

УДК: 347.121.2

DOI <https://doi.org/10.24144/2307-3322.2024.82.2.22>

ПРАВОВА ОХОРОНА ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я В УКРАЇНІ

Діордіца І.В.,

*доктор юридичних наук, професор,
професор кафедри приватного та публічного права
Київського Національного університету технологій та дизайну
ORCID: <https://orcid.org/0000-0001-7765-6591>
e-mail: dior-law@ukr.net*

Коваленко І.А.,

*кандидат юридичних наук, доцент,
доцент кафедри приватного та публічного права
Київського Національного університету технологій та дизайну
ORCID: <https://orcid.org/0000-0001-7595-777X>
e-mail: ilchenkoin@ukr.net*

Коваль О.М.,

*кандидат юридичних наук, доцент,
доцент кафедри приватного та публічного права
Київського Національного університету технологій та дизайну*

Діордіца І.В., Коваленко І.А., Коваль О.М. Правова охорона персональних даних у сфері охорони здоров'я в Україні.

Зростаюча кількість випадків порушення конфіденційності та безпеки електронних даних підвищує обурення та занепокоєння серед користувачів і фахівців у багатьох галузях, зокрема в медичній сфері. Ризики, пов'язані з недостатньою захищеністю медичних даних, включають можливість несанкціонованого доступу до особистої медичної інформації, її фальсифікацію, а також розголошення конфіденційних даних без дозволу пацієнтів.

Це може мати серйозні наслідки для пацієнтів, включаючи порушення їхньої приватності, страх перед втратою конфіденційної інформації та навіть можливість недостовірного діагнозу чи лікування внаслідок фальсифікації медичних даних.

Тому, для захисту медичних даних і забезпечення їхньої конфіденційності необхідно приділяти особливу увагу впровадженню відповідних заходів кібербезпеки та дотриманню відповідних правових норм і стандартів. Це включає розвиток сучасних технологій шифрування даних, регулярне навчання медичного персоналу з питань кібербезпеки, а також невідворотне виконання вимог нормативно-правових актів щодо захисту конфіденційної інформації.

Конфіденційність медичної інформації у сфері охорони здоров'я необхідно розглядати в контексті широкого спектру культурних, соціальних і релігійних переконань та традицій. Деякі медичні дані можуть бути особливо чутливими і приватними, наприклад, інформація про репродуктивне здоров'я, психічні розлади, лікування ВІЛ/СНІДу, а також медичні послуги для підлітків.

Відповідно до Закону України «Про захист персональних даних» персональні дані – відомості або сукупність відомостей про фізичну особу, яку ідентифіковано або може бути конкретно ідентифіковано.

Стаття 2 Конвенції про захист осіб щодо автоматизованої обробки персональних даних 1981 року визначає персональні дані як будь-яку інформацію, що стосується конкретно ідентифікованої особи або особи, яка може бути конкретно ідентифікована. Це означає, що будь-яка інформація, яка дозволяє або може дозволити ідентифікувати конкретну особу, вважається персональними даними і підпадає під захист відповідно до цієї конвенції.

Ця визначення є загальним стандартом, який застосовується в багатьох країнах та міжнародних правових актах для забезпечення захисту приватності та конфіденційності особистих даних. Воно охоплює широкий спектр інформації, включаючи ім'я, адресу, номер телефону, електронну пошту, інформацію про здоров'я, фінансову інформацію, та багато іншого.

Ключові слова: правова охорона, охорона здоров'я, персональні дані, медична сфера, особиста інформація, порушення приватності.

Diorditsa I., Kovalenko I., Koval O. Legal protection of personal data in the field of health care in Ukraine.

The growing number of breaches of the privacy and security of electronic data is raising outrage and concern among users and professionals in many industries, particularly in the medical field. Risks associated with insufficient security of medical data include the possibility of unauthorized access to personal medical information, its falsification, as well as the disclosure of confidential data without the consent of patients.

This can have serious consequences for patients, including violations of their privacy, fear of losing confidential information, and even the possibility of inaccurate diagnosis or treatment due to falsification of medical records.

