

УДК: 347.121.2

[https://doi.org/10.52058/2786-6025-2024-4\(32\)-60-68](https://doi.org/10.52058/2786-6025-2024-4(32)-60-68)

**Коваленко Інна Анатоліївна** кандидат юридичних наук, доцент, доцент кафедри приватного та публічного права, Київський національний університет технологій та дизайну, вул. Мала Шияновська, 2, м. Київ. 01011, тел. (044)280-55-45, <https://orcid.org/0000-0001-7595-777X>

**Коваль Ольга Миколаївна** кандидат юридичних наук, доцент, доцент кафедри приватного та публічного права, Київський національний університет технологій та дизайну, вул. Мала Шияновська, 2, м. Київ. 01011, тел. (044)280-55-45, <https://orcid.org/0000-0003-1509-7258>

## ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я

**Анотація.** Враховуючи велику кількість приватних операторів, які надають інформаційні послуги зі збору, обробки та зберігання персональних даних пацієнтів, необхідно наголосити на необхідності створення нового органу державного нагляду за безпекою персональних даних у сфері охорони здоров'я. Правовий статус такого органу має надати йому інституційну спроможність ефективно впливати на приватних суб'єктів у досліджуваній сфері та застосовувати реальні механізми попередження порушень та відповідальності за них.

Серед напрямків удосконалення теми дослідження – перегляд вимог до інформації про систему охорони здоров'я, реєстраційної та ліцензійної тематики. Об'єктом детальної перевірки мають бути не лише організаційно-правові основи діяльності суб'єкта, а й його технічні можливості, використання сучасних ліцензованих засобів обробки та зберігання інформації.

Право на конфіденційність медичної інформації передбачає, що інформація про стан здоров'я пацієнта повинна залишатися конфіденційною та недоступною для сторонніх осіб, які не мають прямого відношення до надання медичних послуг.

Проте, право на доступ до медичної інформації також має важливе значення, особливо для пацієнтів, які мають право на ознайомлення зі своїми медичними записами та історією хвороби. У такому разі особа, яка володіє медичною інформацією, може надати доступ до цієї інформації лише за запитом самого пацієнта або особи, яку він уповноважує. Таким чином, забезпечується баланс між правом на конфіденційність медичних даних і правом на доступ до цих даних пацієнта.

Охорона та збереження права на таємницю про своє здоров'я є актуальним завжди, адже гарантувати це право завжди було дуже важко. У доцифрову еру медичні записи існували виключно на папері і були більш доступними для сторонніх. Таким чином кожен, хто перебував у даній кімнаті, міг ознайомитись з історією захворювань пацієнтів і увійти туди [1, с. 21].

Псевдонімізація визнана одним із ефективних заходів захисту персональних даних у сфері охорони здоров'я. Так, медичний заклад може створити реєстр пацієнтів і обробляти лише персональні дані (ПІБ, номер телефону, адресу пацієнта), яким присвоєно ідентифікатор. В архіві медичної карти персональні дані замінюються на зазначений ідентифікатор. У цьому випадку сторонні особи, які потребують обробки медичної документації (студенти навчальних закладів, науковці), не матимуть можливості ідентифікувати особу, оскільки працюватимуть із знеособленими даними [2, с. 30].

**Ключові слова:** персональні дані, зберігання інформації, приватність пацієнта, обробка медичної документації, розвиток телемедицини.

**Kovalenko Inna Anatolyivna** Candidate of legal sciences, associate professor, associate professor of the Department of private and public law, Kyiv National University of Technologies and Design, Mala Shyianovska St., 2, Kyiv. 01011, tel. (044)280-55-45, <https://orcid.org//0000-0001-7595-777X>

**Koval Olga Mykolayivna** Candidate of legal sciences, associate professor, associate professor of the Department of private and public law, Kyiv National University of Technologies and Design, Mala Shyianovska St., 2, Kyiv, 01011, tel.: (044)280-55-45, <https://orcid.org/0000-0003-1509-7258>

## PROBLEMS AND PERSPECTIVES OF THE DEVELOPMENT OF PERSONAL DATA PROTECTION IN THE FIELD OF HEALTH CARE

**Abstract.** Considering the large number of private operators that provide information services for the collection, processing and storage of personal data of patients, it is necessary to emphasize the need to create a new body of state supervision over the security of personal data in the field of health care. The legal status of such a body should provide it with the institutional capacity to effectively influence private entities in the researched area and apply real mechanisms of prevention of violations and responsibility for them.

