

АНАЛІТИЧНЕ ДОСЛІДЖЕННЯ ЩОДО ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я ТА ДОТРИМАННЯ ПРАВ ЛЮДИНИ В ЦІЙ ЦАРИНІ



Проект Ради Європи
«Підтримка впровадження європейських
стандартів захисту прав людини в Україні»

Ірина Сенюта

2024

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

**АНАЛІТИЧНЕ ДОСЛІДЖЕННЯ
ЩОДО ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ
У СФЕРІ ОХОРОНИ ЗДОРОВ'Я ТА
ДОТРИМАННЯ ПРАВ ЛЮДИНИ
В ЦІЙ ЦАРИНІ**

КИЇВ, 2024

Аналітичний звіт підготовлений д. юр. наук Іриною Ярославівною Сенютою, професором, завідувачкою катедри медичного права ФПДО Львівського національного медичного університету імені Данила Галицького, адвокаткою, головою Комітету медичного і фармацевтичного права та біоетики Національної асоціації адвокатів України, членкинею правління Європейської асоціації медичного права, президенткою ГО «Фундація медичного права та біоетики України».

Ця публікація розроблена за фінансової підтримки Ради Європи. Погляди, викладені в цьому документі, є відповідальністю його автора і можуть не співпадати з офіційною політикою Ради Європи.

Дозволяється відтворення уривків публікації (до 500 слів) за умови некомерційного використання, збереження цілісності тексту, контексту та надання повної інформації, яка не повинна жодним чином вводити читача в оману щодо характеру, обсягу чи змісту тексту. Необхідно обов'язково зазначити джерело тексту: «© Рада Європи, рік видання». Усі інші запити щодо відтворення або перекладу цієї публікації або будь-якої її частини повинні адресуватися Директорату комунікацій Ради Європи (F-67075 Strasbourg Cedex або publishing@coe.int).

Уся інша кореспонденція щодо цієї публікації повинна направлятися до Головного Директорату з прав людини та верховенства права.

Верстка, дизайн обкладинки та друк: «K.I.C.»

Фото: © Shutterstock

Council of Europe Publishing
F-67075 Strasbourg Cedex
(<http://book.coe.int>)

© Рада Європи, 2024

ЗМІСТ

УМОВНІ СКОРОЧЕННЯ	5
--------------------------	----------

ВСТУП	6
--------------	----------

РОЗДІЛ 1.

ЗАГАЛЬНІ РЕКОМЕНДАЦІЇ, СПРЯМОВАНІ НА ДОТРИМАННЯ ПРАВ ЛЮДИНИ ПРИ ОБРОБЦІ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я	7
--	----------

РОЗДІЛ 2.

ДОСЛІДЖЕННЯ ТИПОВИХ ПОРУШЕНЬ ПРАВ ЛЮДИНИ ПРИ ОБРОБЦІ ПЕРСОНАЛЬНИХ ДАНИХ І РЕКОМЕНДАЦІЇ ЩОДО ЇХ НЕДОПУЩЕННЯ	10
---	-----------

Типове порушення: ненадання медичної інформації та копій медичної документації пацієнтові або законному представнику пацієнта... .10

Типове порушення: неповідомлення Уповноваженого з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних... .14

Типове порушення: безпідставне відбирання суб'єктами обробки даних згоди про обробку персональних даних від пацієнтів при наданні медичної допомоги.18

Типове порушення: безпідставне відбирання згоди про обробку персональних даних від своїх працівників суб'єктами обробки персональних даних... .22

Типове порушення: обробка даних при контролі якості медичної допомоги без згоди суб'єкта персональних даних.24

Типове порушення: ненадання медичної інформації та копій медичної документації членам сім'ї померлого пацієнта... .26

Типове порушення: незаконне розголошення лікарської таємниці... .30

Типове порушення: недотримання правил обробки даних при функціонуванні електронної системи охорони здоров'я.37

Типове порушення: відсутні документи, які регулюють процеси, пов'язані з обробкою та захистом персональних даних.45

ДОДАТКИ	48
----------------	-----------

Додаток 148

Додаток 253

Додаток 356

Додаток 457

УМОВНІ СКОРОЧЕННЯ

ЄСПЛ	Європейський суд з прав людини
Конвенція з прав людини	Конвенція про захист прав людини і основоположних свобод від 04.11.1950
Конвенція Ов'єдо	Конвенція про захист прав і гідності людини щодо застосування біології та медицини: Конвенція про права людини та біомедицину від 04.04.1997
ЦПК України	Цивільний процесуальний кодекс України
ЦК України	Цивільний кодекс України
КПК України	Кримінальний процесуальний кодекс України
КК України	Кримінальний кодекс України
КУпАП України	Кодекс України про адміністративні правопорушення
Основи	Закон України «Основи законодавства України про охорону здоров'я»
Уповноважений з прав людини	Уповноважений Верховної Ради України з прав людини

ВСТУП

Тематика персональних даних у сфері охорони здоров'я особливо актуальна й уразлива водночас з огляду на цифровізацію та чутливість інформації. Чинне національне законодавство містить численні гарантії, виснувано правові позиції судових інстанцій, чатують численні державні інституції, а судова практика рясніє судовими справами і права людини все ж зазнають утисків в одній із найсенситивніших сфер.

У Ваших руках професійний порадник, у якому, з одного боку, зібрано необхідні матеріали за тематикою, а з іншого — дороговказ для дії при виникненні типової проблемної ситуації. Дослідження зорієнтовано насамперед на суб'єктів господарювання, які провадять свою господарську діяльність з медичної практики, аби при взаємодії з пацієнтами/законними представниками та членами їхніх сімей не виникало конфліктів і забезпечувався захист прав людини. Опрацювання цього дослідження також мало б оптимізувати роботу зі спектральними зверненнями, які надходять до володільців персональних даних, та забезпечити при цьому праволюдні стандарти обробки персональних даних.

Метою дослідження є викристалізація найбільш частих порушень прав людини в окресленій царині та вироблення рекомендацій надавачам медичних послуг і їхнім працівникам з метою недопущення і профілактики порушень прав людини при обробці персональних даних у сфері охорони здоров'я. Окрім того, в розділі 1 викладено загальні пропозиції органам державної влади, зокрема Уповноваженому з прав людини, спрямовані на дотримання прав людини при обробці персональних даних у сфері охорони здоров'я: від сприяння національним нормативним змінам до розробки рекомендацій щодо обробки персональних даних у сфері охорони здоров'я. Врахування пропозицій слугуватиме удосконаленню законодавства у царинах охорони здоров'я й обробки персональних даних, а також оптимізації правореалізації і правозастосування у цих сферах. Результати дослідження також будуть корисними для всіх, хто цікавиться тематикою прав людини у сфері охорони здоров'я й персональних даних.

Під аналітичний об'єкт потрапили міжнародні та регіональні стандарти, законодавство України, акти автентичного тлумачення, судова практика, зокрема ЄСПЛ, що дало змогу спектрально дослідити типові порушення прав людини й підготувати рекомендації для попередження таких у майбутньому в сфері охорони здоров'я.

Окрім того, підготовлено два додатки: перший містить перелік міжнародних і регіональних стандартів за тематикою дослідження, що стане в нагоді при глибинному вивченні питання, а другий є проєктом плану дій на випадки несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій, що передбачений як вимога до розробки володільцями персональних даних.

Безумовне дотримання володільцями персональних даних вимог чинного законодавства України буде ефективною превенцією порушення прав людини при обробці персональних даних у сфері охорони здоров'я. Пропоноване видання сприятиме кращому розумінню нормативних вимог щодо обробки персональних даних в окресленій царині.

РОЗДІЛ 1.

ЗАГАЛЬНІ РЕКОМЕНДАЦІЇ, СПРЯМОВАНІ НА ДОТРИМАННЯ ПРАВ ЛЮДИНИ ПРИ ОБРОБЦІ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ОХОРОНИ ЗДОРОВ'Я

1. Необхідно внести зміни до Основ в аспекті оновлення дефініції юридичної конструкції «медична інформація». Чинне законодавство України містить два різні визначення цієї терміноконструкції, а саме в Основах і в постанові КМУ «Деякі питання електронної системи охорони здоров'я» від 25.04.2018 № 411. В Основах під медичною інформацією розуміється інформація про медичне обслуговування особи або його результати, викладена в уніфікованій формі відповідно до вимог, встановлених законодавством, у тому числі інформація про стан здоров'я, діагнози та будь-які документи, що стосуються здоров'я та обмеження повсякденного функціонування/життєдіяльності людини¹. У Постанові № 411 медичну інформацію визначено як інформацію про стан здоров'я пацієнта, його діагноз, відомості, одержані під час медичного обстеження, зокрема відповідні медичні документи, що стосуються здоров'я пацієнта².

Відтак: 1) два визначення у законодавстві недоречні, крім того, вони дисонують; 2) перевагу матиме визначення в Основах за принципом ієрархії актів за юридичною силою; 3) більше ніж спірним є ототожнення інформації з документами, адже останні — джерело інформації. У ст. 1 Закону України «Про інформацію» закріплено дефініції термінів «інформація» та «документ». Під інформацією розуміються будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді, а під документом — матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі³; 4) пропонуємо нову редакцію норми ст. 3 Основ: «медична інформація — інформація про медичне обслуговування особи або його результати, викладена в уніфікованій формі відповідно до вимог, встановлених законодавством, у тому числі інформація про стан здоров'я, діагнози, обмеження повсякденного функціонування/життєдіяльності людини».

2. У Роз'ясненнях Уповноваженого Верховної Ради України з прав людини основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, від 08.01.2014 необхідно змінити формулювання юридичної конструкції зі «стан здоров'я особи» на «медична інформація». При формулюванні визначення використати законодавче, проте не включаючи сегмент ототожнення медичної інформації з документами.

1. Основи законодавства України про охорону здоров'я : Закон України від 19.11.1992 № 2801-XII.
URL: <https://zakon.rada.gov.ua/laws/show/2801-12#Text>
2. Деякі питання електронної системи охорони здоров'я : Постанова КМУ від 25.04.2018 № 411.
URL: <https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text>
3. Про інформацію : Закон України від 02.10.1992 № 2657-XII.
URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>

3. Необхідно уніфікувати віковий ценз реалізації права фізичної особи на медичну інформацію, адже в ЦК України (ст. 285) та Основах (ст. 39) визначено повноліття, тобто 18 років, а в Законі України «Про психіатричну допомогу» (ст. 26) та в Законі України «Про протидію поширенню хвороб, зумовлених вірусом імунодефіциту людини (ВІЛ), та правовий і соціальний захист людей, які живуть з ВІЛ» (ст. 7) встановлено можливість здійснення права з 14 років. У Постанові Верховного Суду від 25.01.2023 справа № 676/47/21 зазначено: *«У доктрині приватного права зауважується, що ієрархія актів цивільного законодавства може базуватися на їх юридичній силі (вимір по вертикалі). Вона поширюється, по-перше, на співвідношення закону та підзаконних актів та, по-друге, на співвідношення Конституції та законів (як кодифікованих, так і інших (поточних)). Одночасно слід визнати існування ієрархії між ЦК як кодифікованим законом та іншими (поточними) законами, що регулюють цивільні відносини. Ця ієрархія базується на визнанні ЦК основним актом цивільного законодавства (вимір ієрархії по горизонталі). Стосовно виміру ієрархії актів цивільного законодавства по горизонталі, то в статті 4 ЦК України закріплюється пріоритет норм ЦК (як основного регулятора приватних відносин) над нормами інших законів»⁴. З наведеного розуміємо, що в усіх випадках треба використовувати норми ст. 285 ЦК України через пріоритетність норм Кодексу, отож, і віковий ценз в усіх випадках — повноліття.*

4. Наказ МОЗ України «Про затвердження Порядку інформування майбутніх батьків, батьків, інших законних представників, а також особи, яка досягла 14 років, про діагноз, включно зі спадковими та вродженими патологіями або ризиком їх появи, що можуть призвести до інвалідності або смерті дитини» від 10.08.2023 № 1435 суперечить ЦК України (ст. 285) та Основам (ст. 39). Відтак відомчий нормотворець повинен узгодити норми підзаконного акта з вимогами законів України. Традиційним для правової системи України є дисонанс між законами та підзаконними актами, на що звертав увагу ЄСПЛ. У рішенні ЄСПЛ у справі «М. К. проти України» зазначено: *«Суд також зазначає, що Закон «Про ВІЛ» мав юридичну силу Закону України, прийнятого Верховною Радою України, тоді як наказ Міністерства оборони України, яким було затверджено Положення, був підзаконним актом і не міг на законних підставах вводити додаткові обмеження прав та обов'язків, передбачених законом. За цих обставин важко зрозуміти, чому Положення необхідно було вважати таким, яке мало перевагу над Законом «Про ВІЛ». Ні національні суди у своїх рішеннях, ні Уряд у своїх зауваженнях жодним чином не розглянули цей конкретний і важливий аргумент заявниці, який вона прямо висувала під час провадження як на національному рівні, так і в Суді. Таким чином, навіть погоджуючись, що передача результатів медичного огляду заявниці до військової частини мала певні законні підстави в національному законодавстві, Суд вважає, що така неузгодженість у чинній на момент події нормативно-правовій базі стосовно такого важливого питання, як розголошення ВІЛ-статусу особи, як у цій справі, становило порушення вимоги «якості закону», згідно з Конвенцією, та створило ситуацію, яку заявниця не могла передбачити у розумінні практики Суду за пунктом 2 статті 8 Конвенції»⁵.*

5. Реалізація права на згоду на медичну допомогу, гарантована ст. 284 ЦК України, або на згоду на медичне втручання за ст. 43 Основ, яка має бути інформованою, не корелює з віковим цензом здійснення права на інформацію. Згоду на медичну допомогу надає пацієнт з 14 років, проте право на інформацію про стан здоров'я здійснюється з повноліття. Необхідно внести зміни до законів і привести у відповідність позначення віку, з якого фізична особа стає компетентною реалізувати свої права на згоду на медичне допомогу та на інформацію про стан здоров'я.

4. Постанова Верховного Суду від 25.01.2023 справа № 676/47/21. URL: https://verdictum.ligazakon.net/document/108654283?utm_source=jurliga.ligazakon.ua&utm_medium=news&utm_content=jl03

5. Рішення ЄСПЛ у справі «М. К. проти України» від 15.12.2022. URL: https://zakon.rada.gov.ua/laws/show/974_i18#Text

6. У Положення про медичну раду закладу охорони здоров'я, затверджене наказом МОЗ України «Про організацію клініко-експертної оцінки якості надання медичної допомоги та медичного обслуговування» від 05.02.2016 № 69, необхідно внести зміни, зокрема включити обов'язок членів медичної ради забезпечувати конфіденційність отриманої інформації при проведенні внутрішнього контролю якості надання медичної допомоги.

7. У п. 3.4. Типового порядку обробки персональних даних, затвердженого Наказом Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1-02/14, закріплено один із організаційних заходів щодо захисту персональних даних, а саме регулярне навчання співробітників, які працюють з персональними даними. Це нормативне положення не є достатньо ефективним, оскільки в ньому не визначено періодичність такого навчання, зокрема відповідальних за обробку даних, а також немає відомостей про інституції, у яких таке навчання треба проходити. Отже, необхідно забезпечити внесення змін до нормативного акта та регламентувати питання навчання, що буде одним з інструментів профілактики правопорушень (на кшталт національного регламенту навчання щодо ведення військового обліку). Зокрема, до Порядку проведення атестації лікарів, затвердженого Наказом МОЗ України «Деякі питання безперервного професійного розвитку лікарів» від 22.02.2019 № 446, внести зміни до п. 6 р. VI «Механізм нарахування балів безперервного професійного розвитку та проведення їх щорічної перевірки», включивши в перелік тем навчання щодо захисту персональних даних: з питань захисту персональних даних — не більше ніж 20 балів.

8. Необхідно забезпечити належне складання протоколів про притягнення до адміністративної відповідальності в межах компетенції уповноваженими представниками Офісу Уповноваженого з прав людини та їх своєчасне надсилання до суду з метою притягнення до адміністративної відповідальності винних і невідворотності покарання за неправомірну обробку персональних даних. Аналіз Єдиного реєстру судових рішень дає підстави стверджувати про значну кількість справ, закритих через сплив строків давності притягнення до адміністративної відповідальності, що свідчить про неефективність механізмів захисту суб'єктів персональних даних. Окрім того, тривалим є час розгляду справ у суді (з різних суб'єктивних чи об'єктивних причин, зокрема умисного затягування строків особами, які беруть участь у провадженні в справі про адміністративне правопорушення), що також негативно впливає на притягнення винних до відповідальності. Вважаємо за необхідне внести зміни до ст. 38 КУпАП України з метою нормативного коригування строків накладення адміністративних стягнень і забезпечення невідворотності покарання винних. Пропонуємо закріпити нове положення у нормі ст. 38 КУпАП України в такій редакції: «Адміністративне стягнення за вчинення правопорушення, передбаченого статтею 188-39 цього Кодексу, може бути накладене протягом шести місяців з дня його виявлення, але не пізніше двох років з дня його вчинення».

9. Простежується законодавчий дисонанс між нормами п. 6 ч. 2 ст. 7 Закону України «Про захист персональних даних» і ч. 3 ст. 24-2 Основ щодо необхідності надання згоди на доступ до даних, що містяться в електронній системі охорони здоров'я (далі — ЕСОЗ). Пріоритетним вважаємо спеціальний акт — Закон України «Про захист персональних даних», відтак згоди суб'єкта персональних даних (пацієнта/(його/її) законного представника) щодо доступу до даних в ЕСОЗ медичним працівникам не потрібно, а підставою для їхньої легітимної обробки слугуватиме саме закон. Цю колізію треба усунути на законодавчому рівні.

10. Доречно підготувати рекомендації Уповноваженого з прав людини для володільців персональних даних — суб'єктів господарювання, які провадять господарську діяльність із медичної практики, з метою превенції порушень прав людини при обробці персональних даних у сфері охорони здоров'я. Окрім того, з огляду на мету парламентського контролю Уповноваженого з прав людини, сприяти удосконаленню законодавства України про права і свободи людини і громадянина, зокрема в контексті захисту персональних даних й охорони здоров'я.

РОЗДІЛ 2.

ДОСЛІДЖЕННЯ ТИПОВИХ ПОРУШЕНЬ ПРАВ ЛЮДИНИ ПРИ ОБРОБЦІ ПЕРСОНАЛЬНИХ ДАНИХ І РЕКОМЕНДАЦІЇ ЩОДО ЇХ НЕДОПУЩЕННЯ

Типове порушення: ненадання медичної інформації та копій медичної документації пацієнтові або законному представнику пацієнта.

Національне законодавство й акти автентичного тлумачення

Згідно зі ст. 8 Конвенції з прав людини, кожен має право на повагу до свого приватного і сімейного життя⁶. У ст. 32 Конституції України кожному гарантовано право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею⁷.

Відповідно до ст. 8 Закону України «Про захист персональних даних», суб'єкт персональних даних має низку прав, з-поміж яких — право знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом (п. 1), на доступ до своїх персональних даних (п. 3)⁸. Відповідно до ч. 6 ст. 16 Закону України «Про захист персональних даних», суб'єкт персональних даних має право на одержання будь-яких відомостей про себе у будь-якого суб'єкта відносин, пов'язаних з персональними даними, крім випадків, встановлених законом. Відмова у доступі до персональних даних допускається, якщо доступ до них заборонено згідно із законом (частина третя статті 17 зазначеного Закону).

У ч. 1 ст. 285 ЦК України закріплено, що повнолітня фізична особа має право на достовірну й повну інформацію про стан свого здоров'я, у тому числі на ознайомлення з відповідними медичними документами, що стосуються її здоров'я⁹. Аналогічною є норма ст. 39 Основ, у якій визначено, що пацієнт, який досяг повноліття, має право на отримання достовірної й повної інформації про стан свого здоров'я, у тому числі на ознайомлення з відповідними медичними документами, що стосуються його здоров'я¹⁰.

6. Конвенція про захист прав людини і основоположних свобод від 04.11.1950.
URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

7. Конституція України від 28.06.1996. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>

8. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI.
URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

9. Цивільний кодекс України від 16.01.2003 № 435-IV.
URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>

10. Основи законодавства України про охорону здоров'я : Закон України від 19.11.1992 № 2801-XII.
URL: <https://zakon.rada.gov.ua/laws/show/2801-12#Text>

У ч. 2 ст. 285 ЦК України та ч. 2 ст. 39 Основ закріплено, що батьки (усиновлювачі), опікун, піклувальник мають право на інформацію про стан здоров'я дитини або підопічного.

Відповідно до ст. 6 Закону України «Про психіатричну допомогу», право на одержання й використання конфіденційних відомостей про стан психічного здоров'я особи та надання їй психіатричної допомоги має сама особа чи її законний представник.