Therefore, to protect medical data and ensure their confidentiality, it is necessary to pay special attention to the implementation of appropriate cyber security measures and compliance with relevant legal norms and standards. This includes the development of modern data encryption technologies, regular training of medical personnel on cyber security issues, as well as strict implementation of regulations on the protection of confidential information.

Confidentiality of medical information in the field of health care must be considered in the context of a wide range of cultural, social and religious beliefs and traditions. Some medical data can be particularly sensitive and private, such as information about reproductive health, mental disorders, HIV/AIDS treatment, and adolescent health services.

According to the Law of Ukraine «On Protection of Personal Data» personal data is information or a set of information about a natural person who is identified or can be specifically identified.

Article 2 of the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data defines personal data as any information relating to a specifically identified person or a person who can be specifically identified. This means that any information that allows or can allow the identification of a specific person is considered personal data and is subject to protection under this convention.

This definition is a general standard used in many countries and international legal acts to ensure the protection of privacy and confidentiality of personal data. It covers a wide range of information, including name, address, phone number, email, health information, financial information, and much more.

Key words: legal protection, health care, personal data, medical field, personal information, violation of privacy.

Постановка проблеми. Сучасна тенденція до стрімкого збільшення кількості даних, що циркулюють в інформаційному просторі, не оминула й сферу охорони здоров'я, яка має високий ступінь уразливості через чутливість даних про стан здоров'я людини та громадянина.

Нині, з розвитком інформаційного суспільства, ідентифікувати особу конкретної людини та отримати конфіденційну особисту інформацію про неї досить легко. Тому залишаються актуальними питання захисту від третіх осіб персональних даних, що містяться в централізованих базах медичних інформаційних систем.

Метою роботи є дослідження проблематики правової охорони захисту персональних даних у сфері охорони здоров'я в Україні.

Аналіз останніх досліджень і публікацій. Питанням захисту персональних даних в цілому та у сфері охорони здоров'я присвячували свої праці такі вчені, як І.М. Сопілко, В.О. Торічний, О.В. Манжура, А.В. Мусієнко, В.В. Мусієнко, В.І. Теремецький, Д.В. Цвірюк, М.В. Ковалів, Т.М. Ямненко, І.Ф. Літвінова, А.М. Гуз та інші. Однак в умовах безперервного процесу діджиталізації сфери охорони здоров'я актуальність окресленої проблематики зростає.

Виклад основного матеріалу. Систематизація, розробка законів та національних стандартів, а також чітке визначення термінів і понять є важливими кроками для забезпечення захисту персональних даних у всіх сферах життя, включаючи охорону здоров'я.

Питання законності оприлюднення персональних даних у судових рішеннях та інших офіційних документах, доступ до яких не обмежено, також потребує уваги та розробки відповідних правових механізмів для захисту приватності осіб, згаданих у цих документах.

Міжнародно-правові норми, такі як Рекомендація № R (97) 5 Комітету міністрів держав-членів Ради Європи, визначають важливі стандарти щодо захисту медичних даних. Ці стандарти встановлюють, що медичні дані можуть збирати та обробляти лише кваліфіковані медичні працівники або особи, які діють від імені таких медичних працівників. Дотримання цих правил конфіденційності є обов'язковим для всіх медичних працівників та установ, що працюють з медичною інформацією.

Особлива увага приділяється безпеці даних з боку менеджерів файлів, які повинні дотримуватися ефективних гарантій, встановлених національним законодавством. Рекомендація поділяє заходи безпеки, пов'язані з медичними даними, на технічні та організаційні, зокрема: запобігання несанкціонованому доступу до обладнання, що містить персональні медичні дані; запобігання третім особам від читання, копіювання, зміни або видалення таких носіїв даних; виконання моніторингу пам'яті та використання; здійснення зв'язку, введення даних, транспортування та контроль доступності; тощо.

Конфіденційність медичних даних визнається як один з основних принципів правових систем багатьох країн і міжнародних організацій, включаючи держави-члени Європейської конвенції. Цей принцип підтримується для захисту прав та приватності пацієнтів і має на меті забезпечення довіри до медичної системи та збереження приватності медичних даних.

