УДК 347
DOI https://doi.org/10.32782/2524-0374/2024-5/165

ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ МЕДИЧНОЇ ІНФОРМАЦІЇ ПРИ ОБРОБЦІ ДАНИХ ПАЦІЄНТА В ПРОЦЕСІ ФУНКЦІОНУВАННЯ ЕЛЕКТРОННОЇ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я

ENSURING THE CONFIDENTIALITY OF MEDICAL INFORMATION DURING THE PROCESSING OF PATIENT DATA IN THE OPERATION OF THE ELECTRONIC HEALTH SYSTEM

Блащук Т.В., к.ю.н., доцент,
завідувач кафедри цивільно-правових дисциплін
Навчально-науковий інститут права імені Іоаннікія Малиновського
Національного університету «Острозька академія»

Придатко Д.О., магістр права

У статті розглянуто поняття Електронної системи охорони здоров'я, її структурні особливості та призначення, зокрема роль у забезпеченні якісного та оперативного надання медичних послуг. Окремо проаналізовано особливості функціонування центральної бази даних та медичних інформаційних систем, що складають собою Електронну систему охорони здоров'я, акцентуючи увагу на їх взаємодії та інтеграції з іншими системами. Авторами визначено особливості медичних даних пацієнтів, які обробляються Електронною системою охорони здоров'я, підкреслюючи важливість точності, актуальності та безпеки таких даних для збереження конфіденційності пацієнтів. Досліджено загальну законодавчу базу обробки медичних даних, таку як Закон України «Про захист персональних даних», Закон України «Основи законодавства України про охорону здоров'я». Також, проведено аналіз спеціального законодавства, що регулює функціонування Електронної системи охорони здоров'я. Детально розглянуто принципи обробки інформації медичними закладами та працівниками, такі як: законність, мета та прозорість обробки, мінімізація, актуальність і точність даних. Окремий наголос авторами зроблено на зберіганні медичної інформації в межах функціонування Електронної системи охорони здоров'я, підкреслено важливість забезпечення її захисту від несанкціонованого доступу. У статті акцентовано увагу на контролі доступу до медичної інформації, що зберігається у центральній базі даних, та на необхідності впровадження надійних механізмів автентифікації та авторизації. Авторами проаналізовано особливості доступу медичних працівників до такої інформації, а також звернено увагу на необхідність розмежування прав доступу в залежності від посади та функціональних обов'язків. Досліджено питання необхідності та важливості проведення як внутрішніх, так і зовнішніх перевірок щодо належної обробки медичної інформації пацієнтів суб'єктами надання медичних послуг. Авторами вказано на необхідність постійного моніторингу та аудиту процесів обробки даних з метою виявлення та усунення потенційних загроз, а також зроблено висновок про необхідність створення окремого органу у сфері персональних даних, в тому числі й медичних, для проведення перевірок та притягнення до відповідальності у разі виявлення порушень.

Ключові слова: Електронна система охорони здоров'я, інформація, обробка інформації, медичні дані, права пацієнтів, право на інформацію.

This article examines the concept of the Electronic Health System, its structural features, and its purpose, particularly its role in ensuring the quality and timely delivery of medical services. The specific features of the central database and medical information systems that make up the Electronic Health System are separately described, with an emphasis on their interaction and integration with other systems. The characteristics of patient medical data processed by the Electronic Health System are identified, highlighting the importance of the accuracy, relevance, and security of such data to maintain patient confidentiality. The general legislative framework for the processing of medical data, such as the Law of Ukraine "On Personal Data Protection" and the Law of Ukraine "Fundamentals of the Legislation of Ukraine on Health Care," is explored. Furthermore, a detailed analysis of the special legislation regulating the operation of the Electronic Health System is conducted. The principles of information processing by medical institutions and employees, such as legality, purpose and transparency of processing, minimization, relevance, and accuracy of data, are thoroughly examined. Special attention is given to the storage of medical information within the functioning of the Electronic Health System, emphasizing the importance of ensuring its protection against unauthorized access. Attention is focused on access control to medical information stored in the central database and the need to implement reliable authentication and authorization mechanisms. The peculiarities of medical personnel's access to such information are described, with an emphasis on the necessity of differentiating access rights depending on the position and functional responsibilities. The need and importance of conducting both internal and external audits to ensure the proper processing of patient medical information by healthcare service providers are explored. The necessity of continuous monitoring and auditing of data processing processes to identify and eliminate potential threats is highlighted. A conclusion is drawn on the need to establish a separate body in the field of personal data, including medical data, to conduct inspections and hold accountable in case of violations.