Згідно зі ст. 26 Закону України «Про психіатричну допомогу», лікар-психіатр зобов'язаний пояснити особі, якій надається психіатрична допомога, з урахуванням її психічного стану, у доступній формі інформацію про стан її психічного здоров'я, прогноз можливого розвитку захворювання, про застосування методів діагностики та лікування, альтернативні методи лікування, можливий ризик і побічні ефекти, умови, порядок і тривалість надання психіатричної допомоги, її права та передбачені цим Законом можливі обмеження цих прав при наданні психіатричної допомоги. Право на одержання зазначеної інформації щодо неповнолітнього віком до 14 років та особи, визнаної у встановленому законом порядку недієздатною, мають їхні законні представники. Особа при наданні їй психіатричної допомоги або її законний представник має право на ознайомлення з історією хвороби та іншими документами, а також на отримання в письмовій формі будь-яких рішень щодо надання їй психіатричної допомоги відповідно до закону¹¹.

У ч. 3 ст. 7 Закону України «Про протидію поширенню хвороб, зумовлених вірусом імунодефіциту людини (ВІЛ), та правовий і соціальний захист людей, які живуть з ВІЛ» зазначено, що в разі виявлення ВІЛ у дітей віком до 14 років та осіб, визнаних у встановленому законом порядку недієздатними, уповноважений медичний працівник повідомляє про це батьків або інших законних представників зазначених осіб¹².

Під медичною інформацією у ст. 3 Основ розуміється інформація про медичне обслуговування особи або його результати, викладена в уніфікованій формі відповідно до вимог, встановлених законодавством, у тому числі інформація про стан здоров'я, діагнози та будь-які документи, що стосуються здоров'я та обмеження повсякденного функціонування/ життєдіяльності людини¹³. У постанові КМУ «Деякі питання електронної системи охорони здоров'я» від 25.04.2018 № 411¹⁴ медична інформація визначена як інформація про стан здоров'я пацієнта, його діагноз, відомості, одержані під час медичного обстеження, зокрема відповідні медичні документи, що стосуються здоров'я пацієнта.

У рішенні Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К. Г. Устименка) від 30.10.1997 зазначено, що медична інформація — свідчення про стан здоров'я людини, історію її хвороби, про мету запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, в тому числі про наявність ризику для життя і здоров'я, — за своїм правовим режимом належить до конфіденційної, тобто інформації з обмеженим доступом. У випадках відмови у наданні або навмисного приховування медичної інформації від пацієнта, членів його сім'ї або законного представника вони можуть оскаржити дії чи бездіяльність

11. Про психіатричну допомогу : Закон України від 22.02.2000 № 1489-III.

URL: <https://zakon.rada.gov.ua/laws/show/1489-14#Text>

12. Про протидію поширенню хвороб, зумовлених вірусом імунодефіциту людини (ВІЛ), та правовий і соціальний захист людей, які живуть з ВІЛ : Закон України від 12.12.1991 № 1972-XII (ред. від 23.12.2010).

URL: <https://zakon.rada.gov.ua/laws/show/1972-12#Text>

13. Основи законодавства України про охорону здоров'я : Закон України від 19.11.1992 № 2801-XII.

URL: <https://zakon.rada.gov.ua/laws/show/2801-12#Text>

14. Деякі питання електронної системи охорони здоров'я : Постанова КМУ від 25.04.2018 № 411.

URL: <https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text>

лікаря безпосередньо до суду або, за власним вибором, до медичного закладу чи органу охорони здоров'я¹⁵.

У п. 3 Порядку інформування майбутніх батьків, батьків, інших законних представників, а також особи, яка досягла 14 років, про діагноз, включно зі спадковими та вродженими патологіями або ризиком їх появи, що можуть призвести до інвалідності або смерті дитини», затвердженого наказом МОЗ України від 10.08.2023 № 1435, зазначено, що інформування майбутніх батьків, батьків або законних представників дитини, а також особи, яка досягла 14 років, про виявлення підозри або встановлення патології вагітності чи невиліковного діагнозу (включно зі спадковими та вродженими патологіями або ризиком їх появи) у дитини, що може призвести до інвалідності або можливої смерті дитини або загибелі плоду, проводиться у формі розмови¹⁶.

У Роз'ясненнях Уповноваженого Верховної Ради України з прав людини основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, від 08.01.2014 міститься дефініція терміноконструкції «стан здоров'я особи». Під нею розуміється медична інформація про особу, що містить свідчення не лише про стан здоров'я, а й про історію її хвороби, про запропоновані дослідження й лікувальні заходи, прогноз можливого розвитку захворювання, у тому числі про наявність ризику для життя і здоров'я (виняток становлять медичні довідки, листи працездатності і т. д., які обробляються володільцем при реалізації трудових відносин)¹⁷.

Практика національних судів

Постанова Верховного Суду від 11.11.2020 у справі № 442/4791/17: «ОСОБА_1 має право, відповідно до вимог статті 285 ЦК України, статей 21, 23 Закону України «Про інформацію», статей 39, 39-1 Закону «№ 2801-XII», статей 2, 4 Закону України «Про захист персональних даних», отримати медичну інформацію стосовно себе (копію медичної карти стоматологічного хворого ОСОБА_1) та інформацію про прізвище, ім'я та по батькові лікаря, його кваліфікаційний рівень, документацію, що стосується письмової угоди з лікарнею на отримання медичних послуг, виконаних робіт, оплати та сертифікатів якості встановлених імплантантів, тобто інформацію, про яку відповідач як надавач послуг повинен був повідомити споживача стоматологічних послуг, тобто ОСОБА_1. Отже, правильними є висновки судів попередніх інстанцій у тій частині, що своєю відмовою ПП «Стоматологічний центр» порушив права клієнта ОСОБА_1 на отримання інформації відносно себе, зокрема медичної інформації»¹⁸.

15. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К. Г. Устименка) від 30.10.1997 справа № vd971030 vn5-зп. URL: <https://zakon.rada.gov.ua/laws/show/v005p710-97#Text>
16. Про затвердження Порядку інформування майбутніх батьків, батьків, інших законних представників, а також особи, яка досягла 14 років, про діагноз, включно зі спадковими та вродженими патологіями або ризиком їх появи, що можуть призвести до інвалідності або смерті дитини : Наказ МОЗ України від 10.08.2023 № 1435. URL: <https://zakon.rada.gov.ua/laws/show/z1494-23#Text>
17. Роз'яснення Уповноваженого Верховної Ради України з прав людини основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, від 08.01.2014. URL: <https://zakon.rada.gov.ua/laws/show/n0003715-14#Text>
18. Постанова Верховного Суду від 11.11.2020 у справі № 442/4791/17. URL: <https://zakononline.com.ua/court-decisions/show/93666639>

Правові позиції ЄСПЛ

Рішення ЄСПЛ у справі «К.Х. та інші проти Словаччини»: справа стосувалася реалізації заявниками свого права на ефективний доступ до інформації про їхнє здоров'я і репродуктивний статус, тобто вона пов'язана з їхнім особистим і сімейним життям, згідно зі ст. 8 Конвенції з прав людини.

ЄСПЛ відзначив: «Пам'ятаючи про те, що реалізація права на повагу до особистого та сімейного життя, передбаченого ст. 8, повинна бути практичною й ефективною (див., наприклад, Пінікарідоу проти Кіпру, № 23890/02, §64, ЄСПЛ 2007, з подальшими посиланнями), Суд дотримується думки, що такий позитивний обов'язок повинен бути розширений, зокрема у справах, подібних до тієї, що є предметом цього розгляду, коли йдеться про персональні дані, щоб уможливити виготовлення копій документів з персональними даними. Можна погодитись з тим, що розпорядник документів має право визначати умови копіювання документів, які містять персональні дані, чи вимагати оплати за це від суб'єктів цих даних. Однак Суд не вважає, що суб'єкт даних повинен чітко обґрунтовувати свій запит щодо надання копій документів, які містять персональні дані. Це, радше, обов'язок органів влади обґрунтувати відмову в такій можливості вагомими причинами»¹⁹.

Рекомендації

1. За загальним правилом пацієнт має право на медичну інформацію з повноліття, як і право на отримання копій медичної документації.
2. Пацієнт або законний представник пацієнта має право на отримання копій медичних документів у суб'єкта господарювання, у якого пацієнт отримував медичну послугу.
3. Пацієнт або законний представник пацієнта, аби отримати копії медичних документів у закладі охорони здоров'я чи у фізичної особи — підприємця, яка має ліцензію на провадження господарської діяльності з медичної практики, повинні підготувати у письмовій формі запит щодо доступу до персональних даних. Запит повинен бути складений з дотриманням вимог ст. 16 Закону України «Про захист персональних даних» у письмовій формі.

Пам'ятаймо: суб'єкт господарювання надає на безоплатній основі копії медичної документації пацієнтові відповідно до ч. 1 ст. 19 Закону України «Про захист персональних даних». Пацієнтові в запиті достатньо вказати прізвище, ім'я та по батькові, місце проживання (місце перебування) і реквізити документа, що посвідчує фізичну особу, яка його подає. Отож, вимога вказувати, приріром, мету, правову підставу запиту — незаконна.

Законним представником пацієнта є: батьки (усиновлювачі) є законними представниками своїх малолітніх і неповнолітніх дітей; опікун є законним представником малолітньої особи та фізичної особи, визнаної недієздатною; прийомні батьки, як і батьки-вихователі, є законними представниками прийомних дітей і діють без спеціальних на те повноважень як опікуни або піклувальники; піклувальники є законними представниками неповнолітніх осіб і фізичних осіб, цивільна дієздатність яких обмежена.

Пам'ятаймо: якщо над фізичною особою, яка перебуває у навчальному закладі, закладі охорони здоров'я або закладі соціального захисту населення, не встановлено опіку чи піклування або

19. Рішення ЄСПЛ у справі «К. Х. та інші проти Словаччини» від 06.11.2009. URL: [file:///C:/Users/user/Downloads/CASE%20OF%20K.H.%20AND%20OTHERS%20v.%20SLOVAKIA%20-%20\[Ukrainian%20Translation\]%20by%20the%20All-Ukrainian%20Public%20Organization%20%E2%80%9CFoundation%20of%20Medical%20Law%20and%20Bioethics%20of%20Ukraine%E2%80%9D-1.pdf](file:///C:/Users/user/Downloads/CASE%20OF%20K.H.%20AND%20OTHERS%20v.%20SLOVAKIA%20-%20[Ukrainian%20Translation]%20by%20the%20All-Ukrainian%20Public%20Organization%20%E2%80%9CFoundation%20of%20Medical%20Law%20and%20Bioethics%20of%20Ukraine%E2%80%9D-1.pdf)

якщо їй не призначено опікуна чи піклувальника, опіку або піклування над нею здійснює цей заклад (ст. 66 ЦК України).

Законними представниками не можуть бути бабусі, дідусі й інші родичі, незважаючи на те, що вони проживають разом з неповнолітніми або малолітніми, виховують їх тощо (якщо тільки вони не є опікунами/піклувальниками).

Особи, позбавлені батьківських прав, перестають бути законними представниками дітей.

Типове порушення: *неповідомлення Уповноваженого з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних.*

Національне законодавство й акти автентичного тлумачення

У ст. 9 Закону України «Про захист персональних даних» зазначено, що володілець персональних даних повідомляє Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, упродовж тридцяти робочих днів з дня початку такої обробки. Володілець персональних даних зобов'язаний повідомляти Уповноваженого про кожну зміну відомостей, що підлягають повідомленню, упродовж десяти робочих днів з дня настання такої зміни. Інформація, що повідомляється відповідно до цієї статті, підлягає оприлюдненню на офіційному веб-сайті Уповноваженого в порядку, визначеному Уповноваженим. У ст. 24 цього ж Закону визначено, що в органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього Закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов'язану із захистом персональних даних при їх обробці. Інформація про зазначений структурний підрозділ або відповідальну особу повідомляється Уповноваженому Верховної Ради України з прав людини, який забезпечує її оприлюднення. Фізичні особи — підприємці, у тому числі лікарі, які мають відповідну ліцензію, адвокати, нотаріуси особисто забезпечують захист персональних даних, якими вони володіють, згідно з вимогами закону²⁰.

У ст. 15 «Захист персональних даних» Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, закріплено, що сторони домовились співпрацювати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських і міжнародних стандартів, зокрема відповідних документів Ради Європи. Співробітництво у сфері захисту персональних даних може включати, *inter alia*, обмін інформацією та експертами. У ст. 129 цієї Угоди визначено, що кожна Сторона вживає адекватних спеціальних заходів з метою захисту права на приватне життя та основоположних прав і свобод людини, зокрема у зв'язку з передачею персональних даних²¹.

У ч. 1 ст. 188-39 КУпАП України вказано, що неповідомлення або несвоєчасне повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних або про зміну відомостей, які підлягають повідомленню згідно із законом, повідомлення неповних чи

20. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI.
URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

21. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 21.03.2014 та 27.06.2014 (ратиф. Законом України від 16.09.2014). URL: https://zakon.rada.gov.ua/laws/show/984_011#Text

недостовірних відомостей тягнуть за собою накладення штрафу на громадян від ста до двохсот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян — суб'єктів підприємницької діяльності — від двохсот до чотирьохсот неоподатковуваних мінімумів доходів громадян²².

У п. 1.2 Порядку повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації, затвердженому наказом Уповноваженого з прав людини від 08.01.2014 № 1-02/14 (далі — Порядок повідомлення), зазначено, що для цілей цього Порядку обробка персональних даних, яка становить особливий ризик для прав і свобод суб'єктів, — це будь-яка дія або сукупність дій, а саме збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання й поширення (розповсюдження, реалізація, передача), знеособлення, знищення, у тому числі з використанням інформаційних (автоматизованих) систем, яка здійснюється відносно персональних даних про:

- расове, етнічне та національне походження;
- політичні, релігійні або світоглядні переконання;
- членство в політичних партіях та/або організаціях, професійних спілках, релігійних організаціях чи в громадських організаціях світоглядної спрямованості;
- стан здоров'я;
- статеве життя;
- біометричні дані;
- генетичні дані;
- притягнення до адміністративної чи кримінальної відповідальності;
- застосування щодо особи заходів у межах досудового розслідування;
- вжиття щодо особи заходів, передбачених Законом України «Про оперативно-розшукову діяльність»;
- вчинення щодо особи тих чи інших видів насильства;
- місцеперебування та/або шляхи пересування особи²³.

У п. 3 Роз'яснення Уповноваженого Верховної Ради України з прав людини основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, від 08.01.2014 зазначено, що обробка вважатиметься чутливою в разі, якщо: 1) склад персональних даних про особу, які обробляються володільцем, включає відомості вказаного в п. 2 змісту або 2) коли володільцем обробляються персональні дані певної категорії суб'єктів, яку можна виділити за

22. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-Х.

URL: <https://zakon.rada.gov.ua/laws/show/80731-10#Text>

23. Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації: Наказ Уповноваженого ВРУ з прав людини від 08.01.2014 № 1-02/14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n215

вказаним в п. 2 критерієм²⁴. Підкреслимо, що в п. 2 Роз'яснення перелічено дані, визначені в Порядку повідомлення.

Рекомендації

1. Володілець персональних даних повідомляє Уповноваженого з прав людини про здійснення ним будь-яких видів обробки персональних даних, які становлять особливий ризик для прав і свобод суб'єктів персональних даних, крім випадків, встановлених у Порядку повідомлення. До переліку винятків не належить провадження медичної практики. Проте виняток становить, згідно з Порядком повідомлення, обробка, необхідна для реалізації прав і виконання обов'язків володільца персональних даних у сфері трудових правовідносин відповідно до закону. Отже, закладам охорони здоров'я та ФОП, які провадять господарську діяльність з медичної практики, не треба інформувати Уповноваженого з прав людини про обробку даних своїх працівників, навіть якщо така становить особливий ризик для прав і свобод суб'єктів персональних даних.
2. Володілець персональних даних повинен подавати до Секретаріату Уповноваженого з прав людини Заяву про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних (Додаток 1 до Порядку повідомлення). Кожна сторінка заяви має бути пронумерована та скріплена печаткою (у разі наявності) і підписом уповноваженої на те особи.
3. Заявники повинні зберігати копії заяв, які були подані до Секретаріату Уповноваженого з прав людини.
4. При чутливій обробці даних необхідно повідомляти Уповноваженого з прав людини про створення структурного підрозділу або призначення відповідальної особи, що організовує роботу, пов'язану з захистом персональних даних при їх обробці. До Секретаріату Уповноваженого з прав людини подається Заява про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці (Додаток 4 до Порядку повідомлення).
5. Щодо строків повідомлення треба пам'ятати: а) володілець персональних даних повідомляє Уповноваженого з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, упродовж 30 робочих днів з дня початку такої обробки; б) володілець персональних даних повідомляє Уповноваженого з прав людини про створення структурного підрозділу або призначення відповідальної особи впродовж 30 днів з моменту створення підрозділу або призначення відповідальної особи.
6. Повідомлення здійснюються на вибір володільца персональних даних у такі способи: а) надсилаються листом; б) надсилаються електронною поштою; в) надсилаються факсом; г) подаються особисто через спеціально встановлену скриньку для вхідної кореспонденції у приміщенні Секретаріату Уповноваженого з прав людини. У разі надсилання електронною поштою заява має бути відсканована.
7. Володілець персональних даних, який повідомив Уповноваженого з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, повинен повідомити Уповноваженого з прав людини про кожну зміну відомостей, вказаних у п. 2.4. Порядку повідомлення. Приміром, про зміну персональних даних, що обробляються,

24. Роз'яснення Уповноваженого Верховної Ради України з прав людини основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, від 08.01.2014.
URL: <https://zakon.rada.gov.ua/laws/show/n0003715-14#Text>

мету обробки персональних даних. Повідомлення про кожну зміну відомостей здійснюється упродовж 10 робочих днів з дня настання такої зміни. До Секретаріату Уповноваженого з прав людини подається Заява про зміну відомостей щодо обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних (Додаток 2 до Порядку повідомлення).

8. Володілець персональних даних, який повідомив Уповноваженого з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, повинен повідомити Уповноваженого з прав людини про припинення такої обробки персональних даних. До Секретаріату Уповноваженого з прав людини подається Заява про припинення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних (Додаток 3 до Порядку повідомлення). Повідомлення про припинення обробки даних здійснюється упродовж 10 днів з моменту припинення такої обробки.

9. Володілець персональних даних повинен сформулювати систему заходів щодо захисту персональних даних при провадженні діяльності, зокрема не допускати незаконної обробки. А саме: а) підготувати й затвердити для медичної практики локальний порядок обробки персональних даних (приміром, Положення про обробку персональних даних). Для цього доцільно скористатися Типовим порядком обробки персональних даних²⁵; б) забезпечити надання медичними працівниками письмового зобов'язання про нерозголошення персональних даних, які їм було довірено або які стали їм відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків, що корелює з п. 3.7 Типового порядку обробки персональних даних; в) заклад охорони здоров'я/ФОП, яка провадить господарську діяльність з медичної практики, повинен повідомляти суб'єкта персональних даних про склад і зміст зібраних персональних даних, його права, визначені Законом України «Про захист персональних даних», мету збору персональних даних і третіх осіб, яким передаються його персональні дані; г) заклад охорони здоров'я/ ФОП, яка провадить господарську діяльність з медичної практики, повинен вести облік операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них; г) підготувати План дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій, або як додаток до локального порядку обробки персональних даних, або як окремий документ; д) у локальний порядок обробки персональних даних треба вмістити розділ про заходи безпеки та механізми доступу до комп'ютерів чи іншої техніки, на яких здійснюється обробка персональних даних при функціонуванні електронної системи охорони здоров'я. Приміром, доречно вказати, що: а) приміщення, де здійснюється обробка персональних даних, замикаються (або не замикаються) та обладнані сигналізацією (не обладнані сигналізацією); б) доступ до таких приміщень мають виключно певні працівники, які визначені керівником закладу охорони здоров'я/ФОП, яка провадить господарську діяльність з медичної практики (всі працівники володільця); в) доступ до бази здійснюється за допомогою ключа ідентифікаційної чи мікропроцесорної карти; г) комп'ютери захищені кодом доступу (паролем); г) комп'ютери, на яких здійснюється обробка персональних даних, приєднані до мережі та на них встановлено антивірусне та інше програмне забезпечення.

10. При повідомленні Уповноваженого з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, володілець повинен зазначити загальний опис технічних та організаційних заходів, до яких він вдається з метою забезпечення захисту персональних даних. Згідно з Роз'ясненнями Уповноваженого Верховної Ради України з прав людини основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод

25. Типовий порядок обробки персональних даних : Наказ Уповноваженого ВРУ з прав людини від 08.01.2014 № 1-02/14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n215

суб'єктів персональних даних, від 08.01.2014, текст може бути таким: *Володільцем прийнято внутрішній порядок обробки персональних даних та визначено відповідальну особу. Приміщення, де стоять комп'ютери, на яких здійснюється обробка персональних даних, замикаються. Для отримання ключа необхідно поставити відмітку в журналі. Визначено коло працівників, які мають доступ до персональних даних, а також рівні доступу таких працівників. Комп'ютери, у яких містяться персональні дані, захищені паролем. Кожен працівник має особистий пароль. Усі операції, пов'язані з обробкою персональних даних, автоматично фіксуються за допомогою спеціалізованого програмного забезпечення²⁶.*

Типове порушення: безпідставне відбирання суб'єктами обробки даних згоди про обробку персональних даних від пацієнтів при наданні медичної допомоги.