Among the areas of improvement of the research topic is the review of requirements for information about the health care system, registration and licensing topics. The object of a detailed inspection should be not only the organizational and legal basis of the subject's activity, but also its technical capabilities, the use of modern licensed means of processing and storing information.

The right to confidentiality of medical information provides that information about the patient's health must remain confidential and inaccessible to third parties who are not directly related to the provision of medical services.

However, the right to access medical information is also important, especially for patients who have the right to access their medical records and medical history. In this case, the person who has medical information can provide access to this information only at the request of the patient himself or a person authorized by him. Thus, a balance is ensured between the right to privacy of medical data and the right of access to this data of the patient.

Protection and preservation of the right to secrecy about one's health is always relevant, because guaranteeing this right has always been very difficult. In the pre-digital era, medical records existed exclusively on paper and were more accessible to outsiders. Thus, anyone who was in this room could get acquainted with the history of the patients' illnesses and enter there [1, с. 21].

Pseudonymization is recognized as one of the effective measures to protect personal data in the field of health care. Yes, a medical institution can create a register of patients and process only personal data (name, phone number, address of the patient) to which an identifier has been assigned. In the archive of the medical card, personal data is replaced by the specified identifier. In this case, third parties who need to process medical documentation (students of educational institutions, scientists) will not have the opportunity to identify the person, since they will be working with depersonalized data [2, p. 30].

**Keywords:** personal data, information storage, patient privacy, processing of medical documentation, development of telemedicine.

**Постановка проблеми.** З урахуванням зазначеної мети в роботі ставимо перед собою завдання проаналізувати значення персональних даних у сфері охорони здоров'я в умовах інформатизації. Адже концепція розвитку електронної системи охорони здоров'я містить положення щодо забезпечення доступу пацієнтів до своїх персональних даних та інших функціональних можливостей електронної системи охорони здоров'я через електронний кабінет пацієнта. Згідно із заявами МОЗ України, медичні дані, які зберігаються в електронній системі охорони здоров'я, захищені краще, ніж картки пацієнтів на паперових носіях у закладах охорони здоров'я.

**Метою статті** є висвітлення та дослідження проблеми захисту та перспектив розвитку захисту персональних даних у сфері охорони здоров'я України в умовах інформатизації.

**Аналіз останніх досліджень і публікацій.** Дослідженням даної теми займалися такі науковці: 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.

**Виклад основного матеріалу.** Важливим кроком у розвитку сфери охорони здоров'я в цілому є створення електронної системи охорони здоров'я, збір та обробка персональних даних суб'єкта даних в якій відбувається відповідно до положень Закону України «Про захист персональних даних», Закон України «Про державні фінансові гарантії медичного обслуговування населення», Постанови Кабінету Міністрів України «Деякі питання електронної системи охорони здоров'я» [3].

Однією з реформ у системі охорони здоров'я є запровадження заяви про вибір лікаря, що надає первинну медичну допомогу (затверджено наказом МОЗ України від 19.03.2018 № 503). Заповнюючи його, пацієнт (його законний представник) надає необхідні персональні дані про себе, а підписом підтверджує, що йому роз'яснено положення Закону України «Про захист персональних даних» і він розуміє, що мета збору та обробки його персональних даних.

Таким чином особа погоджується на те, що її персональні дані будуть міститися в електронній системі охорони здоров'я та будуть доступні для обробки обраному в декларації лікарю та іншим лікарям, до яких вона в майбутньому звертатиметься за направленням.

Декларація може бути заповнена пацієнтом (його законним представником) як у письмовій, так і в електронній формі. Заповнення письмової форми відбувається на бланку, а у разі пошкодження бланка необхідно знищити у спосіб, що не дозволяє прочитати документ або його відновити, відповідно до наказу Міністерства юстиції України від 18.06.2015р. № 1000/5 «Про затвердження Правил організації діловодства та архівного зберігання документів у державних органах, органах місцевого самоврядування, на підприємствах, в установах та організаціях».

Сучасні проблеми, які обмежують належний розвиток захисту персональних даних про здоров'я, включають [4, с.43]:

1. Невідповідність нормативно-правової бази сучасному стану інформатики охорони здоров'я: швидкі темпи розвитку інформаційних технологій у сфері охорони здоров'я можуть перевершувати законодавство, що регулює цю сферу. Однак, потрібно постійно оновлювати та адаптувати нормативно-правову базу для відповідності сучасним технологічним реаліям.