Key words: Electronic Health System, information, information processing, medical data, patients' rights, right to information.

Постановка проблеми. У сучасному світі інформаційні технології відіграють важливу роль у всіх аспектах життя, включаючи охорону здоров'я. Кожен з нас все частіше звертається до сімейного лікаря дистанційно, замовляє ліки через електронні сервіси, онлайн записується на прийом до лікарів та виконує безліч інших медичних операцій. Впровадження електронної системи охорони здоров'я забезпечує значні переваги для медичних закладів та пацієнтів, зокрема прискорення процесів обміну інформацією, зручність доступу до медичних послуг та підвищення якості лікування. Проте, разом із цими перевагами виникають нові виклики, пов'язані з дотриманням законодавства у сфері захисту персональних даних та конфіденційності медичних записів.

Електронна система охорони здоров'я за своєю суттю передбачає доступ до великої кількості персональних даних пацієнтів, включаючи такі важливі елементи, як: повне ім'я, реєстраційний номер облікової картки платника податків, вік, стать, місце проживання, а також детальну інформацію про стан здоров'я пацієнтів, процес лікування, діагнози, медичні рекомендації та історію хвороб. Поєднання цих складових створює великий обсяг конфіденційної інформації, яка потребує особливого захисту з боку законодавства. Забезпечення належного рівня захисту медичних даних стає критично важливим завданням, оскільки порушення конфіденційності може мати серйозні наслідки для пацієнтів, медичних закладів та суспільства в цілому.

З одного боку, система охорони здоров'я повинна забезпечувати безперебійний обмін даними між медичними закладами, практиками, лікарями та іншими розпорядни-

ками реєстрів для надання швидких та якісних медичних послуг. З іншого боку, необхідно гарантувати надійний захист персональних даних пацієнтів від несанкціонованого доступу, витоку або неправомірного використання. Це створює серйозну проблему, яка полягає у необхідності балансування між можливістю ефективної обробки широкого спектру інформації про пацієнта для покращення медичних послуг та забезпеченням надійного захисту персональних даних.

Водночас виникає питання ефективності існуючих правових механізмів та стандартів, які регулюють обробку медичної інформації, що вимагає детального аналізу та вдосконалення в умовах зростаючих цифрових загроз. Це дослідження є особливо актуальним у контексті постійного розвитку цифрових технологій та потреби в адаптації правової бази до нових викликів.

Аналіз останніх досліджень і публікацій. Питання захисту персональних даних у сфері охорони здоров'я досліджували Миронова Г. А., Діордіца І. В., Коваленко І. А., Коваль О. М., Пономаренко І. С., Червякова О. Б., Мех Ю. В., Санжаровська Л. І. Однак, не дослідженим залишається питання забезпечення конфіденційності інформації про пацієнта саме в межах функціонування електронної системи охорони здоров'я. До того ж, в силу розвитку інформаційних технологій та спеціалізованих сервісів зазначена тема набуває нової актуальності.

Метою дослідження є комплексний аналізі правових аспектів забезпечення конфіденційності медичних даних в межах функціонування електронної системи охорони здоров'я, визначення ключових принципів функціонування такої системи та дослідження проблем в межах даної сфери.

Завданням дослідження є аналіз особливостей функціонування електронної системи охорони здоров'я, медичної інформації в межах цієї системи, принципів роботи з такою інформацією та розроблення рекомендацій задля гарантування безпеки даних пацієнтів.