Національне законодавство й акти автентичного тлумачення

Відповідно до ст. 32 Конституції України, ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини²⁷.

Згідно зі ст. 6 Закону України «Про захист персональних даних», обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб'єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством (ч. 5). Не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини (ч. 6 ст. 6 цього ж Закону).

У ст. 11 Закону України «Про захист персональних даних» нормативно визначено вичерпний перелік підстав для обробки персональних даних, а саме: 1) згода суб'єкта персональних даних на обробку його персональних даних; 2) дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень; 3) укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних; 4) захист життєво важливих інтересів суб'єкта персональних даних; 5) необхідність виконання обов'язку володільця персональних даних, який передбачений законом; 6) необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта персональних даних у зв'язку з обробкою його даних переважають такі інтереси. У ч. 1 ст. 7 Закону України «Про захист персональних даних» зазначено, що забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях і професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних. У ч. 2 цієї ж статті Закону України «Про захист персональних даних» вказано, що положення частини першої цієї статті не застосовується, якщо обробка персональних даних: 6) необхідна в цілях охорони здоров'я для: встановлення

26. Роз'яснення Уповноваженого Верховної Ради України з прав людини основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, від 08.01.2014. URL: <https://zakon.rada.gov.ua/laws/show/n0003715-14#Text>

27. Конституція України від 28.06.1996. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>

медичного діагнозу, для забезпечення піклування чи лікування або надання медичних послуг, моніторингу відповідності встановленим умовам надання таких послуг (у тому числі умовам договорів про медичне обслуговування населення та договорів про реімбурсацію за програмою медичних гарантій), функціонування електронної системи охорони здоров'я за умови, що такі дані обробляються медичним працівником, фахівцем з реабілітації або іншою особою закладу охорони здоров'я, реабілітаційного закладу 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 і поширюється дія законодавства про лікарську таємницю, працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення, працівниками закладу, що здійснює державний санітарно-епідеміологічний нагляд і провадить діяльність у галузі громадського здоров'я, який одержав ліцензію на провадження господарської діяльності з медичної практики, на яких покладено обов'язки щодо забезпечення захисту персональних даних.

У ч. 2 ст. 12 Закону України «Про захист персональних даних» закріплено, що суб'єкт персональних даних повідомляється про володільця персональних даних, склад і зміст зібраних персональних даних, свої права, визначені цим Законом, мету збору персональних даних та осіб, яким передаються його персональні дані: в момент збору персональних даних, якщо персональні дані збираються у суб'єкта персональних даних; в інших випадках протягом тридцяти робочих днів з дня збору персональних даних, крім випадків, встановлених законом²⁸.

У п. 23 Порядку функціонування електронної системи охорони здоров'я, затвердженому постановою КМУ від 25.04.2018 № 411, 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 і поширюється дія законодавства про лікарську таємницю, працівниками Національної служби здоров'я України (НСЗУ), на яких покладено обов'язки щодо забезпечення захисту персональних даних. Оператори електронної медичної інформаційної системи обробляють персональні дані за наявності правових підстав відповідно до вимог Закону України «Про захист персональних даних»²⁹.

Відповідно до п. 2.7 Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого з прав людини від 08.01.2014 № 1-02/14 (далі — Типовий порядок), обробка персональних даних здійснюється володільцем персональних даних лише за згодою суб'єкта персональних даних, за винятком тих випадків, коли такої згоди не вимагає Закон.

Згідно з п. 2.9 Типового порядку, володільць персональних даних, крім випадків, передбачених законодавством України, повідомляє суб'єкта персональних даних про склад і зміст зібраних персональних даних, його права, визначені Законом, мету збору персональних даних і третіх осіб, яким передаються його персональні дані:

- у момент збору персональних даних, якщо персональні дані збираються у суб'єкта персональних даних;

28. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI.

URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

29. Порядок функціонування електронної системи охорони здоров'я : Постанова КМУ від 25.04.2018 № 411.

URL: <https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text>

- в інших випадках протягом тридцяти робочих днів з дня збору персональних даних.

Володілець зберігає інформацію (документи), які підтверджують надання заявнику вищезазначеної інформації протягом усього періоду обробки персональних даних³⁰.

У Наказі МОЗ України «Про внесення змін до деяких наказів Міністерства охорони здоров'я України» від 08.08.2014 № 549 зазначено, що, відповідно до Закону України «Про захист персональних даних», з метою виконання подання Уповноваженого Верховної Ради України з прав людини від 02.06.2014 № 1-1014/14-105, Міністр наказує:

1. Внести зміни до таких наказів Міністерства охорони здоров'я України:

1) у наказі Міністерства охорони здоров'я України від 14 лютого 2012 року № 110 «Про затвердження форм первинної облікової документації та інструкцій щодо їх заповнення, що використовуються у закладах охорони здоров'я незалежно від форми власності та підпорядкування», зареєстрованому в Міністерстві юстиції України 28 квітня 2012 року за № 661/20974: підпункт 1.38 пункту 1 виключити³¹.

У Наказі МОЗ України «Про затвердження форм первинної облікової документації та Інструкцій щодо їх заповнення, що використовуються у закладах охорони здоров'я незалежно від форми власності та підпорядкування» від 14.02.2012 № 110 закріплено: підпункт 1.38 пункту 1 (вкладний листок до облікових форм «Інформована добровільна згода пацієнта на обробку персональних даних») виключено на підставі Наказу МОЗ № 549 від 08.08.2014³².

У п. 15 Роз'яснення до Типового порядку обробки персональних даних від 08.01.2014 зазначено: також не можна обумовлювати реалізацію законодавчо встановлених прав наданням особою згоди на обробку її персональних даних³³.

У листі-роз'ясненні Уповноваженого Верховної Ради України з прав людини «Щодо деяких питань взаємодії з Уповноваженим Верховної Ради України з прав людини стосовно порушень у сфері захисту персональних даних» від 11.03.2020 № 26.4/1365-20 зазначено: також необхідно усвідомлювати, що чинне законодавство передбачає можливість укладення правочину через процедуру приєднання до публічного договору (публічної оферти). Приєднання може бути реалізовано, зокрема, шляхом завантаження мобільного додатка, заповнення певної форми на вебсайті або вчиненням якихось конклюдентних дій (отримання грошових коштів, здійснення розрахунків тощо), які можуть свідчити про таке приєднання. Оскільки процедура приєднання та умови використання персональних даних у таких випадках мають бути врегульовані умовами правочину (договору), радимо ретельно вивчати його умови³⁴.

30. Типовий порядок обробки персональних даних : Наказ Уповноваженого ВРУ з прав людини від 08.01.2014 № 1-02/14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n215

31. Про внесення змін до деяких наказів Міністерства охорони здоров'я України : Наказ МОЗ України від 08.08.2014 № 549. URL: <https://zakon.rada.gov.ua/laws/show/z1049-14#n8>

32. Про затвердження форм первинної облікової документації та Інструкцій щодо їх заповнення, що використовуються у закладах охорони здоров'я незалежно від форми власності та підпорядкування : Наказ МОЗ України від 14.02.2012 № 110. URL: <https://zakon.rada.gov.ua/laws/show/z0661-12#Text>

33. Роз'яснення до Типового порядку обробки персональних даних від 08.01.2014. URL: <https://zakon.rada.gov.ua/laws/show/n0001715-14#Text>

34. Лист-роз'яснення Уповноваженого Верховної Ради України з прав людини «Щодо деяких питань взаємодії з Уповноваженим Верховної Ради України з прав людини стосовно порушень у сфері захисту персональних даних» від 11.03.2020 № 26.4/1365-20. URL: <https://ombudsman.gov.ua/storage/app/media/uploaded-files/onovleniyshchodo-deyakikh-pitan-stosovno-porushen-u-sferi-zakhistu-personalnikh-danikh-finansovimi-kompaniyami.pdf>

Рекомендації

1. Підставою для обробки персональних даних пацієнта (за потреби — даних членів його/її сім'ї, законних представників) закладами охорони здоров'я/ФОП, яка провадить господарську діяльність з медичної практики, є дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень (п. 2 ч. 1 ст. 11 Закону України «Про захист персональних даних»). У законі, а саме в п. 6 ч. 2 ст. 7 Закону України «Про захист персональних даних», право на обробку персональних даних визначено і є достатньою підставою для обробки персональних даних. Це право не залежить від надання чи не надання згоди суб'єктом персональних даних.
2. Гарантоване Конституцією України право особи на охорону здоров'я, медичну допомогу та медичне страхування (ст. 49) не може залежати від надання особою згоди на обробку персональних даних, а особа не може бути примушена закладом охорони здоров'я/ФОП, яка провадить господарську діяльність з медичної практики, до надання такої згоди.
3. Підкреслимо, що МОЗ України виключило форму «Інформована добровільна згода пацієнта на обробку персональних даних» з наказу від 14.02.2012 № 110, що корелює з вимогами Закону України «Про захист персональних даних», про що зазначено в преамбулі наказу МОЗ України від 08.08.2014 № 549.
4. Умови обробки персональних даних можуть бути закріплені в різних документах, приміром, бути умовою правочинів (у тому числі публічних), ліцензійних умов використання програмних продуктів (зокрема мобільних медичних додатків), угод користувача, політики конфіденційності, реєстраційних форм на вебсайтах тощо. Отож, фізичним особам, які звертаються за медичними послугами, треба уважно знайомитись з такими документами (приміром, при укладенні/приєднанні до правочину треба ретельно ознайомитися з його умовами), а закладу охорони здоров'я/ФОП, яка провадить господарську діяльність з медичної практики, необхідно чітко регламентувати порядок обробки персональних даних.
5. Заклад охорони здоров'я/ФОП, яка провадить господарську діяльність з медичної практики, повинен повідомляти пацієнта/законного представника пацієнта про обробку персональних даних. Повідомлення повинно містити інформацію про склад і зміст зібраних персональних даних, права суб'єкта персональних даних, визначені Законом України «Про захист персональних даних» (ст. 8), мету збору персональних даних і третіх осіб, яким передаються його персональні дані. Доречно примірну форму затвердити розпорядчим актом. Привернемо увагу до питання щодо можливості робити застереження при повідомленні про обробку персональних даних. Відповідно до норми пп. 10 п. 2 ст. 8 Закону України «Про захист персональних даних», суб'єкту персональних даних можна вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди. Проте, вважаємо, що з огляду на подібні за змістом цивільні відносини, використовуючи принцип аналогії закону, у повідомленні також доречно робити застереження. Приміром, таким застереженням може бути інформація про коло осіб, яким пацієнт (законний представник пацієнта) дозволяє медичним працівникам надавати свою (пацієнта та/або свою) медичну інформацію. Але важливо, аби така гарантія щодо застереження у повідомленні мала чіткий нормативний регламент, що потребує внесення змін до Закону України «Про захист персональних даних» і розширення обсягу прав суб'єкта персональних даних.

Типове порушення: безпідставне відбирання згоди про обробку персональних даних від своїх працівників суб'єктами обробки персональних даних.

Національне законодавство й акти автентичного тлумачення

У ст. 11 Закону України «Про захист персональних даних» нормативно визначено вичерпний перелік підстав для обробки персональних даних, а саме: 1) згода суб'єкта персональних даних на обробку його персональних даних; 2) дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень; 3) укладення та виконання правочину, стороною якого є суб'єкт персональних даних або який укладено на користь суб'єкта персональних даних чи для здійснення заходів, що передують укладенню правочину на вимогу суб'єкта персональних даних; 4) захист життєво важливих інтересів суб'єкта персональних даних; 5) необхідність виконання обов'язку володільця персональних даних, який передбачений законом; 6) необхідність захисту законних інтересів володільця персональних даних або третьої особи, якій передаються персональні дані, крім випадків, коли потреби захисту основоположних прав і свобод суб'єкта персональних даних у зв'язку з обробкою його даних переважають такі інтереси. У ч. 1 ст. 7 Закону України «Про захист персональних даних» зазначено, що забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях і професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних. У ч. 2 цієї ж статті Закону України «Про захист персональних даних» вказано, що положення частини першої цієї статті не застосовується, якщо обробка персональних даних: 2) необхідна для здійснення прав і виконання обов'язків володільця у сфері трудових правовідносин відповідно до закону із забезпеченням відповідного захисту³⁵.

Відповідно до п. 2.7. Типового порядку обробки персональних даних, затвердженого наказом Уповноваженого з прав людини від 08.01.2014 № 1-02/14 (далі — Типовий порядок), обробка персональних даних здійснюється володільцем персональних даних лише за згодою суб'єкта персональних даних, за винятком тих випадків, коли такої згоди не вимагає Закон.

Згідно з п. 2.9 Типового порядку, володільць персональних даних, крім випадків, передбачених законодавством України, повідомляє суб'єкта персональних даних про склад і зміст зібраних персональних даних, його права, визначені Законом, мету збору персональних даних і третіх осіб, яким передаються його персональні дані:

- у момент збору персональних даних, якщо персональні дані збираються у суб'єкта персональних даних;
- в інших випадках протягом тридцяти робочих днів з дня збору персональних даних.

Володільць зберігає інформацію (документи), які підтверджують надання заявнику вищезазначеної інформації, протягом усього періоду обробки персональних даних³⁶.

У п. 2.1 Порядку повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної

35. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI.
URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

36. Типовий порядок обробки персональних даних : Наказ Уповноваженого Верховної Ради України з прав людини від 08.01.2014 № 1-02/14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n215

інформації, затвердженому Наказом Уповноваженого з прав людини від 08.01.2014 № 1-02/14 (далі — Порядок повідомлення), зазначено: володілець персональних даних повідомляє Уповноваженого про здійснення ним будь-яких видів обробки персональних даних, які становлять особливий ризик для прав і свобод суб'єктів персональних даних, крім випадків, якщо: обробка необхідна для реалізації прав і виконання обов'язків володільця персональних даних у сфері трудових правовідносин відповідно до закону (п. 2.1.3.)³⁷.

У п. 15 Роз'яснення до Типового порядку обробки персональних даних від 08.01.2014 зазначено: також не можна обумовлювати реалізацію законодавчо встановлених прав наданням особою згоди на обробку її персональних даних³⁸.

Рекомендації

1. Підставою для обробки персональних даних закладами охорони здоров'я/ФОП, яка провадить господарську діяльність з медичної практики, у сфері трудових правовідносин є дозвіл на обробку даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень (п. 2 ч. 1 ст. 11 Закону України «Про захист персональних даних»). У законі, а саме в п. 2 ч. 2 ст. 7 Закону України «Про захист персональних даних», право на обробку персональних даних у сфері трудових правовідносин визначено і є достатньою підставою для обробки персональних даних працівників із забезпеченням відповідного їх захисту. Це право не залежить від надання чи ненадання згоди суб'єктом персональних даних.

2. Гарантоване Конституцією України право особи на працю (ст. 43) не може залежати від надання особою згоди на обробку персональних даних, а особа не може бути примушена роботодавцем до надання такої згоди. Підкреслимо, що, відповідно до ч. 2 ст. 24 Кодексу законів про працю України, при укладенні трудового договору громадянин зобов'язаний подати паспорт або інший документ, що посвідчує особу, трудову книжку (у разі наявності) або відомості про трудову діяльність з реєстру застрахованих осіб Державного реєстру загальнообов'язкового державного соціального страхування, а у випадках, передбачених законодавством, — також документ про освіту (спеціальність, кваліфікацію), про стан здоров'я, відповідний військово-обліковий документ та інші документи³⁹. Отож, працівник згоди на обробку персональних даних у сфері трудових правовідносин не подає.

3. Повідомляти Уповноваженого з прав людини про обробку персональних даних, які становлять особливий ризик для прав і свобод суб'єктів персональних даних у сфері трудових правовідносин відповідно до закону, не потрібно.

4. Роботодавець повинен повідомляти працівника про обробку персональних даних. Повідомлення повинно містити інформацію про склад і зміст зібраних персональних даних, права суб'єкта персональних даних, визначені Законом України «Про захист персональних даних» (ст. 8), мету збору персональних даних і третіх осіб, яким передаються його персональні дані. Доречно примірну форму затвердити розпорядчим актом.

37. Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов'язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації: Наказ Уповноваженого ВРУ з прав людини від 08.01.2014 № 1-02/14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n215

38. Роз'яснення до Типового порядку обробки персональних даних від 08.01.2014. URL: <https://zakon.rada.gov.ua/laws/show/n0001715-14#Text>

39. Кодекс законів про працю України : Закон від 10.12.1971 № 322-VIII. URL: <https://zakon.rada.gov.ua/laws/show/322-08#Text>

5. Треба враховувати, що заклади охорони здоров'я, які слугують базами стажування для лікарів-інтернів для підготовки в інтернатурі, що здійснюється за кошти державного бюджету, не повинні брати згоди на обробку персональних даних від лікарів-інтернів. Адже якщо лікар-інтерн навчається за бюджетні кошти, то база стажування формує штатний розпис, у якому є посада лікаря-інтерна, і включає його в штат. Такого лікаря-інтерна на посаді табелюють і виплачують йому заробітну плату.

6. Проте якщо лікар-інтерн навчається за кошти фізичних або юридичних осіб, то його не включають у штат закладу охорони здоров'я, табель на нього не ведеться, йому надаються платні послуги й база стажування лише створює умови для його навчання. Важливо, аби при укладенні договору між базою стажування і лікарем-інтерном отримувалась згода на обробку персональних даних лікаря-інтерна або щоб пункт про згоду на обробку даних був відображений при договірному регулюванні відносин.

Типове порушення: обробка даних при контролі якості медичної допомоги без згоди суб'єкта персональних даних.

Національне законодавство й акти автентичного тлумачення

У ч. 1 ст. 7 Закону України «Про захист персональних даних» зазначено, що забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях і професійних спілках, засудження до кримінального покарання, а також даних, які стосуються здоров'я, статевого життя, біометричних або генетичних даних. У ч. 2 цієї ж статті Закону України «Про захист персональних даних» зазначено, що положення ч. 1 цієї статті не застосовується, якщо обробка персональних даних: б) необхідна в цілях охорони здоров'я для: контролю якості надання медичних послуг за умови, що такі дані обробляються працівниками центрального органу виконавчої влади, який реалізує державну політику у сфері контролю якості надання медичних послуг⁴⁰.

У п. 7 р. IV Положення про клініко-експертну комісію МОЗ України, затвердженого Наказом МОЗ України від 05.02.2016 № 69, зазначено, що члени КЕК МОЗ беруть участь у засіданнях КЕК МОЗ особисто та повинні забезпечувати конфіденційність отриманої інформації. У п. 19 р. IV цього ж Положення з-поміж обов'язків експерта КЕК МОЗ закріплено: забезпечення конфіденційності отриманої інформації⁴¹.

У п. 7 р. IV Положення про клініко-експертну комісію Міністерства охорони здоров'я Автономної Республіки Крим, структурних підрозділів з питань охорони здоров'я обласних, Київської та Севастопольської міських державних адміністрацій, затвердженого Наказом МОЗ України від 05.02.2016 № 69, закріплено, що члени КЕК беруть участь у засіданнях КЕК особисто та повинні забезпечувати конфіденційність отриманої інформації. У п. 19 р. IV цього ж Положення з-поміж обов'язків експерта КЕК закріплено: забезпечення конфіденційності отриманої інформації⁴².

40. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI.
URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

41. Про організацію клініко-експертної оцінки якості надання медичної допомоги та медичного обслуговування : Наказ МОЗ України від 05.02.2016 № 69. URL: <https://zakon.rada.gov.ua/laws/show/z0285-16#Text>

42. Про організацію клініко-експертної оцінки якості надання медичної допомоги та медичного обслуговування : Наказ МОЗ України від 05.02.2016 № 69. URL: <https://zakon.rada.gov.ua/laws/show/z0286-16#n4>

Правові позиції ЄСПЛ

Рішення ЄСПЛ у справі «Л. Х. проти Латвії»: справа стосувалася скарги заявниці щодо збору її персональних медичних даних державною установою, що порушило її право на повагу до приватного життя, гарантоване ст. 8 Конвенцією з прав людини.

ЄСПЛ відзначив: «Сенат висловив згоду із заявницею, що обробка її конфіденційних даних є втручанням в її права, гарантовані, серед іншого, ст. 8 Конвенції... Далі Сенат перейшов до висновків Страсбурзького Суду у двох справах, на які заявниця зробила посилання, зазначивши, зокрема, що Конвенція залишає державам широку свободу розсуду щодо балансу між конфіденційністю медичних даних і необхідністю збереження конфіденційності пацієнтів у медичній професії, а також у наданні медичних послуг загалом...