У сучасному цифровому середовищі, де обмін медичною інформацією здійснюється за допомогою електронних систем, захист конфіденційності медичних даних стає ще більш актуальним і складним завданням. Такі міжнародні рішення, як зазначене вище, підкреслюють необхідність постійного вдосконалення законодавства щодо захисту персональних медичних даних для забезпечення недоторканості приватного життя та громадянських прав людини.

На нашу думку, слід погодитися з визначенням Т.М. Ямненко та І.Ф. Літвінової, які розкривають поняття «персональні дані у сфері охорони здоров'я» як «сукупність відомостей про особу (пацієнта), що дозволяють її ідентифікувати, та відомості про стан її здоров'я, медичні огляди, лікувальні заходи, прогноз захворювання, а також відомості, пов'язані з генетичними даними» [1, с. 186].

Збір та обробка персональних даних пацієнтів за їх письмовою згодою є важливим кроком для забезпечення конфіденційності та приватності медичної інформації. Система «Електронне здоров'я» дозволяє збирати та зберігати дані пацієнтів в цифровій формі для полегшення доступу до необхідної медичної інформації та забезпечення швидкого та ефективного надання медичної допомоги.

Контрольований доступ до персональних даних забезпечується шляхом встановлення прав доступу для різних категорій медичних працівників залежно від їхніх функціональних обов'язків та необхідності відповідно до законодавства. Наприклад, медичні працівники можуть мати обмежений доступ лише до тих персональних даних пацієнтів, які необхідні для виконання їхніх медичних обов'язків.

Така система контролю за доступом допомагає забезпечити безпеку та конфіденційність медичної інформації, дозволяючи медичним працівникам мати доступ лише до необхідної та відповідної їхнім функціям інформації про пацієнтів.

Згідно з постановою Кабінету Міністрів України № 411 від 25 квітня 2018 року, державне підприємство «Електронне здоров'я» має статус оператора центральної бази даних, проте ця база не обробляє персональні дані пацієнтів. Власником цієї бази даних є Національна служба здоров'я України (НСЗУ), яка виконує роль розпорядника Реєстру лікарів-спеціалістів, Реєстру суб'єктів господарювання у сфері охорони здоров'я та Реєстру медичних висновків. Міністерство охорони здоров'я України (МОЗ) виступає власником зазначених реєстрів.

Таким чином, система захисту персональних даних у сфері охорони здоров'я включає три основні суб'єкти: Міністерство охорони здоров'я, Національну службу здоров'я України та державне підприємство «Електронне здоров'я» [2, с. 73]. Що стосується практики захисту персональних даних на місцях, то в закладах охорони здоров'я, як правило, немає самостійної посади керівника. Зазвичай функції адміністратора покладаються на працівника відділу кадрів, бухгалтерії або медичного закладу, які можуть використовувати доступну їм інформацію лише відповідно до професійних, службових і трудових обов'язків.

Заклади охорони здоров'я повинні вимагати від своїх працівників письмові зобов'язання щодо нерозголошення інформації та медичних персональних даних, які стали їм відомі під час виконання службових обов'язків. Це зобов'язання доцільно здійснювати письмово, щоб зробити його більш юридично обов'язковим [3].

До правового регулювання персональних даних у сфері охорони здоров'я також слід віднести Закон України «Про державні фінансові гарантії медичного обслуговування населення», який передбачає створення електронної системи охорони здоров'я, а також право на охорону здоров'я. пацієнтам надавати «лікарям і третім особам право доступу до персональних даних та іншої інформації, що міститься в електронній системі охорони здоров'я, включаючи інформацію про стан вашого здоров'я, діагноз та інформацію, отриману під час медичного огляду, за умови, що ці особи відповідають вимогам законодавства про захист персональних даних» та про «отримання

Стаття 41 Закону України «Про реабілітацію інвалідів в Україні» регламентує створення централізованої бази даних з питань інвалідності, яка містить досить конфіденційні персональні дані, а саме: дані про реабілітаційні заклади, характер та причини інвалідності, навчальні заклади, професійний рівень інвалідів, дітей-інвалідів, рівень доходів, склад сім'ї, потреба та забезпеченість засобами реабілітації, лікуванням у санаторіях, виробами медичного призначення, реабілітаційними послугами, автомобілями тощо.