2. Ігнорування ліцензованих засобів обробки та зберігання медичних даних: ліцензовані засоби гарантують дотримання встановлених стандартів та забезпечують високий рівень захисту даних. Ігнорування цих засобів може призвести до порушення безпеки даних та порушення прав пацієнтів.

3. Надмірна кількість персональних даних пацієнтів у одній базі даних: зберігання надмірної кількості даних може збільшити ризик їх несанкціонованого доступу та порушити приватність пацієнтів.

4. Відсутність контролю з боку державних органів за діяльністю приватних операторів медичних інформаційних систем: ефективний контроль

за діяльністю приватних операторів є важливим для забезпечення високого рівня захисту персональних даних.

5. Недостатні знання медичного персоналу з комп'ютера та відсутність у медичних закладах ІТ-спеціалістів: освіта та підготовка медичного персоналу з питань комп'ютерної безпеки та захисту даних є критично важливими. Також необхідно мати ІТ-спеціалістів, які можуть забезпечити належний технічний захист медичної інформації.

6. Ігнорування стандартів технічного захисту інформації: встановлення та дотримання стандартів технічного захисту є критично важливим для забезпечення безпеки медичних даних.

Розвиток електронної системи охорони здоров'я в Україні вимагає особливого ставлення до персональних даних пацієнта для забезпечення його прав та гарантій. Доступ до персональних даних пацієнта в електронній системі охорони здоров'я обмежено обмеженою кількістю осіб. Насамперед, мова йде про лікаря, який надає первинну медичну допомогу. Саме він вносить інформацію щодо декларації про вибір лікаря до центральної бази даних електронної системи охорони здоров'я. При цьому лікар, який надає первинну медичну допомогу, повинен чітко встановити (ідентифікувати) особу пацієнта [5, с.90].

Така ідентифікація можлива при наданні документа, що посвідчує особу пацієнта. Крім того, персональні дані пацієнта можуть стати відомі лікарям, до яких він направлений для надання спеціалізованої медичної допомоги. Водночас частиною третьою статті 25 Основ законодавства України про охорону здоров'я зазначено, що такі лікарі мають доступ до інформації про пацієнта в межах, необхідних для надання ними медичних послуг [6].

Залежно від того, які дані використовуються, вони повинні бути анонімними, таким чином мінімізуючи ризики для захисту цих даних. Але також має бути зрозуміло, що анонімізація даних може вплинути на якість медичних послуг. Тому тут необхідно підтримувати певний баланс, який, з одного боку, дозволяє лікарю отримати доступ до даних, необхідних йому для лікування пацієнта, а з іншого боку, захищає пацієнта від надмірного розширення даних лікарем.

Також цікавим є положення частини другої статті 242 Основ законодавства України про охорону здоров'я, де зазначено, що: «Доступ до інформації про пацієнта в електронній системі охорони здоров'я можливий лише за умови отримання згоди такого пацієнта (його законного представника) письмово або у формі, з якої можна зробити висновок про надання згоди» [6].

Виходячи з такого тлумачення, варто звернути увагу на поняття «форма, яка дає можливість зробити висновок про надання згоди». Стаття (32) Загального регламенту захисту даних передбачає, що згода на обробку

персональних даних повинна бути надана у формі письмової заяви, у тому числі за допомогою електронних засобів, або у формі усної заяви. Це може включати, наприклад, заповнення поля галочкою під час відвідування веб-сайту в Інтернеті, вибір технічних налаштувань для послуг інформаційного суспільства або інші заяви чи дії, які чітко вказують на згоду суб'єкта даних на запропоновану обробку персональних даних. При цьому мовчання, автоматичне заповнення клітинок маркерами або пасивність не є згодою [7, с.36].

Врахування специфіки медичної сфери та розвиток телемедицини вимагають адаптації законодавства щодо захисту персональних даних. У випадках, коли пацієнт не може особисто дати згоду на обробку своїх персональних даних, наприклад, у телемедицині, важливо розглядати можливість надання згоди за допомогою аудіовізуального зв'язку між пацієнтом та лікарем. Це може забезпечити ефективний механізм збереження конфіденційності медичних даних пацієнта при використанні телемедицини.