Суд бере до уваги аргумент Уряду про те, що, виходячи з тлумачення національного законодавства Сенатом Верховного Суду, MADEKKI була уповноважена здійснювати оцінку якості медичних послуг, що надавалися медичними установами, не лише після отримання скарг від пацієнтів, але також у відповідь на «запити», які, на думку Сенату, є запитами від медичних установ (п. 48). Суд зауважує, що чинні законодавчі норми описували повноваження MADEKKI в загальних рисах. Сенат Верховного Суду не надав пояснень, які з цих повноважень виконувала MADEKKI або яку суспільну мету вона мала, коли надавала звіт з приводу законності проведення лікування заявниці. Відповідно, Сенат не міг перевірити й не перевірів пропорційність втручання у право заявниці на повагу до приватного життя проти будь-яких суспільних інтересів, особливо, коли стало відомо, що такого висновку вже дійшов законодавець.

Суд зазначає, що, як вбачається, MADEKKI збрала медичні дані заявниці безсистемно, без будь-якої попередньої оцінки щодо того, чи будуть зібрані дані «потенційно вирішальними», «доречними» або «важливими» (див. справу М. С. проти Швеції, яка цитується вище, пп. 38, 42 та 43, та справу Л.Л. проти Франції (L.L. v. France), № 7508/02, п. 46, ЄСПЛ 2006 XI) для досягнення будь-якої мети розслідування, що проводилось MADEKKI. У такому контексті вже не так важливо, чи був персонал MADEKKI юридично зобов'язаний зберігати конфіденційність персональних даних (п. 52)»⁴³.

Рекомендації

1. Підставою для обробки персональних даних пацієнта (за потреби — даних членів його/її сім'ї, законних представників) Клініко-експертною комісією МОЗ є дозвіл на обробку персональних даних, наданий комісії відповідно до закону виключно для здійснення її повноважень (п. 2 ч. 1 ст. 11 Закону України «Про захист персональних даних»). У законі, а саме в абз. 2 п. 6 ч. 2 ст. 7 Закону України «Про захист персональних даних», право на обробку персональних даних визначено і є достатньою підставою для обробки персональних даних. Це право не залежить від надання чи ненадання згоди суб'єктом персональних даних.

2. Підставою для обробки персональних даних пацієнта (за потреби — даних членів його/її сім'ї, законних представників) Клініко-експертною комісією Міністерства охорони здоров'я Автономної Республіки Крим, структурних підрозділів з питань охорони здоров'я обласних, Київської та Севастопольської міських державних адміністрацій є згода суб'єкта персональних даних на обробку його персональних даних (п. 1 ч. 1 ст. 11 Закону України «Про захист персональних даних»). Така згода повинна отримуватись від пацієнта/законного представника пацієнта при зверненні його до комісії.

43. Рішення Європейського суду з прав людини щодо захисту персональних даних : збірник. С. 91.
URL: <https://rm.coe.int/168059920d>

3. У разі надсилання постанови органу досудового розслідування чи ухвали суду про проведення клініко-експертної оцінки якості медичної допомоги та медичного обслуговування згоди суб'єкта персональних даних не потрібно, адже підставами для обробки даних комісією буде дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень, і захист життєво важливих інтересів суб'єкта персональних даних (п. 2 і 4 ч. 1 ст. 11 Закону України «Про захист персональних даних»). Згідно з ч. 2 ст. 93 КПК України, органи досудового розслідування здійснюють збирання доказів, зокрема шляхом отримання актів перевірок. При провадженні досудового розслідування у медичних справах (справах, пов'язаних з правовідносинами у сфері медичного обслуговування) постановою слідчого неодмінно призначається проведення клініко-експертної оцінки, адже відомче розслідування є необхідним, відповідно до п. 24 Правил проведення комісійних судово-медичних експертиз у бюро судово-медичної експертизи, затверджених Наказом МОЗ України від 17.01.1995 № 6, для проведення комісійної судово-медичної експертизи, яка є обов'язковою для такої категорії справ (ч. 2 ст. 242 КПК України). У цьому випадку доречно говорити про баланс публічного та приватного інтересів й переважатиме саме публічний. У рішенні ЄСПЛ «З. проти Фінляндії» зазначено: водночас ЄСПЛ визнає, що інтереси розслідування злочину та гласності судового процесу можуть переважати над інтересами як пацієнта, так і громадськості загалом стосовно недопущень розголошення медичної таємниці (п. 97)⁴⁴.

4. Підставою для обробки персональних даних пацієнта (за потреби — даних членів його/її сім'ї, законних представників) медичною радою є згода суб'єкта персональних даних на обробку його персональних даних. Така згода повинна отримуватись від пацієнта/законного представника пацієнта при його зверненні до медичної ради.

5. Усі члени медичної ради повинні забезпечувати конфіденційність отриманої інформації при проведенні внутрішнього контролю якості медичної допомоги. Оскільки пряма нормативна вказівка не закріплена в Положенні про медичну раду закладу охорони здоров'я, затвердженому Наказом МОЗ України від 05.02.2016 № 69, то при підготовці локального акта у закладі охорони здоров'я треба прописати норму щодо конфіденційності.

Типове порушення: ненадання медичної інформації та копій медичної документації членам сім'ї померлого пацієнта.

Національне законодавство й акти автентичного тлумачення

У ч. 2 ст. 34 Конституції України гарантовано, що кожен має право вільно збирати, зберігати, використовувати й поширювати інформацію усно, письмово або в інший спосіб — на свій вибір. Водночас у ч. 3 цієї ж статті визначено, що здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя⁴⁵.

Згідно зі ст. 5 Закону України «Про інформацію», кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів. Реалізація права на інформацію

44. Рішення ЄСПЛ у справі «З проти Фінляндії» від 25.02.1997.

URL: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-58033%22%7D>

45. Конституція України від 28.06.1996.

URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>

не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб⁴⁶.

У ст. 7 Закону України «Про поховання та похоронну справу» зазначено, що держава гарантує конфіденційність інформації про померлого. Надання такої інформації здійснюється відповідно до Закону України «Про інформацію»⁴⁷.

У ч. 4 ст. 285 ЦК України зазначено, що у разі смерті фізичної особи члени її сім'ї або інші фізичні особи, уповноважені ними, мають право бути присутніми при дослідженні причин її смерті та ознайомитись із висновками щодо причин смерті, а також право на оскарження цих висновків до суду⁴⁸. Відповідно до ч. 5 ст. 39 Основ, у разі смерті пацієнта члени його сім'ї або інші уповноважені ними фізичні особи мають право бути присутніми при дослідженні причин його смерті та ознайомитись з висновками щодо причин смерті, а також право на оскарження цих висновків до суду⁴⁹.

У Рішенні Конституційного Суду України від 20.01.2012 № 2-рп/2012 у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України зазначено, що інформація про особисте та сімейне життя особи (персональні дані про неї) — це будь-які відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована, а саме: національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, матеріальний стан, адреса, дата і місце народження, місце проживання та перебування тощо, дані про особисті майнові та немайнові відносини цієї особи з іншими особами, зокрема членами сім'ї, а також відомості про події та явища, що відбувалися або відбуваються у побутовому, інтимному, товариському, професійному, діловому та інших сферах життя особи, за винятком даних стосовно виконання повноважень особою, яка займає посаду, пов'язану зі здійсненням функцій держави або органів місцевого самоврядування. Така інформація про фізичну особу та членів її сім'ї є конфіденційною і може бути поширена тільки за її згодою, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини⁵⁰.

У рішенні Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К. Г. Устименка) від 30.10.1997 зазначено, що медична інформація — свідчення про стан здоров'я людини, історію її хвороби, про мету запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, у тому числі про наявність ризику для життя і здоров'я, за своїм правовим режимом належить до конфіденційної інформації, тобто інформації з обмеженим доступом. Лікар зобов'язаний на вимогу пацієнта, членів його сім'ї або законних представників надати їм таку інформацію повністю і в доступній формі.

У випадках відмови у наданні або навмисного приховування медичної інформації від пацієнта, членів його сім'ї або законного представника вони можуть оскаржити дії чи бездіяльність

46. Про інформацію : Закон від 02.10.1992 № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>

47. Про поховання та похоронну справу : Закон від 10.07.2003 № 1102-IV.

URL: <https://zakon.rada.gov.ua/laws/show/1102-15#Text>

48. Цивільний кодекс України від 16.01.2003 № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>

49. Основи законодавства України про охорону здоров'я : Закон України від 19.11.1992 № 2801-XII.

URL: <https://zakon.rada.gov.ua/laws/show/2801-12#Text>

50. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України від 20.01.2012 № 2-рп/2012.

URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12#Text>

лікаря безпосередньо до суду або, за власним вибором, до медичного закладу чи органу охорони здоров'я⁵¹.

У листі-роз'ясненні Уповноваженого Верховної Ради України з прав людини від 25.01.2018 № 2/9-Кзоб655.17/26-131 зазначено: «З аналізу вказаних положень законодавства вбачається, що відомості про померлу особу, котра була членом сім'ї або близьким родичом запитувача інформації про неї, які стосуються їхніх особистих майнових або немайнових відносин або пов'язані з подіями, що відбулися у їхньому спільному житті, можуть розглядатись як персональні дані особи, яка запитує інформацію про померлу особу. Отже, можна дійти висновку, що інформація про померлу особу може надаватись членам її сім'ї, близьким особам та родичам, якщо така інформація необхідна їм для реалізації їхніх прав, свобод і законних інтересів, за умови надання копій документів, які підтверджують родинний зв'язок»⁵².

Практика національних судів

Першотравневий суд м. Чернівці розглядав цивільну справу за позовом ОСОБА_1 до Чернівецької обласної клінічної лікарні, Лікарні швидкої медичної допомоги про надання копій історії хвороби (справа № 2-438/12; рішення від 11.06.2012 (рішення набрало законної сили. — І.С.)): «ОСОБА_1 09.09.2011 р. зверталась до головного лікаря Чернівецької обласної клінічної лікарні щодо надання копії історії хвороби її чоловіка ОСОБА_2, який перебував на стаціонарному лікуванні в ОКЛ у відділенні реанімації з 27.06.2011 р. до 28.07.2011 р. Відповідь їй було надано у формі резолюції на заяві: «Первинна медична документація приватним особам не надається». Цього ж дня ОСОБА_1 звернулася до головного лікаря обласної комунальної установи «Лікарні швидкої медичної допомоги» щодо надання копії історії хвороби її чоловіка ОСОБА_2, який поступив у відділення урології ЛШМД 20.06.2011 р. та був виписаний з відділення реанімації 27.06.2011 р. На зазначений запит 28.09.2011 р. отримала відповідь від ЛШМД без зазначення мотивів відмови, а лише з посиланням на Закон України «Про доступ до публічної інформації», без зазначення статті та з вказівкою, що «підстави для надання запитуваної інформації відсутні». Представник обласної клінічної лікарні позов визнав, не заперечував проти надання копії історії хвороби. Представник лікарні швидкої медичної допомоги позов не визнав, у своїх поясненнях і письмових запереченнях просив у позові відмовити.

У процесі судового розгляду, вислухавши доводи сторін і дослідивши матеріали справи, суд вважав, що позов підлягає задоволенню. Визнано протиправними дії Чернівецької обласної клінічної лікарні та Лікарні швидкої медичної допомоги щодо ненадання ОСОБА_1 копій історій хвороби її чоловіка ОСОБА_2. Зобов'язано Чернівецьку обласну клінічну лікарню та Лікарню швидкої медичної допомоги надати ОСОБА_1: 1) копію історії хвороби ОСОБА_2 1946 р. н. (у повному обсязі), який поступив у відділення урології ЛШМД 20.06.2011 р. та був виписаний з відділення реанімації 27.06.2011 р. та 2) копію історії хвороби ОСОБА_2 1946 р. н. народження (у повному обсязі), який перебував на стаціонарному лікуванні в обласній клінічній лікарні у відділенні реанімації з 27.06.2011 р. до 28.07.2011 р. Своє рішення суд, зокрема, мотивував так: «У ст. 285 Цивільного кодексу України закріплено право членів сім'ї у разі смерті фізичної особи бути присутніми при дослідженні причин її смерті та ознайомитись із висновками щодо причин смерті. У Рішенні Конституційного Суду України від 30 жовтня 1997 р. у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та ст. 12 Закону України «Про прокуратуру» визначено,

51. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К. Г. Устименка) від 30.10.1997 справа № vd971030 vn5-зп. URL: <https://zakon.rada.gov.ua/laws/show/v005p710-97#Text>

52. Лист-роз'яснення Уповноваженого Верховної Ради України з прав людини № 2/9-Кзоб655.17/26-131 від 25.01.2018. Медичне право. 2018. № 1(21).

що медична інформація — це свідчення про стан здоров'я людини, історію її хвороби, про мету запропонованих досліджень і лікувальних заходів, прогноз можливого розвитку захворювання, у тому числі про ризик для життя і здоров'я, яка за своїм правовим режимом належить до конфіденційної. Також у Рішенні Конституційного Суду України зазначено обов'язок лікаря на вимогу пацієнта та членів його сім'ї або законних представників надавати їм таку інформацію повністю і в доступній формі. Рішення Конституційного Суду України є обов'язковим для виконання на території України, остаточною і не може бути оскарженим»⁵³.

Рекомендації

1. Нормативною підставою для підготовки запиту члена сім'ї до закладу охорони здоров'я/ФОП, яка провадить господарську діяльність з медичної практики, у разі смерті пацієнта є Закон України «Про інформацію», адже йдеться про витребування документів, які містять інформацію (зокрема, медичні дані) померлого/померлої. Закон України «Про інформацію» не передбачає спеціального засобу звернення та строків розгляду такого. Отже, поряд з інформаційним законом треба використовувати положення Закону України «Про звернення громадян». Алгоритм за результатами аналізу обидвох законів буде таким: засіб звернення — заява, а строки для її розгляду треба використовувати ті, які передбачені в ст. 20 Закону України «Про звернення громадян». Підкреслимо, що особа, яка звертається із заявою, повинна дотримуватись вимог законодавства, аби звернення було задоволено та особа отримала необхідну інформацію.
2. У разі смерті пацієнта законодавчі акти, зокрема ч. 4 ст. 285 ЦК України, ч. 5 ст. 39 Основ, наділяють членів його сім'ї деякими правами в сфері охорони здоров'я. Приміром, аналіз форми № 003/о «Медична карта стаціонарного хворого» та Інструкції щодо заповнення форми № 003/о, затверджених Наказом МОЗ України «Про затвердження форм первинної облікової документації та Інструкцій щодо їх заповнення, що використовуються у закладах охорони здоров'я незалежно від форми власності та підпорядкування» від 14.02.2012 № 112 (ред. від 21.01.2016 № 29) дає підстави стверджувати, що в медичній карті стаціонарного хворого містяться, поряд з іншою інформацією, відомості про причини смерті, адже в цій формі є окремий підрозділ «Виписка з протоколу (карти) патологоанатомічного обстеження» (п. 58–65), який є складовою форми № 003/о. Відтак, аби забезпечити належну реалізацію права, окресленого в наведених вище нормах, проте, пам'ятаючи про право на таємницю про стан здоров'я пацієнта, яке повинно дотримуватись після його смерті, вважаємо, що копії медичної документації повинні надаватись членам сім'ї за умови належно оформленої заяви на підставі Закону України «Про інформацію».
3. У кожному конкретному випадку заявник повинен надати підтверджувальні документи, що він член сім'ї померлого пацієнта, вказавши в додатку до заяви конкретний документ, який засвідчує ці дані. Як додатки необхідно долучати такі документи: а) копію паспорта, завірену власноручним підписом; б) копію документа, яка засвідчує, що особа була членом сім'ї померлого (зокрема, копію свідоцтва про шлюб, якщо йдеться про подружжя).
4. У законодавстві України про охорону здоров'я не міститься спеціальної дефініції поняття «член сім'ї» для царини охорони здоров'я. Ця прогалина породжує чимало правореалізаційних і правозастосовних проблем, адже межа між лікарською таємницею та медичною інформацією надто хистка. Відтак лакуну треба заповнити, аби не виникало проблем на практиці.

53. Сенюта І. Я. Цивільно-правове регулювання відносин у сфері надання медичної допомоги: питання теорії і практики : монографія. Львів : Видавництво ЛОБФ «Медицина і право», 2018. 640 с.

Національне законодавство й акти автентичного тлумачення

Згідно зі ст. 8 Конвенції з прав людини, кожен має право на повагу до свого приватного і сімейного життя⁵⁴. У ст. 32 Конституції України зазначено, що ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини⁵⁵.

У ст. 286 ЦК України гарантовано право на таємницю про стан здоров'я. Фізична особа має право на таємницю про стан свого здоров'я, факт звернення за медичною допомогою, діагноз, а також про відомості, одержані при її медичному обстеженні. Забороняється вимагати та подавати за місцем роботи або навчання інформацію про діагноз і методи лікування фізичної особи. Фізична особа зобов'язана утримуватися від поширення інформації, зазначеної у частині першій цієї статті, яка стала їй відома у зв'язку з виконанням службових обов'язків або з інших джерел. Фізична особа може бути зобов'язана до проходження медичного огляду у випадках, встановлених законодавством⁵⁶.

У ст. 39-1 Основ визначено, що пацієнт має право на таємницю про стан свого здоров'я, факт звернення за медичною допомогою, діагноз, а також про відомості, одержані при його медичному обстеженні. Забороняється вимагати та надавати за місцем роботи або навчання інформацію про діагноз і методи лікування пацієнта.

Відповідно до ст. 40 «Лікарська таємниця» Основ, медичні працівники та інші особи, яким у зв'язку з виконанням професійних або службових обов'язків стало відомо про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя громадянина, не мають права розголошувати ці відомості, крім передбачених законодавчими актами випадків. При використанні інформації, що становить лікарську таємницю, у навчальному процесі, науково-дослідній роботі, у тому числі у випадках її публікації у спеціальній літературі, повинна бути забезпечена анонімність пацієнта. Відповідно до п. «г» ч. 1 ст. 78 Основ, медичні працівники зобов'язані дотримуватися вимог професійної етики і деонтології, зберігати лікарську таємницю⁵⁷.

У ст. 13 Закону України «Про протидію поширенню хвороб, зумовлених вірусом імунодефіциту людини (ВІЛ), та правовий і соціальний захист людей, які живуть з ВІЛ» зазначено, що відомості про результати тестування на ВІЛ, про наявність або відсутність в особі ВІЛ-інфекції є конфіденційними та становлять лікарську таємницю. Медичні працівники зобов'язані вживати необхідних заходів для забезпечення дотримання встановленого законодавством порядку зберігання конфіденційної інформації про людей, які живуть з ВІЛ, захисту такої інформації від розголошення та розкриття третім особам. Будь-які особи, яким стала відомою інформація про результати тестування на ВІЛ, зобов'язані не розголошувати її, крім випадків, встановлених законом. Передача медичним працівником відомостей, зазначених у частині третій цієї статті, дозволяється лише: іншим медичним працівникам і закладам охорони здоров'я, фізичним особам — підприємцям, які провадять господарську діяльність з медичної практики, виключно у зв'язку з наданням усіх

54. Конвенція про захист прав людини і основоположних свобод від 04.11.1950.

URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

55. Конституція України від 28.06.1996.

URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>

56. Цивільний кодекс України від 16.01.2003 № 435-IV. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>

57. Основи законодавства України про охорону здоров'я : Закон України від 19.11.1992 № 2801-XII.

URL: <https://zakon.rada.gov.ua/laws/show/2801-12#Text>

видів медичної допомоги людям, які живуть з ВІЛ, та закладам громадського здоров'я з метою здійснення епідеміологічного нагляду за ВІЛ-інфекцією. Передача відомостей, зазначених у частині третій цієї статті, іншим медичним працівникам і закладам охорони здоров'я допускається лише для цілей, пов'язаних з лікуванням хвороб, зумовлених ВІЛ, та у разі якщо поінформованість лікаря щодо ВІЛ-статусу пацієнта має істотне значення для його лікування⁵⁸.

Згідно зі ст. 6 Закону України «Про психіатричну допомогу», медичні працівники, інші фахівці, які беруть участь у наданні психіатричної допомоги, та особи, яким у зв'язку з навчанням або виконанням професійних, службових, громадських чи інших обов'язків стало відомо про наявність у особи психічного розладу, про факти звернення за психіатричною допомогою та лікування у закладі з надання психіатричної допомоги чи про перебування у закладі соціального захисту осіб, які страждають на психічні розлади, або спеціальному навчальному закладі, а також інші відомості про стан психічного здоров'я особи, її приватне життя, не можуть розголошувати ці відомості, крім випадків, передбачених частинами третьою, четвертою та п'ятою цієї статті. За усвідомленою письмовою згодою особи або її законного представника відомості про стан психічного здоров'я цієї особи та надання їй психіатричної допомоги можуть передаватися іншим особам лише в інтересах особи, яка страждає на психічний розлад, для проведення обстеження та лікування чи захисту її прав і законних інтересів, для здійснення наукових досліджень, публікацій у науковій літературі, використання в навчальному процесі. У листку непрацездатності, що видається особі, яка страждає на психічний розлад, діагноз психічного розладу вписується за згодою цієї особи, а у разі її незгоди — лише причина непрацездатності (захворювання, травма або інша причина).