Відповідно до законодавства України, за порушення вимог щодо роботи з персональними даними пацієнтів передбачена адміністративна та кримінальна відповідальність. Уповноважений Верховної Ради України з прав людини здійснює контроль за дотриманням законодавства про захист персональних даних, для чого у його апараті створено відділ з питань захисту персональних даних.

Проте багато експертів і громадських організацій відзначають необхідність створення окремого незалежного наглядового органу, який би відповідав за контроль за дотриманням права на захист персональних даних та права на доступ до публічної інформації. Такий орган міг би бути спеціалізованим і мати необхідні ресурси та повноваження для ефективного контролю за діяльністю установ і організацій, які мають доступ до персональних даних.

Важливо зазначити, що хоча законодавство не деталізує конкретні види відповідальності за порушення законодавства про захист персональних даних, воно встановлює нормативну норму, за якою порушення законодавства про захист персональних даних тягне за собою відповідальність (згідно зі статтею 28 відповідного закону).

Для аналізу норм відповідальності за порушення законодавства у цій сфері слід звернутися до норм Цивільного кодексу України, Кодексу України про адміністративні правопорушення, Кримінального кодексу України, Кодексу законів про працю України.

Згідно з частиною 1 статті 270 ЦК України, фізичній особі належать особисті немайнові права, серед яких зазначене право на свободу та особисту недоторканність, право на недоторканність особистого і сімейного життя, право на повагу до гідності та честі. Порушення цих прав може призвести до матеріальної та/або моральної шкоди, яка підлягає відшкодуванню відповідно до статті 280 ЦК України [4].

Статтею 1167 ЦК України встановлено підстави відповідальності за моральну шкоду. Зокрема, моральна шкода вважається немайновою шкодою, яка виникає у результаті порушення особистих немайнових прав фізичної особи [4].

Стаття 237-1 КЗпП України визначає порядок відшкодування моральної шкоди працівникові. Згідно з цим положенням, відшкодування моральної шкоди працівникові здійснюється власником або уповноваженим ним органом у разі, якщо порушення його законних прав призвело до моральних страждань та втрати нормальних життєвих зв'язків [5].

Отже, вказані норми законодавства встановлюють механізм відшкодування моральної шкоди у разі порушення прав на приватне життя та особисту недоторканність.

Зокрема ст. 188-39 Кодексу України про адміністративні правопорушення передбачено відповідальність за порушення законодавства про захист персональних даних [6].

Стягнення штрафів передбачено за порушення вимог Закону України «Про захист персональних даних». Штрафи можуть бути накладені на фізичних осіб у розмірах від 100 до 200 неоподатковуваних мінімумів доходів громадян, а на державних службовців та фізичних осіб – суб'єктів підприємницької діяльності – у розмірах від 200 до 400 неоподатковуваних мінімумів доходів громадян.

За невиконання законних вимог або розпоряджень Уповноваженого Верховної Ради України з прав людини або уповноважених ним посадових осіб щодо запобігання порушенням договору або усунення недоліків у сфері захисту персональних даних можуть бути накладені штрафи на фізичних осіб у розмірах від 200 до 300 неоподатковуваних мінімумів доходів громадян і державних службовців, громадян – суб'єктів підприємницької діяльності – від 300 до 1000 неоподатковуваних мінімумів доходів громадян.

Повторне вчинення порушень протягом року після адміністративного стягнення може призвести до збільшення розміру штрафу.

Такі штрафні санкції є механізмом забезпечення додержання законодавства про захист персональних даних та виконання вимог Уповноваженого Верховної Ради України з прав людини з цього питання.

Недотримання порядку захисту персональних даних, встановленого законодавством, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних, може призвести до накладення штрафу.