Гармонізація законодавства України з європейськими стандартами щодо захисту персональних даних є важливим кроком для забезпечення відповідності українських законів вимогам міжнародних стандартів. Імплементация Загального регламенту про захист персональних даних є важливою для забезпечення високого рівня захисту особистих даних громадян України, а також для полегшення обміну даними з країнами-членами Європейського Союзу. Виконання цього завдання має велике значення для подальшого розвитку електронної системи охорони здоров'я та забезпечення захисту конфіденційності медичних даних українських громадян.

Чому це також важливо для галузі медицини та захисту персональних даних пацієнтів? Справа в тому, що українська медична компанія, яка пропонує послуги (товари) резидентам ЄС або здійснює моніторинг поведінки суб'єктів даних в ЄС, автоматично підпадає під дію Загального регламенту захисту даних № 2016/679 або GDPR. Наприклад, багато іноземців віддають перевагу українському медичному туризму, головним чином через приємні ціни (майже вдвічі нижчі, ніж у європейських країнах) і високу якість медичних послуг. В медичному туризмі України лідирують такі напрямки, як стоматологія, офтальмологія, репродукція, неврологія, кардіологія, клітинна терапія та реабілітація.

GDPR передбачає можливість для регуляторів із захисту персональних даних країн ЄС застосовувати санкції екстериторіально, в тому числі на території України [8, с.73]. Таким чином, застосування GDPR неминуче.

Регламент вносить фундаментальні зміни до збору, обробки, зберігання та передачі даних про здоров'я. Тепер пацієнти повинні дати згоду на використання своїх даних про здоров'я та можуть відкликати або навіть видалити їх, якщо це необхідно. Насправді у світі це нове, адже, наприклад, у США практика медичних організацій зберігати дані пацієнтів необмежений

час поширена вже давно. Відповідно до GDPR, громадянин ЄС може за певних обставин вимагати від закладу охорони здоров'я видалення його чи її медичних даних, і в цьому неможливо відмовити.

**Висновки.** Таким чином можна підвести підсумки викладеного матеріалу, та зробити наступні висновки.

На підставі нашого дослідження ми можемо зробити висновок, що персональні дані, включно з інформацією про стан здоров'я, належать до так званої «чутливої» інформації і тому повинні бути ретельно захищені. Розголошення певних видів такої інформації, наприклад про онкологічні, неврологічні захворювання тощо, може призвести до соціальної стигматизації.

Відповідно до Закону України "Про захист персональних даних", персональні дані включають в себе будь-яку інформацію про фізичну особу, яку можна ідентифікувати або ідентифіковану. В заяві про вибір лікаря загальної практики дійсно зазвичай міститься ряд персональних даних, таких як прізвище, ім'я, по батькові, дата народження, номер облікової картки платника податків (РНОКПП), дані з документа, що посвідчує особу, адреса проживання та контактні дані. Ці дані є конфіденційними і підлягають захисту згідно з вимогами законодавства щодо захисту персональних даних.

Проаналізувавши положення міжнародно-правових стандартів та національного законодавства, вважаємо за доцільне запропонувати авторське визначення медичної інформації: відомості та/або відомості про стан здоров'я пацієнта, його діагноз, мету запропонованої діагностики та лікування, процес і результати надання медичної допомоги, прогноз можливих захворювань розвитку, у тому числі ризиків для життя та здоров'я, що зберігаються на матеріальних носіях або відображаються в електронному вигляді.

На підставі зазначених документів та інформації, наданої пацієнтом, заповнюється декларація в електронному вигляді та її роздрукована копія надається пацієнту, що також вважається згодою на обробку персональних даних лікарем, з яким працює пацієнт підписується заява і лікарі, до яких він буде звертатися за медичною допомогою, для направлення свого лікаря.

Концепція розвитку електронної системи охорони здоров'я містить положення щодо забезпечення доступу пацієнтів до своїх персональних даних та інших функціональних можливостей електронної системи охорони здоров'я через електронний кабінет пацієнта. Згідно із заявами МОЗ України, медичні дані, які зберігаються в електронній системі охорони здоров'я, захищені краще, ніж картки пацієнтів на паперових носіях у закладах охорони здоров'я.

Наразі немає спеціальних правових норм, які б регулювали відносини у сфері охорони здоров'я, що виникають у зв'язку з використанням цифрових технологій. Проте важливо розуміти, що такі стандарти необхідно створювати, оскільки специфіка цих відносин вимагає правового врегулювання питання захисту медичної інформації. Зокрема, це стосується регулювання викорис-

тання шифрування даних, контролю доступу до інформації та аутентифікації користувачів.