Забороняється без письмової згоди особи або без письмової згоди її законного представника та лікаря-психіатра, який надає психіатричну допомогу, публічно демонструвати особу, яка страждає на психічний розлад, фотографувати її чи робити кінозйомку, відеозапис, звукозапис і прослуховувати співбесіди особи з медичними працівниками чи іншими фахівцями при наданні їй психіатричної допомоги⁵⁹.

Кримінально-правові гарантії містяться у ст. 132 КК України, а саме кримінально караним є розголошення службовою особою лікувального закладу, допоміжним працівником, який самостійно здобув інформацію, або медичним працівником відомостей про проведення медичного огляду особи на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби, що є небезпечною для життя людини, або захворювання на синдром набутого імунодефіциту (СНІД) та його результатів, що стали їм відомі у зв'язку з виконанням службових або професійних обов'язків. Окрім того, у ст. 145 КК України зазначено, що протиправним є умисне розголошення лікарської таємниці особою, якій вона стала відома у зв'язку з виконанням професійних чи службових обов'язків, якщо таке діяння спричинило тяжкі наслідки⁶⁰.

У п. 2 ч. 2 ст. 65 КПК України закріплено положення, за яким медичні працівники та інші особи, яким у зв'язку з виконанням професійних або службових обов'язків стало відомо про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторону життя особи, не можуть бути допитані як свідки про відомості, які становлять лікарську таємницю. Звільнення від окресленого професійного обов'язку може бути здійснено лише особою, яка довірила зазначеним вище особам відомості, що становлять лікарську таємницю. Обсяг відомостей, які можуть бути

58. Про протидію поширенню хвороб, зумовлених вірусом імунодефіциту людини (ВІЛ), та правовий і соціальний захист людей, які живуть з ВІЛ : Закон України від 12.12.1991 № 1972-XII (ред. від 23.12.2010).
URL: <https://zakon.rada.gov.ua/laws/show/1972-12#Text>

59. Про психіатричну допомогу : Закон України від 22.02.2000 № 1489-III.
URL: <https://zakon.rada.gov.ua/laws/show/1489-14#Text>

60. Кримінальний кодекс України від 05.04.2001 № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>

правомірно розголошенні, також визначає особа, яка їх надала, тобто це пацієнт чи його законний представник⁶¹.

У ч. 4 ст. 188-39 КУпАП України вказано, що недодержання встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них або порушення прав суб'єкта персональних даних, тягне за собою накладення штрафу на громадян від ста до п'ятисот неоподатковуваних мінімумів доходів громадян і на посадових осіб, громадян — суб'єктів підприємницької діяльності — від трьохсот до однієї тисячі неоподатковуваних мінімумів доходів громадян⁶².

У Клятві лікаря України, затвердженій Указом Президента України від 15.06.1992, закріплено, що лікар клянеться зберігати лікарську таємницю, не використовувати її на шкоду людині⁶³.

У пп. 18 п. 13 Ліцензійних умов провадження господарської діяльності з медичної практики, затверджених постановою КМУ від 02.03.2016 № 285, закріплено обов'язок ліцензіата зберігати лікарську таємницю⁶⁴.

У рішенні Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К. Г. Устименка) від 30.10.1997 зазначено, що правила використання відомостей, які стосуються лікарської таємниці — інформації про пацієнта, на відміну від медичної інформації — інформації для пацієнта, встановлюються статтею 40 Основ законодавства України про охорону здоров'я⁶⁵.

Практика національних судів

Постанова Верховного Суду від 11.11.2020 у справі № 442/4791/17: «З аналізу вказаних нормативних актів вбачається, що медичною таємницею є: факт звернення людини до лікувального закладу за медичною допомогою; стан здоров'я людини; діагноз; обставини, що передували захворюванню або спровокували його, функціональні особливості організму; шкідливі звички, особливості психіки, майновий стан, інші відомості, отримані при медичному обстеженні, зокрема інформація про сімейне, інтимне життя людини, а також про стан здоров'я родичів, близьких пацієнта. Тобто під визначення медичної таємниці підпадають абсолютно всі аспекти, що стосуються здоров'я пацієнта. Лікар, медсестра, будь-який інший медичний працівник або інші особи, яким у зв'язку з виконанням їхніх професійних чи службових обов'язків стало відомо про хворобу, не має права розголошувати як медичну, так і немедичну інформацію про стан здоров'я людини. Такі особи не мають права розголошувати ці відомості, крім передбачених законодавчими актами випадків»⁶⁶.

Постанова Верховного Суду від 29.06.2022 у справі № 205/9115/19: «Оскільки розголошення таких даних може значно вплинути на приватне та сімейне життя особи, на її соціальний статус і зайнятість, піддаючи таку особу ганьбі та ризику бути вигнанцем у суспільстві. Також з

61. Кримінальний процесуальний кодекс України від 13.04.20212 № 4651-VI.

URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text>

62. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X.

URL: <https://zakon.rada.gov.ua/laws/show/80731-10#Text>

63. Клятва лікаря України : Указ Президента України від 15.06.1992 № 349.

URL: <https://zakon.rada.gov.ua/laws/show/349/92#Text>

64. Ліцензійні умови провадження господарської діяльності з медичної практики : Постанова КМУ від 02.03.2016 № 285. URL: <https://zakon.rada.gov.ua/laws/show/285-2016-%D0%BF#Text>

65. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К. Г. Устименка) від 30.10.1997 справа № vd971030 vn5-зп. URL: <https://zakon.rada.gov.ua/laws/show/v005p710-97#Text>

66. Постанова Верховного Суду від 11.11.2020 у справі № 442/4791/17. URL: <https://zakononline.com.ua/court-decisions/show/93666639>

цієї підстави особа може втратити бажання дізнатись про свій діагноз та отримати медичну допомогу, у результаті чого зруйнувати всі ті профілактичні заходи, які вживаються суспільством, щоб запобігти пандемії. Тому зацікавленість у конфіденційності такої інформації матиме вагоміше значення при визначенні того, чи втручання у здійснення цього права відповідає меті закону, яка переслідується. Таке втручання не може визнаватись таким, що відповідає статті 8 Конвенції, якщо тільки воно не виправдане певними важливішими суспільними інтересами. Беручи до уваги особливо інтимну та вразливу природу інформації про захворювання особи на ВІЛ, будь-які державно-владні заходи, які примушують надавати чи розголошувати таку інформацію без згоди пацієнта, зобов'язують суд бути дуже уважним і ретельно досліджувати такі обставини, як це роблять гарантії, прийняті для забезпечення ефективного захисту.

Суди першої та апеляційної інстанцій, відмовляючи у задоволенні вимог про визнання незаконними дії медичного працівника щодо розголошення конфіденційної інформації про стан здоров'я пацієнта, не врахували, що такі дії призвели до втручання у право на повагу до приватного і сімейного життя, закріплене у статті 8 Конвенції. Такі дії медичного працівника не були обґрунтовані належним чином, а отже, підлягають визнанню незаконними. Під час розгляду справи у судах першої та апеляційної інстанцій відповідач не довів, що втручання у право на повагу до приватного і сімейного життя було виправданим»⁶⁷.

Постанова Великої Палати Верховного Суду від 15.04.2021 у справі № 11-727сап19: «До охоронюваної законом таємниці, яка міститься в речах і документах, відповідно до пункту 2 частини першої статті 162 цього Кодексу, належать відомості, що можуть становити лікарську таємницю. Метою обмеження законодавцем доступу до такої інформації є втілення передбаченого частиною першою статті 286 Цивільного кодексу України (далі — ЦК), статтею 39-1 «Основ законодавства України про охорону здоров'я» права пацієнта на нерозголошення відомостей про стан його здоров'я, факт звернення за медичною допомогою, діагноз, а також даних, одержаних при медичному обстеженні. Із зазначеними нормами кореспондується закріплена у частині третій статті 286 ЦК, статті 40 «Основ законодавства про охорону здоров'я України» заборона медичним працівникам та іншим особам, яким відповідна інформація стала відома у зв'язку з виконанням службових обов'язків чи з інших джерел, поширювати її. Об'єктом правового захисту є інформація про стан здоров'я, зі змістом якої особа не може бути обізнаною за відсутності підстав, передбачених законом»⁶⁸.

Постанова Апеляційного суду Запорізької області від 19.10.2016 справа № 335/9129/16-п: «Таким чином, розголосивши всупереч вимогам частини 1 статті 40 Основ законодавства України про охорону здоров'я, частини 3 статті 10, частини 1 статті 24 Закону України «Про захист персональних даних» у листі від 11.05.2016 № 01-01/292 персональні дані ОСОБА_3, її чоловіка ОСОБА_5 та їхньої дитини, а саме повідомив про відомості стосовно групи крові і резус-фактора вказаних осіб, головний лікар КЗ «Обласний перинатальний центр ЗОР» ОСОБА_, як посадова особа володільця персональних даних не забезпечив належний рівень захисту таких даних, чим 11.05.2016 у місті Запоріжжі (вул. Південноукраїнська, буд.17-А) вчинив діяння, яке містить ознаки адміністративного правопорушення, передбаченого частиною 4 статті 188-39 КУпАП, а саме не дотримався встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них сторонніх осіб і порушення прав суб'єкта персональних даних, зокрема ОСОБА_3, ОСОБА_5 та їхньої дитини на захист своїх персональних даних від незаконної обробки (п.7 ч.2 ст.8 Закону).

67. Постанова Верховного Суду від 29.06.2022 у справі № 205/9115/19.

URL: <https://reyestr.court.gov.ua/Review/105110286>

68. Постанова Великої Палати Верховного Суду від 15.04.2021 у справі № 11-727сап19.

URL: <https://zakononline.com.ua/court-decisions/show/96822603>

Отже, дані, що стосуються здоров'я особи та її біометричні дані, є персональними даними, щодо яких законом встановлені особливий порядок обробки та заборона поширення без згоди суб'єкта персональних даних.

Твердження апеляційної скарги про те, що відомості про групу крові та резус-фактор не є конфіденційною інформацією, позбавлені сенсу, оскільки, як встановлено вище, ОСОБА_2 було допущено поширення персональних даних у супереч встановленому законодавством порядку про захист персональних даних»⁶⁹.

Рішення Індустріального районного суду м. Дніпропетровська від 22.05.2015 у справі № 202/2249/15-ц: «Зовнішність є невідчужуваним нематеріальним благом, що належить фізичній особі від народження. У зміст цього правового блага входять можливість фізичної особи формувати свою зовнішність за своїм розсудом, зберігати і змінювати її, визначати коло осіб, яким фізична особа надає можливість огляду своєї зовнішності, фіксувати або дозволяти фіксацію своєї зовнішності в певний момент часу, наприклад фотографуванням, відеозйомкою тощо.

Хоча зовнішність громадянина прямо не згадана в статті 270 ЦК України, за своїми ознаками вона входить у відкритий перелік тих нематеріальних благ, про які йдеться в цій нормі. Зовнішність є індивідуалізуючим фізичну особу в суспільстві елементом її особистості. Саме тому опис зовнішності фізичної особи або її зображення являють собою частину відомостей про її особистість.

Крім того, зовнішність як елемент особистості фізичної особи, зафіксована в її зображенні в певний час, може складати її особисту таємницю. Більш того, будь-яке не оприлюднене самою фізичною особою власне зображення треба сприймати як бажання зберегти його в таємниці від третіх осіб. Представляється, що саме таємниця зовнішнього вигляду фізичної особи і є тим нематеріальним благом, на охорону якого спрямоване положення статті 308 ЦК України. Тому не дозволене фізичною особою оприлюднення її зображення треба розглядати як незаконне розголошення її особистої таємниці, за винятком випадків, коли таке оприлюднення прямо дозволено законом»⁷⁰.

У постанові Орджонікідзевського районного суду м. Запоріжжя від 16.09.2016 у справі № 335/9130/16-п зазначено: «Таким чином, розголосивши всупереч вимогам частини 1 статті 40 Основ законодавства України про охорону здоров'я, частини 3 статті 10, частини 1 статті 24 Закону України «Про захист персональних даних» у листі від 12.02.2016 № 01-8/179 персональні дані ОСОБА_4, а саме відомості про факт його звернення за медичною допомогою, результати його медичного обстеження, діагноз, ступінь тяжкості одержаної травми, групу крові і резус-фактор, головний лікар комунальної установи «Міська клінічна лікарня екстреної та швидкої медичної допомоги м. Запоріжжя» ОСОБА_3 як посадова особа володільця персональних даних не забезпечив належний рівень захисту таких даних, чим 12.02.2016 у місті Запоріжжі (вул. Перемоги, буд.80) вчинив діяння, яке містить ознаки адміністративного правопорушення, передбаченого частиною 4 статті 188-39 КУпАП, а саме не дотримався встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до незаконного доступу до них сторонніх осіб і порушення прав суб'єкта персональних даних, зокрема права ОСОБА_4 на захист своїх персональних даних від незаконної обробки (п.7 ч.2 ст.8 Закону)»⁷¹.

69. Постанова Апеляційного суду Запорізької області від 19.10.2016 у справі № 335/9129/16-п.
URL: <https://reyestr.court.gov.ua/Review/62152284>

70. Рішення Індустріального районного суду м. Дніпропетровська від 22.05.2015 у справі № 202/2249/15-ц.
URL: <https://reyestr.court.gov.ua/Review/44397094>

71. Постанова Орджонікідзевського районного суду м. Запоріжжя від 16.09.2016 у справі № 335/9130/16-п.
URL: <https://reyestr.court.gov.ua/Review/61411160>

У постанові Дніпровського районного суду м. Києва від 14.09.2016 у справі № 755/13162/16-п вказано: «Таким чином, надавши конфіденційну інформацію про факти звернення за медичною допомогою малолітніх дітей ОСОБА_2 на адвокатський запит ОСОБА_, як посадова особа володільця персональних даних («КДЦ дитячий») не забезпечив належний рівень захисту персональних даних ОСОБА_4 та ОСОБА_5, чим 19.12.2014 у м. Київ по просп. П. Тичини, 12 вчинив адміністративне правопорушення, передбачене ч. 4 ст. 188-39 Кодексу України про адміністративні правопорушення, а саме не дотримався встановленого законодавством про захист персональних даних порядку захисту персональних даних, що призвело до порушення права ОСОБА_4 та ОСОБА_5 на захист своїх персональних даних від незаконної: обробки (п. 7 ч. 2 ст. 8 Закону України «Про захист персональних даних») та права на таємницю про стан свого здоров'я, факт звернення за медичною допомогою (ч. 1 ст. 39-1 Основ: законодавства України про охорону здоров'я). ... ОСОБА_1 визнати винним у вчиненні адміністративного правопорушення, передбаченого ч. 4 ст. 188-39 Кодексу України про адміністративні правопорушення»⁷².

Правові позиції ЄСПЛ

Рішення ЄСПЛ у справі «М. К. проти України»: «Хоча сторони не дійшли згоди стосовно певних обставин у зв'язку з цим, не оскаржується, що посадові особи госпіталю надали матері заявниці інформацію про ВІЛ-статус заявниці (див. пункт 16). З огляду на його згадану практику Суд вважає, що розголошення госпіталем конфіденційної інформації про стан здоров'я заявниці її матері, у якій би формі це не було зроблено, призвело до втручання у право заявниці на повагу до її приватного життя, гарантованого ч. 1 ст. 8 Конвенції... Стосовно аргументу Уряду, що матері заявниці вже було відомо про діагноз доньки під час розмови з посадовими особами госпіталю, Суд зазначає, що національні суди чи Уряд не послалися на законні підстави, які б доводили, що цей факт звільняв би їх від загального зобов'язання за законом зберігати конфіденційність відомостей про стан здоров'я заявниці... Суд уже визнавав, що роботодавці можуть мати законний інтерес в отриманні відомостей про стан фізичного здоров'я своїх працівників, зокрема у контексті покладання на них певних професійних обов'язків, пов'язаних з особливими навичками, відповідальністю або повноваженнями, однак він підкреслював, що збирання та обробка відповідних відомостей мають бути законними та забезпечувати справедливий баланс між інтересами роботодавця та захистом недоторканності приватного життя кандидата на зайняття відповідної посади.

У цій справі національні суди посилалися на Положення як на законну підставу для обробки даних про стан здоров'я заявниці. Суд зауважує, що Положення було загальнодоступним документом, який встановлював конкретні правила регулювання медичних оглядів військовослужбовців, і дозволяв доступ до даних про стан здоров'я військовослужбовців за результатами огляду військово-лікарськими комісіями та командиром відповідної військової частини, без винятків стосовно діагнозу (див. пункт 25).

Проте Суд зауважує, що застосування зазначених норм Положення до діагнозу ВІЛ явно суперечить Закону «Про ВІЛ», на який посилалася заявниця і який надавав особливий захист особам з ВІЛ-позитивним статусом і встановлював вичерпний перелік осіб та установ, які могли бути поінформовані про ВІЛ-позитивний статус особи; цей закон не передбачав жодного винятку щодо нерозголошення відомостей стосовно військовослужбовців, якою б не була мета (див. пункт 24)»⁷³.

72. Постанова Дніпровського районного суду м. Києва від 14.09.2016 у справі № 755/13162/16-п.
URL: <https://reyestr.court.gov.ua/Review/61350702>

73. Рішення ЄСПЛ у справі «М. К. проти України» від 15.12.2022.
URL: https://zakon.rada.gov.ua/laws/show/974_i18#Text

Рішення ЄСПЛ у справі «М. С. проти Швеції»: «Охорона даних особистого характеру й особливо медичних даних має основоположне значення для здійснення права на повагу до приватного та сімейного життя. Дотримання конфіденційності відомостей про здоров'я становить основний принцип правової системи всіх держав — учасниць Конвенції. Він є важливим не лише для захисту приватного життя хворих, а й для збереження їхньої довіри до працівників медичних закладів і системи охорони здоров'я взагалі. Національне законодавство має забезпечувати відповідні гарантії, щоб унеможливити будь-яке повідомлення чи розголошення даних особистого характеру стосовно здоров'я, якщо це не відповідає гарантіям, передбаченим статтею 8 Конвенції»⁷⁴.

У рішенні ЄСПЛ у справі «З. проти Фінляндії» зазначено: «Захист персональних даних — у зазначеній справі медичного характеру — має фундаментальне значення для реалізації особою свого права на повагу до приватного та сімейного життя. Відповідно держава зобов'язана визначити ефективні гарантії, аби запобігти оприлюдненню такої інформації. ЄСПЛ зважає на фундаментальне значення захисту персональних даних, причому не лише медичних, для здійснення права на повагу до приватного та сімейного життя, як це гарантується статтею 8 Конвенції. Повага до конфіденційності даних про фізичний стан є основним принципом у правових системах усіх держав — учасниць Конвенції. Суттєво важлива не тільки повага до особистого життя хворих, а й також їхня довіра до представників медичної професії і служби охорони здоров'я загалом. Без такого захисту ті, хто потребує медичної допомоги, можуть утриматися від надання інформації особистого чи інтимного характеру, необхідної для потрібного лікування, і навіть від звернення за такою допомогою, ставлячи під загрозу своє здоров'я, а у випадку заразних хвороб — і здоров'я суспільства. Тому внутрішнє законодавство має надавати належні гарантії для запобігання поширенню або розголошенню таких даних про здоров'я людини, що несумісні з гарантіями статті 8 Конвенції»⁷⁵.