Поняття та структура ЕСОЗ. Електронна система охорони здоров'я (далі – ЕСОЗ) є комплексною інформаційною системою, що використовується в сфері охорони здоров'я для збору, зберігання, використання, передачі медичної інформації про пацієнтів та призначена для оптимізації управління медичною інформацією. Вона об'єднує різноманітні технологічні компоненти та процеси для забезпечення ефективного використання медичних даних. ЕСОЗ створює основу для об'єднання інформації з різних медичних закладів в єдину інформаційну систему, що сприяє поліпшенню комунікації між медичними працівниками і пацієнтами.

ЕСОЗ виконує декілька основних функцій, які сприяють покращенню якості медичних послуг та ефективності їх надання. Одна з головних функцій – це обробка медичної інформації пацієнтів. Цей процес включає оцифровування паперових медичних карток, внесення персональних відомостей про пацієнта, його лікування, діагнози, використання цих даних у подальшому лікуванні, а також надання такої інформації іншим медичним працівника чи закладам охорони здоров'я.

Зазначені дані зберігаються у централізованій базі даних (далі – ЦБД), що забезпечує їхню доступність та безпеку. ЦБД є одним з двох рівнів ЕСОЗ та є ядром функціонування системи, адже саме сюди збігаються усі дані про пацієнтів крізь безліч медичних закладів по всій Україні. Основні функції, які забезпечує ЦБД, це захищене централізоване зберігання визначеного переліку даних ЕСОЗ відповідно до визначеного переліку реєстрів ЦБД ЕСОЗ та надання даних реєстрів авторизованим користувачам [1]. Другим рівнем ЕСОЗ є медичні інформаційні системи (далі – МІС). У найбільш вузькому розумінні МІС – це програмне забезпечення завдяки якому медичні заклади взаємодіють з ЦБД.

Медичні дані пацієнтів мають особливий правовий статус, оскільки вони включають чутливу інформацію, що стосується здоров'я, діагнозів, лікування та інших аспектів медичного обслуговування. Оскільки, медичні дані вважаються особливою категорією персональних даних, то вони потребують підвищеного рівня захисту. Таким чином, забезпечення конфіденційності даних пацієнтів є одним з найважливіших викликів у функціонуванні ЕСОЗ.

Згідно з положеннями Закону України «Основи законодавства України про охорону здоров'я» [2], медичні дані включають будь-яку інформацію, яка стосується фізичного або психічного стану здоров'я пацієнта, наданих медичних послуг, результатів обстежень, діагнозів та іншої інформації, отриманої під час надання медичної допомоги. В подальшому така інформація може бути використане для ідентифікації пацієнта, а отже будь-яка інформація, отримана під час надання медичних послуг, підпадає під дію законодавства про захист персональних даних.

Правові аспекти обробки медичних даних включають отримання згоди пацієнтів на роботу з їхніми даними. Згідно з Законом України «Про захист персональних даних» [3], обробка персональних даних, включаючи медичні дані, може здійснюватися лише за наявності згоди суб'єкта даних або на підставі інших законних підстав, таких як захист життєво важливих інтересів суб'єкта даних. Це означає, що перед роботою з даними пацієнта медичні заклади повинні інформувати перших про мету, обсяг та способи обробки їхніх даних, а також забезпечити можливість надання або відкликання згоди.

До прикладу, електронний документообіг надає також можливість надання такої послуги, як створення профілю пацієнта. Для цього обов'язковим є заповнення особистих даних (прізвище, ім'я, по батькові, дата народження та адресу місця проживання). Після цього кожен пацієнт повинен дати згоду на обробку даних для виконання Закону України «Про захист персональних даних» (необхідно натиснути кнопку «Добре» [4].

Разом з тим, Галина Миронова зазначає, що «в Україні залишається проблема надання поінформованої згоди на обробку персональних даних та «доступу до захищених законодавством даних внаслідок їх неналежного зберігання, передавання. Чинним законодавством не охоплюється врегулювання низки правовідносин, які виникають у зв'язку із обробкою персональних даних в ЕСОЗ» [5]. Ми з таким твердженням повністю погоджуємося. Чинне законодавство залишає без належної уваги ряд питань щодо добровільності та поінформованості згоди на обробку, форми надання згоди, можливість відкликання згоди, тощо.

