалізації права на здоров'я – підвищують доступність, оперативність і персоналізацію медичної допомоги. Разом з тим цифровізація ставить низку правових та етичних викликів: захист персональних і медичних даних, забезпечення якості та безпеки дистанційної допомоги, прозорість алгоритмів і справедливий доступ для вразливих груп. Для збалансованого розвитку цифрового здоров'я необхідна комплексна політика: поєднання чітких правових гарантій (зокрема у сфері персональних даних), технічних стандартів, етичних принципів та практичних інструментів контролю та відповідальності. Впровадження запропонованих заходів сприятиме тому, щоб цифрові технології не лише підвищували ефективність системи охорони здоров'я, а й забезпечували реальну й захищену реалізацію права на здоров'я для кожної людини.

Література:

1. World Health Organization. (2020). Global strategy on digital health 2020-2025. WHO. URL: <https://www.who.int/docs/>
2. Основи законодавства України про охорону здоров'я: Закон України № 2801-XII від 19.11.1992. URL: <https://zakon.rada.gov.ua/laws/show/2801-12#Text>
3. Про захист персональних даних: Закон України № 2297-VI від 21.09.2012. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
4. Про організацію надання медичної допомоги із застосуванням телемедицини в умовах воєнного стану: Наказ МОЗ України від 20.06.2022 № 1062. URL: <https://zakon.rada.gov.ua/laws/show/z0728-22#Text> ;
5. Про схвалення Стратегії розвитку імунопрофілактики та захисту населення від інфекційних хвороб, яким можна запобігти шляхом проведення імунопрофілактики, на період до 2030 року та затвердження операційного плану її реалізації у 2023-2025 роках: Розпорядження Кабінету Міністрів України від 1 червня 2023 р. № 562-р. URL: <https://zakon.rada.gov.ua/laws/show/562-2023-%D1%80#Text>
6. Global strategy on digital health 2020-2025. Geneva: World Health Organization; 2021. URL: https://www.who.int/docs/default-source/documents/g4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf?utm_source=chatgpt.com
7. Nittari G., et al., Telemedicine Practice: Review of the Current Ethical and Legal Issues. International Journal (article; 2020). URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC7757597/?utm_source=chatgpt.com

8. Raluca Bercea. Protection of health related data and privacy rights. URL: https://rm.coe.int/protection-of-health-related-data-and-privacy-rights/16809823ef?utm_source=chatgpt.com

9. Рішення від 01.06.2022 по справі № 367/9129/19 Ірпінський міський суд Київської області. URL: https://zakononline.ua/court-decisions/show/104749099?utm_source=chatgpt.com

10. Постанова від 08.11.2021 по справі № 490/7421/20 Миколаївський апеляційний суд. URL: https://zakononline.ua/court-decisions/show/101051012?utm_source=chatgpt.com

11. Огляд судової практики Касаційного цивільного суду у складі Верховного Суду справах зі спорів, що виникають у сфері охорони здоров'я.

URL: https://supreme.court.gov.ua/userfiles/media/new_folder_for_uploads/supreme/2021_12_ohorona_zdor.pdf?utm_source=chatgpt.com

12. Справа «М.К. проти України» (Заява № 24867/13). URL: https://zakon.rada.gov.ua/laws/main/974_i18?utm_source=chatgpt.com#Text