Штраф на фізичних осіб може становити від 100 до 500 неоподатковуваних мінімумів доходів громадян, а для державних службовців, громадян – суб'єктів підприємницької діяльності – від 300 до 1000 неоподатковуваних мінімумів доходів громадян.

Такі штрафні санкції є механізмом забезпечення додержання законодавства про захист персональних даних та запобігання незаконному доступу до них або порушенню прав суб'єктів персональних даних [7].

Так, кримінальна відповідальність за порушення недоторканності приватного життя, зокрема незаконного збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконної зміни такої інформації, є однією з найсуворіших форм відповідальності. Згідно з Кримінальним кодексом України, за такі дії може бути накладений штраф від 500 до 1000 неоподатковуваних мінімумів доходів громадян або виправні роботи на строк до двох років, або арешт на строк до шести місяців, або обмеження волі на строк не більше трьох років.

У випадках, коли такі дії вчинені повторно або завдали істотної шкоди правам, свободам та інтересам особи, кримінальна відповідальність може бути ще суворішою. Порушення лікарями важливих принципів медичної етики та розголошення відомостей про персональні дані пацієнтів, які становлять лікарську таємницю, може мати серйозні правові наслідки, включаючи кримінальну відповідальність згідно з чинним законодавством [8].

Таким чином, лікарі повинні дотримуватися всіх вимог законодавства про захист персональних даних та збереження конфіденційності медичної інформації, щоб уникнути можливих правових проблем.

Висновки. Захист персональних даних у сфері охорони здоров'я є критично важливим і вимагає уваги з боку законодавця. Важливо доопрацювати та уточнити положення, що стосуються обробки персональних даних у сфері охорони здоров'я, враховуючи сучасні виклики та технологічні можливості. Реформи в системі охорони здоров'я, зокрема впровадження електронних систем, потребують додаткових заходів щодо захисту цих даних.

Належна відповідальність за порушення законодавства про обробку персональних даних у сфері охорони здоров'я є важливим механізмом забезпечення дотримання прав пацієнтів та відповідальності операторів медичної інформації.

Нормативно-правова база, що регулює надання інформації про пацієнтів, повинна бути збалансованою та забезпечувати високий рівень конфіденційності та захисту особистої інформації. Враховуючи складність цієї проблематики, спеціальні та загальні закони мають працювати у взаємодії для забезпечення належного рівня захисту даних і дотримання прав пацієнтів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Четверте покоління прав людини: особливості правового регулювання, проблеми та перспективи розвитку в сфері охорони здоров'я: монографія / за заг. ред.: д.ю.н., проф. С.Б. Булеци; д.ю.н., доц. М.В. Менджул. Ужгород: Вид-во УжНУ «Говерла», 2020. 444 с.
2. Саснко М.І. Сучасне правове регулювання інформаційних відносин у сфері захисту персональних даних в Україні. *Право і суспільство*. 2015. № 3. С. 103.

3. Рекомендація R11(97)5 щодо захисту медичних даних від 13.02.1997 р. та Пояснювальний Меморандум. URL: <http://www.umj.com.ua/article/37381/rekomendacii-radi-uevropi-shhodo-zaxistumedichnix-danix>.
4. Цивільний кодекс України від 16.01.2003 р. № 435-IV. URL: <http://zakon.rada.gov.ua/laws/show/435-15>.
5. Кодекс законів про працю України від 10.12.1971 р. № 322-VIII. URL: <https://zakon.rada.gov.ua/laws/show/322-08#Text>.
6. Кодекс України про адміністративні правопорушення від 07.12.1984 р. № 8074-X. URL: <https://zakon.rada.gov.ua/laws/show/80731-10#Text>.
7. Тарасюк А. Методологічні підходи до вивчення проблеми безпеки людини у кіберпросторі. *Підприємництво, господарство і право*. 2020. № 7. С. 254–258.
8. Основи законодавства про охорону здоров'я: Закон України від 19.11.1992 р. № 2801-XII. URL: <http://zakon.rada.gov.ua/laws/show/2801-12>.