На законодавчому рівні це також має передбачати встановлення положень про необхідність проведення аудитів безпеки інформаційних систем для виявлення потенційних ризиків. Цей крок є необхідним, оскільки медична інформація відноситься до категорії конфіденційних даних і вимагає спеціального поводження.

### **Література:**

1. Брель О. Персональні дані як об'єкт інформаційних правовідносин за участю суб'єктів господарювання. *Право України*. 2011. № 4. С.220-224.
2. Тарасюк А. Методологічні підходи до вивчення проблеми безпеки людини у кіберпросторі. *Підприємництво, господарство і право*. 2020. № 7. С. 254-258.
3. Про захист персональних даних: Закон України від 01 червня 2010 року № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
4. Краус К. М., Краус Н. М., Манжура О. В. Цифрові вектори трансформації «інфраструктурного полотна» країни: соціально-економічні користі та загрози. *Європейський науковий журнал економічних та фінансових інновацій*. 2022. Вип. 2 (10). С. 48-58.
5. 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.
6. 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>.
7. Теремецький В. І., Цвірюк Д. В. Застосування зарубіжного досвіду правового захисту персональних даних в Україні. *Часопис Академії адвокатури України*. 2014. № 2. С. 73-82.
8. Саєнко М.І. Сучасне правове регулювання інформаційних відносин у сфері захисту персональних даних в Україні. *Право і суспільство*. 2015. № 3. С. 103.

### **References:**

1. Brel', O. (2011). Personal'ni dani jak ob'ekt informacijnih pravovidnosin za uchastju sub'ektiv gospodarjuvannja [Personal data as an object of informational legal relations with the participation of business entities]. *Pravo Ukraïni - Law of Ukraine*, 4, 220-224 [in Ukrainian].
2. Tarasjuk, A. (2020). Metodologichni pidhodi do vivchennja problemi bezpeki ljudini u kiberprostori [Methodological approaches to studying the problem of human security in cyberspace]. *Pidpriemnictvo, gospodarstvo i parvo - Entrepreneurship, economy and law*, 7, 254-258 [in Ukrainian].
3. Zakon Ukraïni "Pro zahist personal'nih danih" [The Law of Ukraine "On the protection of personal data"]. (n.d). [zakon.rada.gov.ua](https://zakon.rada.gov.ua/laws/show/2297-17#Text) Retrieved from <https://zakon.rada.gov.ua/laws/show/2297-17#Text> [in Ukrainian].
4. Kraus, K. M., Kraus, N. M., Manzhura, O. V. (2022). Cifrovi vektori transformacii «infrastrukturnogo polotna» kraïni: social'no-ekonomichni koristi ta zagrozi [Digital vectors of transformation of the "infrastructural fabric" of the country: socio-economic benefits and threats]. *Європейський науковий журнал економічних та фінансових інновацій - European Scientific Journal of Economic and Financial Innovations*, 2 (10), 48-58 [in Ukrainian].



5. Buleci, S.B. , Mendzhul, M.V. (2020). *Chetverte pokolinnja prav ljudini: osoblivosti pravovogo reguljuvannja, problemi ta perspektivi rozvitku v sferi ohoroni zdorov'ja* [The fourth generation of human rights: peculiarities of legal regulation, problems and prospects for development in the field of health care]. Uzhgorod: Vid-vo UzhNU «Goverla» [in Ukrainian].

6. Закон України “Основи законодавства про охорону здорov'ja” [The Law of Ukraine “Fundamentals of health care legislation”]. (n.d). Retrieved from [zakon.rada.gov.ua http://zakon.rada.gov.ua/laws/show/2801-12](http://zakon.rada.gov.ua/laws/show/2801-12). [in Ukrainian].

7. Teremec'kij, V. I., Cvirjuk, D. V. (2014). Zastosuvannja zarubizhnogo dosvidu pravovogo zahistu personal'nih danih v Ukraїni [Application of foreign experience of legal protection of personal data in Ukraine]. *Chasopis Akademii advokaturi Ukraїni - Journal of the Academy of Advocacy of Ukraine*, 2, 73-82 [in Ukrainian].

8. Saenko, M.I. (2015). Suchasne pravove reguljuvannja informacijnih vidnosin u sferi zahistu personal'nih danih v Ukraїni [Modern legal regulation of information relations in the field of personal data protection in Ukraine]. *Pravo i suspil'stvo - Law and society*, 3, 103 [in Ukrainian].