Рекомендації

1. Медичні працівники повинні суворо дотримуватись обов'язку зберігати лікарську таємницю. З огляду на нечіткість законодавчої регламентації інституту «лікарської таємниці», зокрема термінологічну, доцільно використовувати дефініцію, запропоновану Верховним Судом: медичною таємницею є: факт звернення людини до лікувального закладу за медичною допомогою; стан здоров'я людини; діагноз; обставини, що передували захворюванню або спровокували його, функціональні особливості організму; шкідливі звички, особливості психіки, майновий стан, інші відомості, отримані при медичному обстеженні, зокрема інформація про сімейне, інтимне життя людини, а також про стан здоров'я родичів, близьких пацієнта. Тобто під визначення медичної таємниці підпадають абсолютно всі аспекти, що стосуються здоров'я пацієнта.
2. Моментом припинення права фізичної особи на таємницю про стан здоров'я як особистого немайнового права є момент смерті особи, проте обов'язок зберігати медичну таємницю зберігається і після смерті пацієнта.
3. Доступ до процесуальних джерел доказів (речей, документів), які містять охоронювану законом таємницю, а саме лікарську, повинен здійснюватися із судовим контролем, на підставі ухвали суду, що чітко закріплено в главі 15 КПК України. Недотримання процедури збору доказів у досліджуваному контексті призведе до порушення законодавства про охорону здоров'я, а саме в аспекті дотримання лікарської таємниці, а також до порушення конвенційного і конституційного

74. Рішення ЄСПЛ у справі «М. С. проти Швеції» від 27.08.1997. URL: <file:///C:/Users/Admin/Downloads/001-45889.pdf>

75. Рішення ЄСПЛ у справі «З. проти Фінляндії» від 25.02.1997. URL: <https://hudoc.echr.coe.int/eng#%7B%22site%22:%5B%22001-58033%22%5D%7D>. Інші рішення ЄСПЛ див.: Рішення Європейського суду з прав людини щодо захисту персональних даних. URL: <https://rm.coe.int/168059920d>

прав людини, що є істотним порушенням прав і свобод людини. Заклад охорони здоров'я або фізична особи — підприємець, яка має ліцензію на провадження господарської діяльності з медичної практики, повинні надавати можливість зробити копії документів та вилучити речі та документи (здійснити їх виїмку) виключно за наявності в органу досудового розслідування ухвали суду про надання тимчасового доступу до речей і документів.

4. Медичний працівник за необхідності фотографування пацієнта, приміром, аби зафіксувати клінічний результат до і після втручання, повинен обов'язково отримати згоду. Хоча законодавець не передбачає такої згоди обов'язково в письмовій формі, видається за доцільну саме письмова форма. Вважаємо, що заява повинна містити такі основні положення: 1) пацієнт надає право на фотографування з клінічною метою, із зазначенням, що такі світлини будуть розміщені в його медичній документації; 2) у разі виникнення у медичного працівника бажання поширити світлини в соціальних мережах з метою презентації своєї діяльності чи оприлюднити на конференціях у наукових цілях тощо пацієнт повинен обов'язково надати згоду саме на таке опублікування фотографій, з позначенням мети, а також з обов'язковою вказівкою щодо персоналізації.

5. Оскільки зовнішність пацієнта або її зображення є частиною персональних даних, то при екстраполюванні на сферу охорони здоров'я віковим цензом, відповідно до ст. 285 ЦК України та ст. 39 Основ, буде повноліття, що пов'язано з реалізацією права на інформацію про стан здоров'я.

6. Медичні працівники можуть бути допитані як свідки у кримінальному процесі виключно за наявності звільнення від обов'язку зберігати професійну таємницю на підставі письмової згоди особи, яка довірила їм ці відомості, у визначеному нею обсязі.

Типове порушення: недотримання правил обробки даних при функціонуванні електронної системи охорони здоров'я.

Національне законодавство й акти автентичного тлумачення

У ч. 1 ст. 7 Закону України «Про захист персональних даних» зазначено, що забороняється обробка персональних даних про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в політичних партіях і професійних спілках, засудження до кримінального покарання, а також даних, що стосуються здоров'я, статевого життя, біометричних або генетичних даних. У ч. 2 цієї ж статті Закону України «Про захист персональних даних» вказано, що положення частини першої цієї статті не застосовується, якщо обробка персональних даних: б) необхідна в цілях охорони здоров'я для: встановлення медичного діагнозу, для забезпечення підключення чи лікування або надання медичних послуг, моніторингу відповідності встановленим умовам надання таких послуг (у тому числі умовам договорів про медичне обслуговування населення та договорів про реімбурсацію за програмою медичних гарантій), функціонування електронної системи охорони здоров'я за умови, що такі дані обробляються медичним працівником, фахівцем з реабілітації або іншою особою закладу охорони здоров'я, реабілітаційного закладу 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 і поширюється дія законодавства про лікарську таємницю, працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення, працівниками закладу, що здійснює державний санітарно-епідеміологічний нагляд і діяльність у галузі громадського здоров'я, який одержав ліцензію на провадження господарської діяльності з медичної практики, на яких покладено обов'язки щодо забезпечення захисту персональних даних. У ч. 2 ст. 8 Закону України «Про захист персональних даних» закріплено право суб'єкта персональних даних: на

доступ до своїх персональних даних (п. 3); отримувати не пізніше як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи обробляються його персональні дані, а також отримувати зміст таких персональних даних (п.4); пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем і розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними (п. 6).

Видалення або знищення персональних даних регламентовано в ст. 15 Закону України «Про захист персональних даних». Персональні дані видаляються або знищуються в порядку, встановленому відповідно до вимог закону. У ч. 2 цієї статті вказано, що персональні дані підлягають видаленню або знищенню у разі: 1) закінчення строку зберігання даних, визначеного згодою суб'єкта персональних даних на обробку цих даних або законом; 2) припинення правовідносин між суб'єктом персональних даних і володільцем чи розпорядником, якщо інше не передбачено законом; 3) видання відповідного припису Уповноваженого або визначених ним посадових осіб секретаріату Уповноваженого; 4) набрання законної сили рішенням суду щодо видалення або знищення персональних даних.

Персональні дані, зібрані з порушенням вимог цього Закону, підлягають видаленню або знищенню у встановленому законодавством порядку⁷⁶.

У ст. 24-1 Основ закріплено, що доступ до відомостей про пацієнта, які містяться в електронній системі охорони здоров'я, можливий лише у разі отримання згоди такого пацієнта (його законного представника) у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. Без згоди доступ до відомостей про пацієнта можливий лише: за наявності ознак прямої загрози життю пацієнта; у разі неможливості отримання згоди такого пацієнта чи його законного представника (до часу, коли отримання згоди стане можливим); за рішенням суду.

Підписуючи декларацію про вибір лікаря, який надає первинну медичну допомогу, пацієнт (його законний представник) надає згоду на доступ до відомостей про нього, що містяться в електронній системі охорони здоров'я, такому лікарю, а також іншим лікарям за його направленням у межах, необхідних для надання медичних послуг такими лікарями⁷⁷.

У ст. 182 КК України закріплено склад злочину «Порушення недоконаності приватного життя», тобто незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями цього Кодексу. Значний обсяг кримінально-правових гарантій закладено в розділі XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» КК України⁷⁸.

У п. 3 Порядку функціонування електронної системи охорони здоров'я, затвердженого постановою КМУ від 25.04.2018 № 411, вказано, що до складу електронної системи охорони здоров'я входять центральна база даних та електронні медичні інформаційні системи, між якими забезпечено автоматизований обмін інформацією, даними та документами через відкритий програмний інтерфейс (API). У п. 5 цього Порядку зазначено, що власником центральної бази даних, у тому числі майнових прав на програмне забезпечення центральної бази даних, є держава в особі НСЗУ. Володільцем відомостей Реєстру медичних спеціалістів, Реєстру суб'єктів господарювання у сфері охорони здоров'я, Реєстру медичних висновків є МОЗ. Розпорядником Реєстру

76. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI.

URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

77. Основи законодавства України про охорону здоров'я : Закон України від 19.11.1992 № 2801-XII.

URL: <https://zakon.rada.gov.ua/laws/show/2801-12#Text>

78. Кримінальний кодекс України від 05.04.2001 № 2341-III. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>

медичних спеціалістів, Реєстру суб'єктів господарювання у сфері охорони здоров'я, Реєстру медичних висновків є НСЗУ. Розпорядником інших реєстрів та володільцем їхніх відомостей та іншої інформації у центральній базі даних є НСЗУ, якщо інше не визначено законодавством.

У п. 23 Порядку зазначено, 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 і поширюється дія законодавства про лікарську таємницю, працівниками НСЗУ, на яких покладено обов'язки щодо забезпечення захисту персональних даних. Оператори електронної медичної інформаційної системи обробляють персональні дані за наявності правових підстав, відповідно до вимог Закону України «Про захист персональних даних».

З-поміж функціональних можливостей електронної системи охорони здоров'я у п. 8 Порядку визначено: можливість надання пацієнтами (їх законними представниками) згоди у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди, на доступ до даних про себе (про пацієнта для законних представників), що містяться в електронній системі охорони здоров'я, лікарям, третім особам (п. 5); отримання пацієнтами відомостей про осіб, які подавали запити щодо надання інформації, що міститься в електронній системі охорони здоров'я, про таких пацієнтів (п. 6); захист інформації від несанкціонованого доступу, знищення, модифікації (п. 10). У п. 11 Порядку встановлено, що обробка персональних даних у електронній системі охорони здоров'я здійснюється з дотриманням вимог Закону України «Про захист персональних даних».

У п. 26 Порядку гарантовано, що зміни та доповнення до інформації, яка міститься у центральній базі даних, здійснюється за заявою користувача. Якщо протягом десяти робочих днів з дня отримання такої заяви НСЗУ не відхилила таку заяву через наявність у ній помилок чи завідомо недостовірної інформації, до інформації у центральній базі даних вносяться відповідні зміни та доповнення. Інформація про користувача, який подав заяву про внесення змін і доповнень, дату та час їх внесення, а також початковий зміст інформації зберігається у центральній базі даних і не підлягає зміні чи видаленню. У п. 49 Порядку визначено, що доступ до персональних даних можливий у разі наявності згоди суб'єкта персональних даних, крім випадків, передбачених законом. З-поміж прав медичного працівника закріплено можливість подавати запити та отримувати доступ до даних про пацієнта, що містяться у центральній базі даних, у цілях охорони здоров'я, встановлення медичного діагнозу, забезпечення лікування або надання медичних послуг, функціонування електронної системи охорони здоров'я, якщо на такого медичного працівника покладено обов'язки щодо забезпечення захисту персональних даних і поширюється дія законодавства про лікарську таємницю у разі надання пацієнтом (його законним представником) на це згоди або без такої згоди у випадках, передбачених законом (п. 45 Порядку)⁷⁹.

У п. 13 Ліцензійних умов провадження господарської діяльності з медичної практики, затверджених постановою КМУ від 02.03.2016 № 285, закріплено обов'язок ліцензіата забезпечити роботу з електронною системою охорони здоров'я, зокрема внесення первинної облікової медичної документації, ведення обліку медичних послуг, управління медичною інформацією та використання інших функціональних можливостей електронної системи охорони здоров'я, які визначені законодавством обов'язковими в процесі провадження господарської діяльності з медичної

79. Порядок функціонування електронної системи охорони здоров'я : Постанова КМУ від 25.04.2018 № 411.
URL: <https://zakon.rada.gov.ua/laws/show/411-2018-%D0%BF#Text>

практики (п. 31); здійснювати обробку персональних даних та іншої інформації про пацієнтів (зокрема інформації про стан здоров'я, діагноз, наявні обмеження повсякденного функціонування/життєдіяльності, відомостей, одержаних під час медичного та/або реабілітаційного обстеження пацієнтів), у тому числі під час роботи в електронній системі охорони здоров'я, з дотриманням вимог Закону України «Про захист персональних даних» (п. 32)⁸⁰.

Відповідно до пп. 6 п. 4 Положення про Національну службу здоров'я України, затвердженого Постановою КМУ від 27.12.2017 № 1101, серед завдань НСЗУ є: отримання та обробка необхідних для здійснення своїх повноважень персональних даних та іншої інформації про пацієнтів (у тому числі інформації про стан здоров'я, діагноз, відомостей, одержаних під час медичного обстеження пацієнтів), надавачів медичних послуг, суб'єктів господарювання, які провадять господарську діяльність на підставі ліцензії на провадження господарської діяльності з роздрібною торгівлі лікарськими засобами та уклали договір про реімбурсацію, незалежно від форми власності та підпорядкування з дотриманням вимог Закону України «Про захист персональних даних»⁸¹.

Порядок ведення Реєстру медичних записів, записів про направлення та рецептів в електронній системі охорони здоров'я, затверджений наказом МОЗ України від 28.02.2020 № 587, визначає особливості ведення Реєстру медичних записів, записів про направлення та рецептів (далі — Реєстр) в електронній системі охорони здоров'я (далі — система), порядок його формування, перелік відомостей, що вносяться до Реєстру, та права доступу до них. Обробка персональних даних у Реєстрі здійснюється з метою забезпечення реалізації програми державних гарантій медичного обслуговування населення, а також для забезпечення функціонування електронної системи охорони здоров'я. Реєстр ведеться в центральній базі даних системи та формується з медичних записів, записів про направлення і рецептів, що внесені до системи відповідно до законодавства. Медичні записи, що внесені до Реєстру відповідно до цього Порядку, є первинною обліковою медичною документацією в електронній формі. Захист інформації в Реєстрі здійснюється відповідно до Закону України «Про захист інформації в інформаційно-комунікаційних системах».

У п. 21 Порядку ведення Реєстру зазначено, що на прохання пацієнта (його законного представника) медичний працівник з правом доступу до відповідних даних у системі повинен надати йому витяг з Реєстру з дотриманням вимог Закону України «Про захист персональних даних». Згідно з п. 22 Порядку ведення Реєстру, персональні дані, які містяться в Реєстрі у формі посилань на записи в інших реєстрах системи, обробляються протягом строку, визначеного порядком ведення відповідних реєстрів. Після закінчення строку обробки персональних даних медичні записи, записи про направлення та рецепти зберігаються у системі в знеособленому вигляді безстроково. Система забезпечує фіксацію та збереження інформації про всі операції, пов'язані з обробкою персональних даних і доступом до них.

Зміни до медичного запису, запису про направлення або рецепту вносяться шляхом створення нового запису в Реєстрі з одночасним проставленням відмітки про відміну запису, до якого вносяться зміни. Початковий зміст інформації, що міститься у медичному записі, записі про направлення або рецепті, зберігається у центральній базі даних та не підлягає зміні чи видаленню.

У п. 23 Порядку ведення Реєстру вказано, що в разі виявлення технічної неточності у медичному записі, записі про направлення або рецепті особою, яка його внесла до Реєстру, така особа повинна внести відповідні зміни до запису, а також повідомити про це пацієнта (його законного

80. Ліцензійні умови провадження господарської діяльності з медичної практики : Постанова КМУ від 02.03.2016 № 285. URL: <https://zakon.rada.gov.ua/laws/show/285-2016-%D0%BF#Text>

81. Положення про Національну службу здоров'я України : Постанова КМУ від 27.12.2017 № 1101. URL: <https://zakon.rada.gov.ua/laws/show/1101-2017-%D0%BF#Text>

представника) телефоном, електронною поштою або іншим доступним способом зв'язку протягом трьох днів з дня внесення таких змін.

Відповідно до п. 24 Порядку ведення Реєстру, право ознайомлення із записами у Реєстрі мають:

- пацієнт (його законний представник) щодо записів про себе (про пацієнта, законним представником якого він є);
- лікар первинної медичної допомоги (ПМД) та інші лікарі за його направленням у межах, необхідних для надання медичних послуг такими лікарями;
- медичні працівники під час надання ними медичної допомоги пацієнту та не більше трьох місяців з дати закінчення надання такої допомоги;
- особи, яким пацієнт надав згоду на доступ до його даних у Реєстрі;
- особа, яка наклала свій кваліфікований електронний підпис на відповідний запис (автор запису);
- уповноважені працівники НСЗУ, на яких покладено обов'язки щодо забезпечення захисту персональних даних, виключно для реалізації визначених законом повноважень;
- уповноважена особа суб'єкта господарювання, до якого пацієнт звернувся за направленням, у частині інформації, яка потрібна для запису пацієнта на прийом;
- уповноважена особа аптечного закладу, яка здійснює реєстрацію відпуску лікарського засобу або медичного виробу за рецептом до відомостей про такий рецепт⁸².

У п. 2.11 Типового порядку обробки персональних даних зазначено, що у разі виявлення відомостей про особу, які не відповідають дійсності, такі відомості мають бути невідкладно змінені або знищені. Суб'єкт персональних даних має право пред'являти вмотивовану вимогу володільцю персональних даних щодо заборони обробки своїх персональних даних (їх частини) та/або зміни їх складу/змісту. Така вимога розглядається володільцем упродовж 10 днів з моменту отримання (п. 2.12). У п. 2.16 Типового порядку обробки персональних даних встановлено, що видавлення та знищення персональних даних здійснюється у спосіб, що виключає подальшу можливість поновлення таких персональних даних⁸³.

У п. 9 Роз'яснень Уповноваженого Верховної Ради України з прав людини до Типового порядку обробки персональних даних зазначено, що всі персональні дані про особу, які обробляються володільцем, повинні відповідати дійсності. У разі виявлення будь-яких неточностей особа, чий персональні дані обробляються, має право звернутися з вимогою внести відповідні зміни до її персональних даних або звернутися зі скаргою до Уповноваженого чи до суду⁸⁴.

Правові позиції ЄСПЛ

Рішення ЄСПЛ у справі «І. проти Фінляндії»: *«Позивачка працювала медсестрою в поліклініці, де проводилося офтальмологічне лікування з 1989 по 1994 рр.; з 1987 р. позивачка проходила лікування у поліклініці, де проводилося лікування від інфекційних захворювань і було виявлено, що вона є ВІЛ-позитивною. На початку 1992 р. позивачка стала здогадуватися, що колеги знали*

82. Порядок ведення Реєстру медичних записів, записів про направлення та рецептів в електронній системі охорони здоров'я : Наказ МОЗ України від 28.02.2020 № 587. URL: <https://zakon.rada.gov.ua/laws/show/z0236-20#Text>

83. Типовий порядок обробки персональних даних: Наказ Уповноваженого ВРУ з прав людини від 08.01.2014 № 1-02/14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n215

84. Роз'яснення Уповноваженого Верховної Ради України з прав людини до Типового порядку обробки персональних даних від 08.01.2014. URL: <https://ombudsman.gov.ua/storage/app/media/uploaded-files/Rozyasnennya08012014-1.pdf>

про її хворобу. Спочатку реєстр пацієнтів був відкритим для усіх працівників лікарні, однак після того, як позивачка заявила про свої підозри своєму лікуючому лікареві, реєстр став доступним виключно для лікуючих лікарів, а сама позивачка фігурувала в реєстрі під несправжнім ім'ям. Згодом позивачка змінила роботу, проте не полишила питання того, хто міг отримати доступ до її медичної інформації, задля чого в листопаді 1996 р. звернулася до Округного адміністративного управління, аби перевірити це. Судячи з відповіді Управління, позивачка назвала кількох осіб, які потенційно могли мати доступ до її медичної документації, однак у відповіді значилося, що по проходженню тривалого періоду часу з'ясувати, хто саме мав цей доступ, уже не було можливим. Тоді позивачка звернулася з позовом до Округного управління охорони здоров'я з цивільним позовом, вимагаючи відшкодування майнової і немайнової шкоди через нездатність забезпечити конфіденційність її медичної інформації у реєстрі пацієнтів. Округний суд у рішенні від 10.04.2001, вислухавши п'ятьох свідків і думку Омбудсмена із захисту персональних даних, залишив позов без задоволення, мотивуючи відсутністю чітких доказів того, що інформація стосовно позивачки в реєстрі пацієнта незаконно переглядалася. Цієї ж думки дійшов і апеляційний суд у рішенні від 07.03.2002, який залишив апеляційну скаргу позивачки без задоволення; Верховний Суд Фінляндії відмовив у дозволі на апеляцію 23.12.2002. Тож позивачка звернулася до ЄСПЛ.

ЄСПЛ вирішив справу на користь позивачки, наголосивши, що лікарня, де проходила лікування позивачка, була державною, і очевидно, що інформація, через доступ до якої позивачка судилася у Фінляндії, а згодом — і в ЄСПЛ, належала до приватного життя позивачки. ЄСПЛ зазначив, що під час розгляду справи раніше не стверджувалося, що доступ до медичної інформації позивачки певних осіб при цьому становив певне умисне та неузгоджене розголошення медичної інформації, не оспорювався і факт, що медична інформація щодо позивачки дійсно зберігалася у вищезгаданих лікарняних реєстрах. Натомість позивачка заявляла, що лікарня не спромоглася належним чином гарантувати захищеність цієї інформації. ЄСПЛ відзначив інформацію у рішенні Округного адміністративного управління, що технічні можливості реєстрів не давали змогу визначити особу (осіб), які мали доступ до лікарняних реєстрів та електронних карток пацієнтів; якщо згадувати ситуацію на момент 1992 р. — на той час до лікарняних реєстрів мали доступ усі працівники лікарні, у тому числі ті, хто не брав безпосередньої участі в лікуванні пацієнтів. Цей момент і став ключовим для ухвалення рішення на користь позивачки. ЄСПЛ також додав, що представники держави-відповідача (Фінляндії) не надали пояснення, з яких причин гарантії законодавства Фінляндії не спрацювали належним чином у випадку витоку інформації стосовно проблем зі здоров'ям позивачки, нагадавши, що лише після витоку інформації, про що скоро здогадалася позивачка, інформація з лікарняних реєстрів стала доступна тільки лікуючим лікарям, а згодом — після звернення позивачки до Округного адміністративного управління — з'явилися нові технічні механізми контролю за доступом до інформації у цих реєстрах. Із цього ЄСПЛ дійшов висновку, що треба підтримати аргумент позивачки стосовно неналежного поводження з її персональними даними, а сам факт можливості в позивачки вимагати компенсацію через заподіяння їй шкоди виявився недостатнім, аби захистити її право на приватність. Отже, ЄСПЛ ухвалив рішення на користь позивачки, вважаючи, що порушення статті 8 (1) Конвенції мало місце в цій справі»⁸⁵.