Окрім згоди на обробку Закон України «Про захист персональних даних» встановлює й інші вимоги до роботи з медичними даних, такі як обмеження метою використання, прозорістю, мінімізацію даних, забезпечення їхньої точності та актуальності, а також захист від несанкціонованого доступу та втрат. Ці вимоги спрямовані на забезпечення високого рівня захисту медичних даних та дотримання прав пацієнтів. Обробка медичних даних у межах ЕСОЗ повинна відповідати вищезазначеним вимогам задля забезпечення законності, конфіденційності та безпеки цих даних. Ці правила встановлюються також міжнародними стандартами, такими як Загальний регламент про захист даних (GDPR) [6], тож розглянемо їх детальніше.

Загальні засади обробки медичних даних. Одним з ключових принципів обробки медичних даних є законність. Стаття 24-2 Закону України «Основи законодавства України про охорону здоров'я» зазначає, що доступ до інформації пацієнта можливий лише у разі отримання згоди такого пацієнта або його законного представника. Без згоди доступ до відомостей про пацієнта неможливий.

Однак, за наявності ознак прямої загрози життю пацієнта, у разі неможливості отримання такої згоди на той момент, доступ до інформації є дозволеним. Також отримати доступ до такої інформації можливо за рішення суду. Це означає, що використання даних повинно здійснюватися на підставі законних підстав, таких як згода суб'єкта даних або задля збереження життя та здоров'я суб'єкта даних. Медичні заклади повинні забезпечити, щоб використання даних відповідало цим підставам і не виходило за їх межі.

Важливим в цьому контексті є також мета обробки інформації. Відповідно до положень статті 6 Закону України «Про захист персональних даних», мета обробки медичної інформації має бути «сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних» [3]. Вона передбачає, що медична інформація повинна збиратися, використовуватися та поширюватися виключно для конкретних, чітко визначених та законних цілей. Цей принцип забезпечує захист прав і свобод фізичних осіб, запобігаючи незаконному або надмірному використанню їхніх персональних даних. Підкреслимо, що пацієнт надає згоду на обробку власних персональних даних тільки з певною конкретною метою, а якщо ж мета змінюється, то дозвіл необхідно отримувати знову.

Мінімізація даних є важливим аспектом використання медичних даних. Це означає, що медичні заклади повинні обробляти лише ті дані, які є необхідними для досягнення визначеної мети обробки. Наприклад, якщо метою обробки є надання медичної допомоги, то оброблятися повинні лише ті дані, які є необхідними для діагностики та лікування пацієнта.

Також медичні заклади повинні забезпечити, щоб оброблювані дані були точними та актуальними. У разі виявлення неточностей, дані повинні бути виправлені або видалені. Це особливо важливо для медичних даних, оскільки неточні дані можуть призвести до неправильних медичних рішень та негативних наслідків для здоров'я пацієнтів. До прикладу, Порядок ведення Реєстру медичних висновків в електронній системі охорони здоров'я затверджений наказом Міністерства охорони здоров'я України від 18.09.2020 № 2136 [7] зазначає, що у разі виявлення неточності медичним працівником, яка його внесла, то вона повинна виправити її і повідомити про це пацієнта. Якщо ж неточність виявив пацієнт, його законний представник або інша особа уповноважена пацієнтом, то вона повинна повідомити про це медичного працівника, який вносив ці відомості. В той же час, варто наголосити, що невірні відомості не підлягають видаленню. Ба більше, початковий зміст даних і надалі буде зберігатися у базі даних.

Прозорість обробки даних є ще одним важливим принципом. Законодавство визначає, що «обробка персональних даних здійснюється відкрито і прозоро із застосуванням засобів та у спосіб, що відповідають визначеним цілям такої обробки» [3]. Пацієнти повинні бути поінформовані про мету, обсяг та способи обробки їхніх даних. Це включає надання інформації про права суб'єктів даних, такі як право на доступ до своїх даних, право на їх виправлення або обмеження обробки, а також право на заперечення проти обробки.