Рекомендації

1. В Основах введено новий вид згоди — згоду на доступ до даних про пацієнта, що містяться в електронній системі охорони здоров'я (далі — ЕСОЗ). Запровадивши ЕСОЗ в закладі охорони

85. Рішення ЄСПЛ у справі «І. проти Фінляндії» від 17.07.2008. URL: [https://hudoc.echr.coe.int/eng#{%22fulltext%22:\[%22%220511/03\%22%22\],\[%22documentcollectionid%22:\[%22GRANDCHAMBER%22,%22CHAMBER%22\],\[%22itemid%22:\[%22001-87510%22\]}](https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22%220511/03\%22%22],[%22documentcollectionid%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],[%22itemid%22:[%22001-87510%22]})

здоров'я чи у фізичної особи — підприємця, яка має ліцензію на провадження господарської діяльності з медичної практики, необхідно отримувати окреслену згоду пацієнта або його законного представника. Форма альтернативна: а) письмова форма або б) форма, яка дає змогу дійти висновку про надання згоди. Законодавець закріпив винятки, за яких доступ до відомостей можливий без згоди: а) за наявності ознак прямої загрози життю пацієнта; б) у разі неможливості отримання згоди такого пацієнта чи його законного представника (до часу, коли отримання згоди стане можливим); в) за рішенням суду.

Водночас, згідно з п. 6 ч. 2 ст. 7 Закону України «Про захист персональних даних», згоди на обробку персональних даних не потрібно для функціонування ЕСОЗ за умови, що такі дані обробляються нормативно визначеним колом суб'єктів. Приміром, при доступі до даних пацієнта в ЕСОЗ згода пацієнта для медичного працівника не потрібна, адже він обробляє такі в силу закону як однієї з підстав, закріплених у п. 2 ч.1 ст. 11 Закону України «Про захист персональних даних».

2. При виникненні на практиці питання щодо законної можливості надання доступу членам сім'ї пацієнта або іншим фізичним особам, уповноваженим ними, до даних пацієнта в ЕСОЗ після його/її смерті, неможливості у такому випадку надати згоду на доступ до його/її даних треба врахувати таке: 1) існує нормативний дисонанс між ч. 4 ст. 285 ЦК України, ч. 5 ст. 39 Основ (у яких гарантовано, що в разі смерті фізичної особи члени її сім'ї або інші фізичні особи, уповноважені ними, мають право бути присутніми при дослідженні причин її смерті та ознайомитись із висновками щодо причин смерті, а також право на оскарження цих висновків до суду) та ч. 2 ст. 24-2 Основ, у якій з аналізу закріпленого випливає, що після смерті пацієнта окреслене коло осіб матиме право отримати доступ до даних померлого пацієнта в ЕСОЗ виключно за рішенням суду. За такого законодавчого дисонансу пріоритет матиме законодавча норма, передбачена ЦК України. У Постанові Верховного Суду від 25.01.2023 у справі № 676/47/21 вказано: *«У доктрині приватного права зауважується, що ієрархія актів цивільного законодавства може базуватися на їх юридичній силі (вимір по вертикалі). Вона поширюється, по-перше, на співвідношення закону та підзаконних актів та, по-друге, на співвідношення Конституції та законів (як кодифікованих, так і інших (поточних)). Водночас треба визнати існування ієрархії між ЦК як кодифікованим законом та іншими (поточними) законами, що регулюють цивільні відносини. Ця ієрархія базується на визнанні ЦК основним актом цивільного законодавства (вимір ієрархії по горизонталі). Стосовно виміру ієрархії актів цивільного законодавства по горизонталі, то в статті 4 ЦК України закріплюється пріоритет норм ЦК (як основного регулятора приватних відносин) над нормами інших законів»⁸⁶.*

3. Підставою для обробки персональних даних в ЕСОЗ є дозвіл на обробку персональних даних, наданий володільцю персональних даних відповідно до закону виключно для здійснення його повноважень (п. 2 ч. 1 ст. 11 Закону України «Про захист персональних даних»). У законі, а саме в абз. 2 п. 6 ч. 2 ст. 7 Закону України «Про захист персональних даних», право на обробку персональних даних визначено і є достатньою підставою для обробки персональних даних. Це право не залежить від надання чи ненадання згоди суб'єктом персональних даних. Звертаємо увагу на умову: такі дані обробляються медичним працівником, фахівцем з реабілітації або іншою особою закладу охорони здоров'я, реабілітаційного закладу 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 і поширюється дія законодавства про лікарську таємницю.

86. Постанова Верховного Суду від 25.01.2023 справа № 676/47/21. URL: https://verdictum.ligazakon.net/document/108654283?utm_source=jurliga.ligazakon.ua&utm_medium=news&utm_content=jl03

4. Заклад охорони здоров'я чи фізична особа — підприємець, яка має ліцензію на провадження господарської діяльності з медичної практики, зобов'язані визначити локальні організаційні заходи щодо захисту персональних даних, закріпивши їх у порядку обробки персональних даних. Зокрема, визначити порядок доступу до персональних даних працівників володільця/розпорядника, у тому числі в ЕСОЗ; порядок ведення обліку операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них; план дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій.

5. Право доступу до ЕСОЗ працівників закладу охорони здоров'я чи фізичної особи — підприємця, яка має ліцензію на провадження господарської діяльності з медичної практики (далі — володільці даних; у розумінні і працівників ФОП і самої ФОП у разі безпосереднього надання медичної допомоги), реалізується із дотриманням таких нормативних вимог:

- 1) володільці забезпечують ведення обліку працівників, які мають доступ до персональних даних суб'єктів персональних даних (зокрема, пацієнтів);
- 2) володільці визначають рівень доступу зазначених працівників до персональних даних суб'єктів;
- 3) кожен працівник володільців користується доступом лише до тих персональних даних (їх частини) суб'єктів, які необхідні йому/їй у зв'язку з виконанням своїх професійних чи службових або трудових обов'язків (тобто до даних своїх пацієнтів);
- 4) кожен працівник володільців, який має доступ до персональних даних, дає письмове зобов'язання про нерозголошення персональних даних, які йому/їй було довірено або які стали йому/їй відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків. Такий документ повинен зберігатися у відповідальній особи за обробку персональних даних, або в структурному підрозділі володільців;
- 5) датою надання права доступу працівнику володільців до персональних даних вважається дата надання зобов'язання відповідним працівником;
- 6) датою позбавлення права доступу до персональних даних вважається дата звільнення працівника володільців, дата переведення на посаду, виконання обов'язків на якій не пов'язане з обробкою персональних даних, або дата, коли фізична особа перестає бути пацієнтом у правовому розумінні (ст. 3 Основ) для працівника володільця;
- 7) володільці зобов'язані вжити заходів щодо унеможливлення доступу працівника, який звільнився чи перевівся на іншу посаду, що не передбачає роботу з персональними даними суб'єктів (зокрема пацієнтів) до персональних даних, а документи та інші носії, що містять персональні дані суб'єктів, передаються іншому працівнику володільців.

6. Володільцям треба пам'ятати, що пацієнт як суб'єкт персональних даних чи його/її законний представник мають право пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних, якщо ці дані обробляються незаконно чи є недостовірними (п. 6 ч. 8 Закону України «Про захист персональних даних»). Право суб'єкта персональних даних на одержання будь-яких відомостей про себе, а також зміни їх на підставі вмотивованої вимоги, відповідно до Закону України «Про захист персональних даних», не може бути обмежене (п. 29 Порядку функціонування електронної системи охорони здоров'я, затвердженого постановою КМУ від 25.04.2018 № 411).

Типове порушення: відсутні документи, які регулюють процеси, пов'язані з обробкою та захистом персональних даних.

Національне законодавство й акти автентичного тлумачення

У ч. 2 ст. 9 Закону України «Про захист персональних даних» закріплено, що повідомлення про обробку персональних даних подається за формою та в порядку, визначених Уповноваженим. У ч. 1 ст. 21 цього ж Закону зазначено, що про передачу персональних даних третій особі володілець персональних даних протягом десяти робочих днів повідомляє суб'єкта персональних даних, якщо цього вимагають умови його згоди або інше не передбачено законом⁸⁷.

У ст. 24-1 Основ закріплено, що доступ до відомостей про пацієнта, які містяться в електронній системі охорони здоров'я, можливий лише у разі отримання згоди такого пацієнта (його законного представника) у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди⁸⁸.

У Типовому порядку обробки персональних даних міститься низка нормативних вимог:

- у п. 1.2. Володільці, розпорядники персональних даних самостійно визначають порядок обробки персональних даних, враховуючи специфіку обробки персональних даних у різних сферах, відповідно до вимог, визначених Законом України «Про захист персональних даних» та цим Порядком.
- у п. 2.9. Володілець зберігає інформацію (документи), які підтверджують надання заявнику вищезазначеної інформації протягом усього періоду обробки персональних даних [стосується повідомлення про обробку даних. — І. С.].
- у п. 3.4. Організаційні заходи охоплюють:
 - ▶ визначення порядку доступу до персональних даних працівників володільця/розпорядника;
 - ▶ визначення порядку ведення обліку операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них;
 - ▶ розробку плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій;
 - ▶ регулярне навчання співробітників, які працюють з персональними даними.
- у п. 3.5. Володілець/розпорядник веде облік працівників, які мають доступ до персональних даних суб'єктів.
- у п. 3.7. Працівники, які мають доступ до персональних даних, дають письмове зобов'язання про нерозголошення персональних даних, які їм було довірено або які стали їм відомі у зв'язку з виконанням професійних чи службових або трудових обов'язків.
- у п. 3.11. Володілець/розпорядник персональних даних самостійно визначає процедуру збереження інформації про операції, пов'язані з обробкою персональних даних суб'єкта та доступом до них. У випадку обробки персональних даних суб'єктів за допомогою автоматизованої системи така система автоматично фіксує вказану інформацію. Ця інформація зберігається володільцем/розпорядником упродовж одного року з моменту закінчення

87. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI.

URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

88. Основи законодавства України про охорону здоров'я : Закон України від 19.11.1992 № 2801-XII.

URL: <https://zakon.rada.gov.ua/laws/show/2801-12#Text>

року, у якому було здійснено зазначені операції, якщо інше не передбачено законодавством України.

- у п. 3.14. З метою забезпечення безпеки обробки персональних даних вживаються спеціальні технічні заходи захисту, у тому числі щодо виключення несанкціонованого доступу до персональних даних, що обробляються, та роботи технічного і програмного комплексу, за допомогою якого здійснюється обробка персональних даних.
- у п. 3.15. В органах державної влади, органах місцевого самоврядування, а також у володільців чи розпорядників персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до Закону, створюється (визначається) структурний підрозділ або відповідальна особа, яка організовує роботу, пов'язану із захистом персональних даних при їх обробці⁸⁹.

У Роз'ясненнях Уповноваженого Верховної Ради України з прав людини основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, від 08.01.2014 зазначено, що володілець самостійно визначає, які заходи безпеки запроваджувати з метою адекватного захисту персональних даних, які ним обробляються. Запроваджені ним заходи вказуються у заяві.

Варто наголосити, що виклад зазначеної інформації у заяві довільний і володілець повинен надати лише загальні відомості. Приклад викладу цієї інформації:

Володільцем прийнято внутрішній порядок обробки персональних даних і визначено відповідальну особу. Приміщення, де знаходяться комп'ютери, на яких здійснюється обробка персональних даних, замикаються. Для отримання ключа необхідно поставити відмітку в журналі. Визначені коло працівників, які мають доступ до персональних даних, а також рівні доступу таких працівників. Комп'ютери, де містяться персональні дані, захищені паролем. Кожен працівник має особистий пароль. Усі операції, пов'язані з обробкою персональних даних, автоматично фіксуються за допомогою спеціального програмного забезпечення⁹⁰.

Рекомендації

1. Заклад охорони здоров'я чи ФОП, яка має ліцензію на провадження господарської діяльності з медичної практики, зобов'язані розробити й затвердити порядок обробки (у тому числі захисту) персональних даних (приміром, положення про порядок обробки персональних даних).
2. Обов'язково треба прописати порядок дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій або в окремому документі, позначивши його як План дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій, або як додаток до локального порядку обробки персональних даних. План дій повинен бути затверджений розпорядчим актом.
3. Підготувати та затвердити зобов'язання про нерозголошення персональних даних. Таке зобов'язання може бути додатком до локального порядку обробки персональних даних. Окрім

89. Типовий порядок обробки персональних даних : Наказ Уповноваженого ВРУ з прав людини від 08.01.2014 № 1-02/14. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#n215

90. Роз'яснення Уповноваженого Верховної Ради України з прав людини основних положень Порядку повідомлення Уповноваженого щодо визначення обробки персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних, від 08.01.2014. URL: <https://zakon.rada.gov.ua/laws/show/n0003715-14#Text>

того, доречно вести Журнал реєстрації зобов'язань про нерозголошення персональних даних, що забезпечить ведення обліку працівників, які мають доступ до персональних даних суб'єктів. У Журналі належить відобразити: 1) ПІБ працівника; 2) структурний підрозділ, посаду; 3) дату надання зобов'язання; 4) перелік персональних даних, до яких є доступ; 5) форму обробки даних; 6) дату позбавлення доступу до персональних даних і їх обробки; 7) причину позбавлення доступу.

4. Заклад охорони здоров'я чи ФОП, яка має ліцензію на провадження господарської діяльності з медичної практики, зобов'язані вести облік операцій, пов'язаних з обробкою персональних даних суб'єкта та доступом до них. Приміром, інструментом обліку операцій при розгляді запитів щодо доступу до персональних даних може бути Журнал обліку операцій, пов'язаних з обробкою персональних даних при розгляді запитів. Складовими якого мали б бути: 1) отриманні запити щодо доступу до персональних даних з відображенням вхідних даних; 2) відповіді на запити (у тому числі відмова в наданні інформації) з відображенням вихідних даних; 3) ПІБ виконавця підготовки відповіді на запит; 4) відомості про інформування суб'єкта персональним даних про передачу його персональних даних третій особі; 5) відображення інформації про несанкціонований доступ до персональних даних при розгляді запитів.

5. Заклад охорони здоров'я чи ФОП, яка має ліцензію на провадження господарської діяльності з медичної практики, зобов'язані розпорядчими документами призначити відповідальну особу, яка організовує роботу, пов'язану із захистом персональних даних при їх обробці або створити структурний підрозділ, відповідальний за обробку персональних даних. У разі призначення відповідальної особи треба: 1) або запровадити окрему посаду та підготувати посадову інструкцію відповідального за обробку персональних даних; 2) або до посадових обов'язків певного працівника долучити додаткові обов'язки та права, пов'язані з обробкою персональних даних, з обов'язковим закріпленням у посадовій інструкції. У разі формування структурного підрозділу треба підготувати положення про такий підрозділ з відображенням його статусу.

6. Заклад охорони здоров'я чи ФОП, яка має ліцензію на провадження господарської діяльності з медичної практики, зобов'язані зберігати копії заяв, що були подані до Секретаріату Уповноваженого з прав людини, пов'язані з обов'язковим повідомленням Уповноваженого з прав людини про обробку персональних даних, які становлять особливий ризик для прав і свобод суб'єктів персональних даних.

7. У ч. 1 ст. 21 Закону України «Про захист персональних даних» не закріплено обов'язкової письмової форми повідомлення суб'єкта персональних даних про передачу персональних даних третій особі. Тому заклад охорони здоров'я чи ФОП, яка має ліцензію на провадження господарської діяльності з медичної практики, можуть використовувати такі варіанти: 1) розробити окрему письмову форму повідомлення пацієнта/законних представників пацієнта про передачу даних суб'єкта персональних даних третім особам (приміром, адвокату пацієнта) і відобразити здійснення такого повідомлення у Журналі обліку операцій, пов'язаних з обробкою персональних даних; або 2) обрати альтернативну форму повідомлення пацієнта/законних представників пацієнта про передачу даних, зокрема усну, і зазначити лише про здійснення такого повідомлення в Журналі обліку операцій, пов'язаних з обробкою персональних даних.

Треба пам'ятати, що існують законодавчі винятки щодо повідомлення, зумовлені суб'єктним складом третіх осіб. Повідомлення не здійснюється у разі: 1) передачі персональних даних за запитами при виконанні завдань оперативно-розшукової чи контррозвідувальної діяльності, боротьби з тероризмом; 2) виконання органами державної влади та органами місцевого самоврядування своїх повноважень, передбачених законом; 3) здійснення обробки персональних даних в історичних, статистичних чи наукових цілях.

Міжнародні та регіональні документи щодо захисту персональних даних і прав людини

Загальна декларація прав людини. Резолюція 217 А (III), прийнята Генеральною Асамблеєю ООН 10.12.1948

Стаття 3. Кожна людина має право на життя, на свободу і на особисту недоторканність.



Міжнародний пакт про громадянські і політичні права 16.12.1966

Стаття 17. Ніхто не повинен зазнавати свавільного чи незаконного втручання в його особисте і сімейне життя, свавільних чи незаконних посягань на недоторканність його житла або таємницю його кореспонденції чи незаконних посягань на його честь і репутацію.



Загальний коментар № 14 до Міжнародного пакту про економічні, соціальні і культурні права 16.12.1966

Стаття 12. Доступність інформації не повинна завдавати шкоди праву на конфіденційність особистих медичних даних.



Конвенція ООН про права дитини, прийнята Генеральною Асамблеєю ООН 20.11.1989

Стаття 16. Жодна дитина не може бути об'єктом свавільного або незаконного втручання в здійснення її права на особисте і сімейне життя, недоторканність житла, таємницю кореспонденції або незаконного посягання на її честь і гідність.



Частина 2 статті 24. Держави-учасниці домагаються повного здійснення цього права, зокрема, вживають заходів щодо: забезпечення інформацією всіх прошарків суспільства, зокрема батьків і дітей, щодо здоров'я і харчування дітей, переваги грудного годування, гігієни, санітарії середовища перебування дитини і запобігання нещасним випадкам, а також доступу до освіти та підтримки у використанні цих знань.

Загальна декларація про біоетику та права людини, прийнята Генеральною конференцією ЮНЕСКО 19.10.2005

Стаття 9. Необхідно дотримуватися недоторканності приватного життя відповідних осіб і конфіденційності інформації, що стосується їх особисто. Максимально можливою мірою таку інформацію не треба використовувати або розголошувати, окрім як для цілей, для яких вона була зібрана або щодо яких давалась згода, відповідно до міжнародного права, зокрема, міжнародних норм у галузі прав людини.



Конвенція про захист прав людини і основоположних свобод 04.11.1950

Стаття 8. Кожен має право на повагу до свого приватного і сімейного життя.



Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних 28.01.1981

Стаття 1. Метою цієї Конвенції є забезпечення на території кожної Сторони для кожної особи, незалежно від її громадянства або місця проживання, дотримання її прав й основоположних свобод, зокрема її права на недоторканність приватного життя, у зв'язку з автоматизованою обробкою персональних даних, що її стосуються.



Конвенція про захист прав і гідності людини щодо застосування біології та медицини: Конвенція про права людини та біомедицину 04.04.1997

Стаття 10. Кожна особа має право на повагу до її особистого життя стосовно інформації про її здоров'я.

Кожна особа має право на ознайомлення з будь-якою зібраною про її здоров'я інформацією. Однак бажання осіб не отримувати такої інформації має також поважатися.

У виняткових випадках в інтересах пацієнта здійснення викладених у пункті 2 прав може обмежуватися законом.



Рекомендації Комітету міністрів Ради Європи R (97)5 щодо захисту медичних даних 13.02.1997

3.1. Під час збору та обробки медичних даних гарантується повага прав і основних свобод та, зокрема, недоторканність приватного життя.

3.2. Медичні дані можуть бути зібрані та оброблені відповідно до певних гарантій, які забезпечуються національним законодавством.

У принципі медичні дані мають збиратися та оброблятися лише медичними працівниками, особами або органами, які працюють від імені медичних фахівців. Особи або органи, які працюють від імені медичних фахівців,



які збирають та обробляють медичні дані, повинні дотримуватися тих самих принципів конфіденційності або аналогічних положень про конфіденційність, що й медичні фахівці.

Особа, що контролює файли, яка не є медичним працівником, повинна збирати та обробляти медичні дані лише відповідно до положень про конфіденційність, аналогічних принципів, покладених на медичного фахівця, або відповідно до гарантій, передбачених національним законодавством, які мають таку саму силу.