Вищеописані принципи можуть застосуватися при роботі з інформацією як в межах функціонування ЕСОЗ, так і за звичайних умов. Вони забезпечують належне, законне та достатнє використання інформації для забезпечення усіх інтересів пацієнта. Водночас, говорячи саме про зберігання інформації, варто зазначити, що в межах функціонування ЕСОЗ таке питання має ряд специфічних рис.

Найголовнішим аспектом в цьому контексті є забезпечення безпеки медичних даних, адже це є критично важливим аспектом обробки даних у межах ЕСОЗ. Медичні заклади повинні впроваджувати відповідні технічні та організаційні заходи для захисту даних від несанкціонованого доступу, втрат, фальсифікації даних або інших загроз. В цьому контексті є важливим також забезпечення балансу між доступністю до медичної інформації та забезпеченням її конфіденційності. Деякі науковці до засобів забезпечення інформаційної безпеки електронного документообігу в медичній галузі включають «процедури ідентифікації та автентифікації суб'єктів телемедичних відносин; розмежування прав доступу до записів про стан здоров'я; шифрування переданих даних; анонімність та псевдоанонімність даних; безпека ІТ-інфраструктури, угоди про інформаційний обмін із закріпленням обов'язків щодо забезпечення інформаційної безпеки» [8]. Ми з таким переліком згідні, однак наголошуємо, що такий список не є вичерпним і з розвитком технологій буде тільки розширюватися.

Одним з ключових заходів забезпечення безпеки даних є контроль доступу. Медичні заклади повинні забезпечити, щоб доступ до медичних даних мали лише ті особи, які мають відповідні повноваження. Статтею 23 Порядку функціонування електронної системи охорони здоров'я, затвердженого постановою Кабінету Міністрів України від 25 квітня 2018 р. № 411, вказано, що «персональні дані у реєстрах можуть оброблятися у цілях охорони здоров'я, встановлення медичного діагнозу, забезпечення лікування або надання медичних послуг, функціонування електронної системи охорони здоров'я. Персональні дані, що стосуються здоров'я, можуть оброблятися за умови, що вони обробляються медичним працівником або іншою особою закладу охорони здоров'я чи фізичною особою – підприємцем, яка одержала ліцензію на провадження господарської діяльності з медичної практики, та її працівниками, на яких покладено обов'язки щодо забезпечення захисту персональних даних та поширюється дія законодавства про лікарську таємницю, працівниками НСЗУ, на яких покладено обов'язки щодо забезпечення захисту персональних даних»[9]. Водночас, далеко не кожен медичний працівник має доступ до даних пацієнта. Відповідно до статті 24-2 Закону України «Основи законодавства України про охорону здоров'я», коли пацієнт підписує декларацію про вибір лікаря, то такий лікар отримує згоду пацієнта на доступ до інформації щодо останнього, які містяться в електронній системі охорони здоров'я. Інші лікарі отримують такий доступ вже за направлення лікаря, з яким укладено декларацію. Однак, подібні лікарі отримують доступ не до всієї інформації, а тільки для тієї, яка є необхідною для надання медичних послуг. Крім того, така категорія лікарів має безумовний доступ до медичних записів, які вони самі зробили. Таким чином, доступ до системи має лише чітко визначена категорія осіб. Процедури забезпечення доступу такої категорії осіб може включати використання багатофакторної автентифікації, обмеження доступу до даних на основі ролей та проведення регулярного аудиту доступу до даних.

Окремо необхідно зупинитися на регулярних заходах перевірки безпеки. Такий аудит дозволяє виявляти та усувати вразливості у системах захисту даних. Медичні заклади повинні проводити регулярні перевірки своїх інформаційних систем для виявлення потенційних загроз та вжиття заходів для їх усунення. Це включає перевірку налаштувань безпеки, аналіз журналів доступу до даних та тестування систем на вразливості. Крім того, це потребує окремих фахівців в ІТ-сфері, які будуть займатися подібною діагностикою та покращеннями системи.

Зовнішній контроль за збереження даних пацієнтів також сприяє захисту прав останніх. Наразі, такі функції здійснює Уповноважений Верховної Ради України з прав людини. Однак експерти і громадські організації відзначають необхідність створення окремого незалежного нагля-

дового 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 [10]. Спроби створення подібного органу були зроблені у 2021 році, коли було подано проект Закону про Національну комісію з питань захисту персональних даних та доступу до публічної інформації [11]. Однак такий законопроект досі знаходиться на розгляді різних профільних комітетів, тому важко навіть зробити припущення чи буде створено такий орган та в який строк.

Висновки. У результаті дослідження встановлено, що забезпечення конфіденційності медичних даних в межах функціонування ЕСОЗ є складним і багатогранним завданням, що потребує комплексного підходу. Забезпечення конфіденційності медичних даних вимагає впровадження ефективних технічних та організаційних заходів із залученням якнайбільшої кількості фахівців у цій галузі. Забезпечення конфіденційності медичних даних є критично важливим для підтримки довіри пацієнтів та ефективності системи охорони здоров'я в цілому.

Законодавство, а саме Закон України «Про захист персональних даних» і Закон України «Основи законодавства України про охорону здоров'я», встановлює чіткі вимоги до обробки медичних даних, однак існує потреба в їх подальшому вдосконаленні з урахуванням сучасних викликів і міжнародних стандартів, таких як GDPR. Досліджена тематика потребує більше обґрунтованих досліджень задля удосконалення національного законодавства та усунення існуючих недоліків у системі.

ЛІТЕРАТУРА

1. Базова інформація про дворівневу архітектуру ЕСОЗ в Україні. Міністерство охорони здоров'я України. офіц. веб-сайт. URL: https://moz.gov.ua/uk/bazova-informaciya-pro-dvorivnevu-arhitekturu-esoz-v-ukrayini
2. Основи законодавства України про охорону здоров'я: Закон України від 19 листопада 1992 р. № 2801-XII. URL: https://zakon.rada.gov.ua/laws/show/2801-12#Text
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. Шушпанов Д.Г. Доступність та якість медичних товарів та послуг в Україні: соціально-економічний аспект. Регіональні аспекти розвитку і розміщення продуктивних сил України. 2018. № 23. С. 118-124. URL: http://dspace.wunu.edu.ua/bitstream/316497/33759/1/%D0%A8%D1%83%D1%88%D0%BF%D0%B0%D0%BD%D0%BE%D0%B2.pdf
5. Миронова А.Г. Впровадження електронних медичних записів пацієнта: проблеми правового регулювання в Україні. *Приватне право і підприємництво*. Збірник наукових праць. 2022 Вип. 21. с. 146 URL: https://repository.ndippp.gov.ua/handle/765432198/883
6. Регламент (Євросоюз) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text
7. Порядок ведення Реєстру медичних висновків в електронній системі охорони здоров'я: Наказ Міністерства охорони здоров'я України від 18.09.2020 № 2136. URL: https://zakon.rada.gov.ua/laws/show/z0952-20#Text
8. Ілюшик О.М., Ярема О.Г. Правові аспекти електронного документообігу у телемедицині. Електронне наукове видання «Аналітично-порівняльне правознавство». Випуск № 6 (2022). URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/60896/1/273744-%d0%a2%d0%b5%d0%ba%d1%81%d1%82%20%d1%81%d1%82%d0%b0%d1%82%d1%82%d1%96-630896-1-10-20230211.pdf
9. Порядок функціонування електронної системи охорони здоров'я: Постанова Кабінету Міністрів України від 25 квітня 2018 р. № 411 URL: https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#top
10. Діордіца І.В., Коваленко І.А., Коваль О.М. Правова охорона персональних даних у сфері охорони здоров'я в Україні. *Науковий* вісник Ужгородського Національного Університету. Випуск 82, частина 2, 2024 рік. Ст. 141-146. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/04/82-part-2.pdf#page=141
11. Проект Закону про Національну комісію з питань захисту персональних даних та доступу до публічної інформації. *Верховна Рада України*. офіц. веб-сайт. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72992