Рекомендації Комітету міністрів РЄ країнам-членам стосовно управління безпекою пацієнтів і запобігання небажаним явищам у сфері охорони здоров'я (2006)

1. Звітування та збір даних про безпеку пацієнтів є значущими, лише якщо ці дані належним чином проаналізувати й передати зворотну інформацію, якщо це доцільно, назад медичним працівникам, менеджерам і пацієнтам.
2. Процедура аналізу основних причин — це систематичний і загальний спосіб збору та аналізу даних, що йдуть слідом за інцидентом про безпеку пацієнтів. Цим процес розслідування не завершується. Сюди також входять розробка, реалізація, оцінка та контроль за удосконаленими системами безпеки.
3. Щодо способу використання зібраних даних — то тут повинно бути чітке розуміння та згода медичних установ і працівників.
4. Збір і використання даних також повинні узгоджуватися з вітчизняним та європейським законодавством про захист даних.

Регламент Європейського парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС 27.04.2016

Стаття 35. Персональні дані стосовно стану здоров'я повинні містити всі дані, що пов'язані зі станом здоров'я суб'єкта даних і розкривають інформацію про минулий, поточний або майбутній стан фізичного або психічного здоров'я суб'єкта даних. Це включає інформацію про фізичну особу, зібрану під час реєстрації на надання послуг, або надання послуг у сфері охорони здоров'я, як вказано у Директиві Європейського Парламенту і Ради 2011/24/ЄС, такий фізичній особі; номер, символічний знак або опис, який приписують фізичній особі для того, щоб однозначно ідентифікувати фізичну особу для цілей охорони здоров'я; інформацію, отриману внаслідок дослідження або огляду частини тіла чи речовини, що міститься в тілі, у тому числі з генетичних даних або біологічних проб; а також будь-яку інформацію, наприклад, про захворювання, недієздатність, ризик захворювання, історію хвороби, клінічне лікування або фізіологічний чи біомедичний стан здоров'я суб'єкта даних, незалежно від джерела її надходження, наприклад, від лікаря або іншого медичного працівника, від лікарні, медичного обладнання або тестів лабораторної діагностики.



Декларація про політику у сфері дотримання прав пацієнта в Європі, прийнята на Європейській консультативній нараді ВООЗ 28.06.1994



Стаття. 4. Уся інформація про стан здоров'я пацієнта, діагноз, прогноз і лікування його захворювання, а також будь-яка інша інформація особистого характеру повинна зберігатися в таємниці, навіть після смерті пацієнта.

Конфіденційну інформацію можна розкрити лише за згодою пацієнта або у передбачених законом випадках. Пацієнт має надати згоду на розкриття конфіденційної інформації про нього медичним працівникам, які беруть участь у його лікуванні.

Персональні дані пацієнта мають бути захищені. Ступінь захисту повинен бути адекватний формі зберігання даних. Частина людського тіла, з яких можна отримати ідентифікаційну інформацію, також повинні зберігатися з дотримання вимог захисту.

Пацієнти мають право доступу до історії хвороби, а також до всіх матеріалів, що мають відношення до діагнозу та лікування. Пацієнт має право отримати копії цих документів. Однак дані, що стосуються третіх осіб, не повинні стати доступними для пацієнта.

Пацієнт має право вимагати корекції, доповнення, уточнення та/або виключення даних особистого та медичного характеру, якщо вони неточні, неповні або не мають відношення до обґрунтування діагнозу та проведення лікування.

Забороняється будь-яке втручання в особисте та сімейне життя пацієнта за винятком тих випадків, коли пацієнт не заперечує проти цього та така інформація є необхідною для діагностики та лікування.

У будь-якому випадку втручання в особисте життя пацієнта безумовно передбачає повагу до його таємниць. Тому таке втручання може здійснюватися лише у присутності чітко визначених осіб, якщо іншого не забажає сам пацієнт.

Лісабонська декларація прав пацієнта, прийнята 34-ю Всесвітньою медичною асамблеєю 01.10.1981



Стаття 8:

а) вся інформація, яка ідентифікується щодо стану здоров'я пацієнта, захворювання, діагнозу, прогнозу й лікування, а також будь-яка інша особиста інформація вважається конфіденційною навіть після смерті пацієнта. У надзвичайних випадках родичі за низхідною лінією можуть отримати право доступу до інформації, яка стосується ризику спадкових захворювань;

б) конфіденційна інформація може розголошуватися тільки в тому разі, якщо пацієнт надасть безпосередню згоду чи таке розголошення прямо передбачене законом. Інформацію можуть повідомляти іншим особам, які надають медичну допомогу, винятково в разі необхідності, якщо пацієнт явно не дав прямої згоди на розкриття відомостей;

с) усі ідентифікаційні відомості про пацієнта повинні зберігатися. Захист даних здійснюється відповідно до порядку їх зберігання. Аналогічно належать захисту субстанції людського організму, які можуть бути джерелом ідентифікаційних відомостей.

Міжнародний кодекс медичної етики 01.10.1949

Лікар повинен тримати в таємниці все, що він знає про свого пацієнта, навіть після його смерті.



Європейська хартія прав пацієнтів, прийнята Активною громадською мережею у співпраці з громадськими організаціями з 12 різних країн ЄС 15.11.2002

Стаття 6. Кожна особа має право на конфіденційність особистої інформації, включаючи інформацію про стан здоров'я, медичний огляд чи обстеження, їх результати, інтимну і сімейну сторони життя, а також право на захист приватності під час проходження діагностичних, лікувальних чи реабілітаційних процедур.



Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони (рат. 16.09.2014)

Стаття 15. Сторони домовились співробітничати з метою забезпечення належного рівня захисту персональних даних відповідно до найвищих європейських і міжнародних стандартів, зокрема відповідних документів Ради Європи. Співробітництво у сфері захисту персональних даних може включати, *inter alia*, обмін інформацією та експертами.



ПЛАН ДІЙ

на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій

№ з/п	Подія/загроза	Дії працівників	Відповідальні особи/ підрозділи
1.	<p>Несанкціонований доступ (НСД) до інформації:</p> <ul style="list-style-type: none"> ▶ шляхом несанкціонованого отримання логінів і паролів доступу; ▶ шляхом підбору паролів і ключів доступу; ▶ унаслідок недбалості користувача 	<ul style="list-style-type: none"> ▶ негайно припинити обробку; ▶ відключити комп'ютер від мережі Інтернет; ▶ змінити паролі доступу; ▶ розпоряднику системи або технічному адміністратору системи ▶ заблокувати доступи до облікового запису; ▶ поінформувати керівництво та особу, відповідальну за обробку персональних даних (або керівника структурного підрозділу, відповідального за обробку персональних даних) 	<ul style="list-style-type: none"> ▶ керівник володільця; ▶ керівники структурних підрозділів; ▶ відповідальна особа за обробку персональних даних (або керівник структурного підрозділу, відповідального за обробку персональних даних); ▶ розпорядник або технічний адміністратор системи
2.	<p>Ненавмисне зараження програмного забезпечення та носіїв інформації комп'ютерними вірусами</p>	<ul style="list-style-type: none"> ▶ негайно припинити обробку персональних даних; ▶ повідомити МОЗ; ▶ відключити комп'ютер від мережі Інтернет та IT-мережі суб'єкта господарювання; ▶ поінформувати керівництво та особу, відповідальну за обробку персональних даних (або керівника структурного підрозділу, відповідального за обробку персональних даних) 	<ul style="list-style-type: none"> ▶ керівник володільця; ▶ керівники структурних підрозділів; ▶ відповідальна особа за обробку персональних даних персональних даних (або керівник структурного підрозділу, відповідального за обробку персональних даних); ▶ розпорядник або технічний адміністратор системи

3.	Відмова та/або збій у роботі програмного забезпечення	<ul style="list-style-type: none"> ▶ повідомити МОЗ; ▶ поінформувати керівництво та особу, відповідальну за обробку персональних даних (або керівника структурного підрозділу, відповідального за обробку персональних даних) 	<ul style="list-style-type: none"> ▶ керівник володільця; ▶ керівники структурних підрозділів; ▶ відповідальна особа за обробку персональних даних (або керівник структурного підрозділу, відповідального за обробку персональних даних); ▶ розпорядник або технічний адміністратор системи
4.	Відмова та/або збій у читанні носіїв інформації	<ul style="list-style-type: none"> ▶ поінформувати керівництво та особу, відповідальну за обробку персональних даних (або керівника структурного підрозділу, відповідального за обробку персональних даних); ▶ вжити заходів щодо ▶ відновлення роботи носіїв інформації 	<ul style="list-style-type: none"> ▶ керівник володільця; ▶ керівники структурних підрозділів; ▶ відповідальна особа за обробку персональних даних (або керівник структурного підрозділу, відповідального за обробку персональних даних); ▶ розпорядник або технічний адміністратор системи
5.	Відмова та/або збій систем забезпечення нормальних умов роботи (електроживлення, охолодження, вентиляції тощо)	<ul style="list-style-type: none"> ▶ поінформувати керівництво та відповідальну особу за обробку персональних даних (або керівника структурного підрозділу, відповідального за обробку персональних даних); ▶ вжити заходів щодо ▶ відновлення роботи носіїв інформації 	<ul style="list-style-type: none"> ▶ керівник володільця; ▶ керівники структурних підрозділів; ▶ відповідальна особа за обробку персональних даних (або керівник структурного підрозділу, відповідального за обробку персональних даних); ▶ розпорядник або технічний адміністратор системи

6.	Випадкові та/або помилкові дії, що можуть призвести до втрати, зміни, поширення, розголошення персональних даних	<ul style="list-style-type: none"> ▶ негайно припинити обробку ▶ персональних даних і про всі події та факти ▶ поінформувати керівництво та особу, відповідальну за обробку персональних даних (або керівника структурного підрозділу, відповідального за обробку персональних даних) 	<ul style="list-style-type: none"> ▶ керівник володільця; ▶ керівники структурних підрозділів; ▶ відповідальна особа за обробку персональних даних (або керівник структурного підрозділу, відповідального за обробку персональних даних); ▶ розпорядник або технічний адміністратор системи
7.	Аварія систем життєзабезпечення (опалення, водопостачання, каналізації тощо)	<ul style="list-style-type: none"> ▶ відключити електроживлення; ▶ вжити заходів щодо збереження електронних і паперових носіїв персональних даних; ▶ поінформувати керівництво та особу, відповідальну за обробку персональних даних (або керівника структурного підрозділу, відповідального за обробку персональних даних) 	<ul style="list-style-type: none"> ▶ керівник володільця; ▶ керівники структурних підрозділів; ▶ відповідальна особа за обробку персональних даних (або керівник структурного підрозділу, відповідального за обробку персональних даних); ▶ розпорядник або технічний адміністратор системи

ЗОБОВ'ЯЗАННЯ ПРО НЕРОЗГОЛОШЕННЯ ПЕРСОНАЛЬНИХ ДАНИХ

Я, _____ (ПІБ працівника), зобов'язуюсь не розголошувати персональні дані, зокрема, про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя пацієнта (пацієнтки), а, в разі необхідності, законного представника і членів його/її сім'ї, які мені будуть довірені або які мені стануть відомі у зв'язку з виконанням професійних або службових обов'язків.

« _____ » _____ 20____ р.

_____ (підпис)

_____ (прізвище й ініціали)

ПОВІДОМЛЕННЯ ПРО ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ ПАЦІЄНТІВ

Шановний пацієнте!

На підставі п. 6 ч. 2 ст. 7 Закону України «Про захист персональних даних» _____ (найменування закладу охорони здоров'я чи ФОП, яка має ліцензію на провадження господарської діяльності з медичної практики) (далі — Медичний центр) здійснює обробку Ваших персональних даних у цілях охорони здоров'я для встановлення медичного діагнозу, для забезпечення піклування чи лікування, надання медичних послуг або функціонування електронної системи охорони здоров'я.

Персональними даними, які збирає Медичний центр, є як загальні дані (зокрема, прізвище, ім'я, по батькові, стать, дата народження), так і спеціальні (медичні дані та дані немедичного характеру). До спеціальних належать: 1) медична інформація; 2) генетичні дані; 3) дані, тісно пов'язані з наданням медичної допомоги (статеве життя, біометричні дані); 4) дані, тісно пов'язані з приватним і сімейним життям.

Згідно зі ст. 8 Закону України «Про захист персональних даних», Ви маєте такі права:

- 1) знати про джерела збирання, місцезнаходження своїх персональних даних, мету їх обробки, місцезнаходження або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;
- 2) отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються Ваші персональні дані;
- 3) на доступ до своїх персональних даних;
- 4) отримувати не пізніше як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь, чи обробляються Ваші персональні дані, а також отримувати зміст таких персональних даних;
- 5) пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних;
- 6) пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем і розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;
- 7) на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять Вашу честь, гідність і ділову репутацію;

- 8) звертатися із скаргами на обробку своїх персональних даних до Уповноваженого або до суду;
- 9) застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;
- 10) вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;
- 11) відкликати згоду на обробку персональних даних;
- 12) знати механізм автоматичної обробки персональних даних;
- 13) на захист від автоматизованого рішення, яке має для нього правові наслідки.

Про передачу персональних даних третій особі Медичний центр повідомить Вас протягом десяти робочих днів, окрім випадків, передбачених ст. 21 Закону України «Про захист персональних даних», яка визначає умови передачі персональних даних.

Поширення персональних даних, що обробляються, без Вашої згоди дозволяється у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини.

Дата _____

Інформацію отримав _____
(ПІБ пацієнта/його (її) законного представника та його/її підпис)

Інформацію надав _____
(ПІБ відповідальної особи медичного центру та її підпис).

**У разі, якщо пацієнт не досягнув віку, з якого він/вона компетентний реалізовувати своє право на інформацію про стан свого здоров'я, тобто повноліття, повідомляти треба законного представника. У законодавчо встановлених випадках, коли право на інформацію про стан свого здоров'я реалізується пацієнтом з 14 років, до 14 років повідомляти треба законних представників, а з 14 років — самого пацієнта.*

Аналітичне дослідження щодо обробки персональних даних у сфері охорони здоров'я та дотримання прав людини у цій царині — актуальна та водночас уразлива тема з огляду на цифровізацію і чутливість інформації. Попри те що законодавство України містить численні гарантії, виснувано правові позиції судових інстанцій, дотримання яких забезпечують численні державні інституції, права людини все ж зазнають утисків в одній із найсенсетивніших сфер. Метою дослідження є виявлення найбільш частих порушень прав людини в окресленій царині та вироблення рекомендацій надавачам медичних послуг і їхнім працівникам для недопущення і профілактики порушень прав людини при обробці персональних даних у сфері охорони здоров'я.

Викладені у розділі 1 загальні рекомендації органам державної влади, зокрема Уповноваженому Верховної Ради України з прав людини, спрямовані на дотримання прав людини при обробці персональних даних у сфері охорони здоров'я: від сприяння національним нормативним змінам до розробки рекомендацій щодо обробки персональних даних у сфері охорони здоров'я. Урахування рекомендацій сприятиме удосконаленню законодавства у царинах охорони здоров'я й обробки персональних даних, а також оптимізації правореалізації і правозастосування у цих сферах.

У розділі 2 проаналізовано низку типових порушень, серед яких: 1) ненадання медичної інформації та копій медичної документації пацієнтові або законному представнику пацієнта; 2) неповідомлення Уповноваженого з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб'єктів персональних даних; 3) безпідставне відбирання суб'єктами обробки даних згоди про обробку персональних даних від пацієнтів при наданні медичної допомоги; 4) безпідставне відбирання суб'єктами обробки персональних даних згоди про обробку персональних даних від своїх працівників; 5) обробка даних при контролі якості медичної допомоги без згоди суб'єкта персональних даних; 6) ненадання медичної інформації та копій медичної документації членам сім'ї померлого пацієнта; 7) незаконне розголошення лікарської таємниці; 8) недотримання правил обробки даних при функціонування електронної системи охорони здоров'я; 9) відсутність документів, які регулюють процеси, пов'язані з обробкою та захистом персональних даних. Кожне типове порушення опрацьовано за такою схемою: 1) окреслено національне законодавство та акти автентичного тлумачення; 2) наведено приклади з практики національних судів; 3) висвітлено практику Європейського суду з прав людини; 4) сформульовано рекомендації, які допоможуть уникнути типових порушень у майбутньому.

Окрім того, видання містить додатки, серед яких — перелік міжнародних і регіональних документів за тематикою дослідження, які стануть у нагоді при глибинному вивченні проблеми, а також проєкт плану дій на випадок несанкціонованого доступу до персональних даних, пошкодження технічного обладнання, виникнення надзвичайних ситуацій, що передбачений як вимога до розробки володільцями персональних даних.

Видання, зорієнтоване насамперед на суб'єктів господарювання, які провадять господарську діяльність з медичної практики, слугуватиме професійним порадином і дороговказом у разі виникнення типової проблемної ситуації, допоможе при взаємодії з пацієнтами/законними представниками та членами їхніх сімей уникнути конфліктів і забезпечити захист прав людини, оптимізувати роботу зі спектральними зверненнями, які надходять до володільців персональних даних. Дослідження також буде корисним усім, хто цікавиться проблематикою охорони здоров'я й обробки персональних даних — від представників органів влади до пацієнтів.

An analytical study on processing of personal data in the healthcare system and observance of human rights in this area covers essential and vulnerable at the same time topic given the digitalisation and sensitivity of information nowadays. Ukrainian legislation contains numerous guarantees, legal positions of the courts have been established, numerous state institutions are on guard however the judicial practice repletes with cases on infringement of human rights within the health care system.

The purpose of the study was to identify the most common human rights violations in this area and to develop recommendations for providers of the medical services and their employees in order to prevent violations connected with the processing of personal data in the healthcare system. Several typical violations have been analysed, including:

1) failure to provide medical information and copies of medical records to the patient or the patient's legal representative; 2) failure to notify the Commissioner for Human Rights about the processing of personal data that poses a particular risk to the rights of data subjects; 3) unreasonable withdrawal of the patients' consent to processing of personal data by data processors in the course of medical care provision; 4) unreasonable withdrawal of consent to processing of personal data by the data processors from their employees; 5) processing of data without the consent of the data subject in the course of quality control of the medical care; 6) failure to provide medical information and copies of medical records to family members of a deceased patient; 7) unlawful disclosure of medical secrecy; 8) non-compliance with the rules of data processing in the functioning of the electronic healthcare system; 9) lack of documents regulating processing and protection of personal data.

Each typical violation has been analysed according to the following algorithm: 1) national legislation and acts of authentic interpretation; 2) national judicial practice; 3) case law of the European Court of Human Rights; 4) recommendations on prevention of the typical violations in the future.

In addition, the general recommendations for public authorities, including for the Ukrainian Parliament Commissioner for Human Rights, has been set out in Section 1. They are focused on observance of human rights within processing of personal data in the healthcare system starting from amendment of the national legislation and finalising with the development of recommendations related to processing of personal data. Implementation of the given recommendations can bring to improvement of the national legislation in both fields — data protection and health care, as well as to optimise implementation and application of the legal norms in an efficient way.

The analytical study will serve as a professional guidebook that on the one hand contains compilation of the necessary thematically related materials, and on the other hand, provides for algorithms of actions if the typical problem occurs.

The analytical study is recommended for legal entities that provide medical services to prevent any conflict situations that might arise while interacting with patients/their legal representatives and family members, and to guarantee human rights observance. This analysis will help to optimise the work of personal data owners with the spectral requests and to ensure processing of personal data in line with the human rights standards. The analysis will be useful to those interested, both public authorities and patients, in the issue of personal data protection and data processing in the healthcare system.

In addition, the analytical study is supplemented with two annexes: the first one presents a list of international and regional standards related to the subject matter of the study and can be used for in-depth study on the issue; and the second one provides for a draft action plan the development of which is an obligatory requirement for the personal data owners and can be used in case of unauthorised access to personal data, damage of technical equipment or emergency situations.

Unconditional compliance by the personal data owners with the national legislation in force can be an effective contraction to human rights violations within processing of personal data in the healthcare system. The present study provides for better understanding of the regulatory requirements to processing of personal data in the healthcare system.

СЕНЮТА Ірина Ярославівна, доктор юридичних наук, професор, завідувачка катедри медичного права ФПДО Львівського національного медичного університету імені Данила Галицького, адвокатка, голова Комітету медичного і фармацевтичного права та біоетики Національної асоціації адвокатів України, членкиня правління Європейської асоціації медичного права, президентка ГО «Фундація медичного права та біоетики України».

UKR

www.coe.int

Рада Європи є провідною організацією із захисту прав людини на континенті. Вона нараховує 46 держав-членів, включно з усіма державами — членами Європейського Союзу. Усі держави — члени Ради Європи приєдналися до Європейської конвенції з прав людини — договору, спрямованому на захист прав людини, демократії та верховенства права. Європейський суд з прав людини здійснює нагляд за виконанням Конвенції у державах-членах.

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE