9. Полянський С. Ю. Правова доктрина як базисна концепція права: природа, структура, значення// Наукові праці НУ ОЮА. Т. 17. 2015. С. 297 – 313

УДК 342.721:614.253.84:004.056.5 DOI: 10.32751/2617-5967-2025-02-06

Пономарьова О.О.
кандидат юридичних наук, старший дослідник,
старший науковий співробітник відділу
дослідження прав інтелектуальної власності
та прав людини у сфері охорони здоров'я НДІ
інтелектуальної власності НАПрН України ORCID: 0000-0002-8232-3748

МЕДИЧНА КОНФІДЕНЦІЙНІСТЬ ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ПАЦІЄНТІВ

Стаття присвячена комплексному аналізу медичної конфіденційності як ключової передумови довіри до системи охорони здоров'я та ефективного захисту прав пацієнтів у добу цифровізації. Мета дослідження окреслити етичні, правові та технологічні засади збереження приватності медичних даних, із фокусом на медичні зображення та алгоритми штучного інтелекту. Методологія ґрунтується на міждисциплінарному підході: доктринальному аналізі норм права (права пацієнта на приватність, інформована згода, пропорційність доступу та метаобмеження обробки), порівняльно-правовому огляді сучасних стандартів і технічній оцінці ризиків (загрози для PACS/DICOM, вразливості ідентифікації та повторної ідентифікації зображень).

Отримані результати свідчать, що найвищі ризики виникають на стику клінічної практики та аналітики даних: секондари-використання знімків, тренування моделей ШІ без належної анонімізації, неузгоджені

політики доступу й зберігання, а також слабкий аудит та журналювання. Аргументовано, що інформована згода повинна поєднуватися з керованим доступом і принципами privacy by design: мінімізацією даних, псевдонімізацією/анонімізацією, шифруванням у стані спокою та під час передачі, багатофакторною автентифікацією, сегментацією мережі, безперервним моніторингом подій безпеки та періодичними оцінками впливу на захист даних. Окремо обґрунтовано баланс між потребами досліджень і національною безпекою: пропонується ризик-орієнтована модель доступу, що враховує контекст, мету обробки та відновлюваність ідентифікації, а також поетапні протоколи depersonalization для зображень.

Наукова новизна полягає у синтезі правових та технічних вимог у вигляді практичної «дорожньої карти» для закладів охорони здоров'я: політика життєвого циклу даних, класифікація чутливості знімків, обов'язкове журналювання, контроль ролей, перевірка сторонніх постачальників і прозорі процедури реалізації прав пацієнтів. Практична значущість полягає у тому, що запропонований набір організаційних і технічних заходів може бути негайно інтегрований у локальні політики безпеки, знижуючи імовірність витоків і правових санкцій та підтримуючи довіру пацієнтів.

Ключові слова: *медична конфіденційність, інформована згода, захист даних, медичні зображення, цифрова безпека, етичні виклики, юридична відповідальність, штучний інтелект.*

The article is devoted to a comprehensive analysis of medical confidentiality as a key precondition for trust in the healthcare system and for the effective protection of patients' rights in the digital age. The aim of the study is to outline the ethical, legal, and technological foundations for preserving the privacy of medical data, with a focus on medical imaging and artificial intelligence algorithms. The methodology relies on an interdisciplinary approach: doctrinal analysis of legal norms (the patient's right to privacy, informed consent, proportionality of access and purpose limitation), a comparative-legal review of current standards, and a

technical risk assessment (threats to PACS/DICOM, vulnerabilities of identification and re-identification of images).

The findings indicate that the highest risks arise at the intersection of clinical practice and data analytics: secondary use of images, training AI models without proper anonymization, inconsistent access and storage policies, and weak auditing and logging. It is argued that informed consent must be combined with controlled access and privacy-by-design principles: data minimization, pseudonymization/anonymization, encryption at rest and in transit, multi-factor authentication, network segmentation, continuous security event monitoring, and periodic data protection impact assessments. A separate discussion substantiates the balance between research needs and national security: a risk-oriented access model is proposed that takes into account context, purpose of processing, and the recoverability of identification, as well as phased de-identification ("depersonalization") protocols for images.

The scientific novelty lies in synthesizing legal and technical requirements into a practical "roadmap" for healthcare institutions: data life-cycle policy, sensitivity classification of images, mandatory logging, role-based control, third-party vendor due diligence, and transparent procedures for exercising patients' rights. The practical significance is that the proposed set of organizational and technical measures can be immediately integrated into local security policies, reducing the likelihood of data breaches and legal sanctions and sustaining patient trust.

Keywords: *medical confidentiality, informed consent, data protection, medical images, digital security, ethical challenges, legal responsibility, artificial intelligence.*

Вступ. Довіра до системи охорони здоров'я дедалі більше визначається тим, наскільки надійно медичні установи захищають конфіденційність даних. У цифровому середовищі медичні історії, зображення та потоки сенсорних вимірів постійно збираються, передаються і зберігаються в електронному вигляді, що збільшує площу атаки та підвищує імовірність несанкціонованого

доступу. Порушення приватності тепер тягне не лише психологічні та соціальні наслідки для пацієнта, а й юридичні та фінансові ризики для закладів, підриває готовність суспільства ділитися даними для лікування та досліджень і, зрештою, гальмує впровадження інновацій.

Окремого значення набувають медичні зображення: їхні великі обсяги, багаті метадані та складні ланцюги обробки роблять екосистеми PACS/DICOM чутливими до помилок конфігурації, слабких політик доступу і збоїв у ланцюгу постачання. Додаткова складність виникає на перетині візуальної діагностики з алгоритмами штучного інтелекту: моделі потребують даних для навчання та валідації, але саме ці етапи найвразливіші до повторної ідентифікації, витоку ознак і недокументованого вторинного використання.

Телемедицина, інтернет медичних речей і хмарні сервіси розширюють периметр обробки, залучаючи численних постачальників і інтеграції. Без чітких ролей, журналювання, шифрування «в дорозі» та «у спокої», а також сегментації мережі зростає системний ризик інцидентів. Паралельно посилюються вимоги нормативного поля: інформована згода, обмеження мети, пропорційність доступу, оцінки впливу на захист даних та реалізація прав суб’єктів мають бути трансформовані з декларацій у практичні політики та технічні контролі.

Етичний вимір виходить за межі підпису під формою згоди. Пацієнтам потрібні зрозумілі пояснення щодо використання їхніх даних, прозорий механізм відкликання згоди і гарантії недискримінації. Саме прозорість, керований доступ і можливість контролю для пацієнта формують соціальний мандат на використання медичних даних у наукових цілях та для покращення якості лікування.

З огляду на зростання кіберзагроз до медичної інфраструктури, інвестиції в безпеку — це не лише питання комплаєнсу, а й ключ до безперервності клінічних процесів та репутаційної стійкості. Водночас інновації не повинні зупинятися: безпечні середовища даних, поетапна деперсоналізація зображень, федеративне навчання та інші privacy-preserving підходи дозволяють поєднати потреби досліджень із вимогами захисту.

Таким чином, актуальність статті зумовлена необхідністю інтегрувати етичні, правові та інженерні підходи в єдину практичну «дорожню карту» для закладів охорони здоров'я. Поєднання принципів інформованої згоди, керованого доступу та privacy by design із конкретними технічними рішеннями — анонімізацією/псевдонімізацією, шифруванням, багатофакторною автентифікацією, сегментацією, аудитом і DPIA — створює реалістичну основу для зниження ризиків, підтримки інновацій та відновлення довіри пацієнтів до цифрової медицини.

Метою даної статті є комплексний аналіз проблематики медичної конфіденційності з акцентом на етичні, юридичні та технологічні аспекти. Серед основних завдань дослідження:

– визначити роль інформованої згоди в забезпеченні конфіденційності медичних даних;

– проаналізувати ризики несанкціонованого доступу до медичних зображень та їх вплив на приватність пацієнтів;

– розглянути вплив сучасних технологій, зокрема штучного інтелекту, на процес обробки медичних даних;

– сформулювати рекомендації для розробки правових рамок, які дозволять збалансувати інтереси національної безпеки і захисту персональної інформації.

Стан дослідження. За даними S.A. Tovino, МРТ-знімки, які є невід'ємною частиною нейровізуалізації, надають високоточну інформацію про мозкові структури, що дозволяє досягати значних діагностичних результатів, але також розкривають деталі мозкової активності, порушуючи питання конфіденційності [7]. Дослідження Cohen, J. та Ezer, T. демонструють, що захист прав пацієнтів у клінічних дослідженнях є базовою умовою дотримання прав людини в охороні здоров'я [3]. Робота Bobinski, M.A. підкреслює, що порушення конфіденційності можуть мати далекосяжні юридичні наслідки та серйозно впливати на автономію пацієнтів [2] Також дослідження Khang, A., Jadhav, B. та Sayyed, M. вказують на важливість використання передових технологій і алгоритмів глибокого навчання для

аналізу медичних даних, що супроводжується ризиками витоку конфіденційної інформації [4]. Додатково, дослідження Chandawarkar, R. та Nadkarni, P. звертає увагу на потребу у вдосконаленні стандартів безпеки при використанні медичної фотографії для зменшення ризиків витоку даних [5]. Таким чином, сучасна література свідчить про те, що хоча технологічні інновації відкривають нові можливості для діагностики та лікування, вони одночасно створюють додаткові загрози для приватності пацієнтів, що потребує інтегрованих підходів до захисту інформації.

Виклад основного матеріалу. Збереження конфіденційності медичних даних є наріжним каменем сучасної системи охорони здоров'я. Пацієнти повинні бути впевнені, що їхня особиста інформація не буде використана без їхньої згоди, адже довіра до медичних установ безпосередньо залежить від цього принципу. Як зазначає Allen, A.L., недовіра до системи охорони здоров'я може призвести до відмови пацієнтів від надання повної медичної історії, що негативно впливає на ефективність лікування [1]. У зв'язку з цим отримання інформованої згоди є критично важливим етичним та юридичним зобов'язанням, яке забезпечує захист прав пацієнтів.

Інформована згода полягає у наданні пацієнту повної інформації щодо мети, методів і можливих ризиків використання його медичних даних, що дозволяє йому самостійно приймати рішення щодо участі у клінічних дослідженнях або використання його даних для наукових цілей. Як підкреслюють Cohen, J. та Ezer, T., право на приватність є ключовим етичним принципом у медицині, який гарантує збереження гідності пацієнтів [3]. Водночас, Bobinski, M.A. зазначає, що недотримання цього принципу може призвести до юридичних позовів і руйнування репутації медичних установ, що підкреслює важливість належного отримання згоди [2]

Цифровізація охорони здоров'я призвела до масового впровадження електронних медичних записів, що суттєво полегшують обмін інформацією між медичними установами, але водночас створюють нові ризики витоку даних. Системи зберігання та обробки медичних зображень, такі як PACS і DICOM, стають об'єктами кібернападів. Експерти вказують на те, що

використання застарілих технологій шифрування, недостатня автентифікація та відсутність регулярного аудиту систем створюють значні вразливості. Як свідчить дослідження Graylight Imaging, впровадження сучасних багаторівневих заходів безпеки є необхідним для запобігання витоку конфіденційної інформації [5]. Постійний моніторинг та аудит дозволяють виявити потенційні загрози та оперативно реагувати на них, що є критично важливим в умовах стрімкого розвитку цифрових технологій.

Юридичний аспект захисту конфіденційності стає ще більш актуальним у зв'язку з розширенням повноважень правоохоронних органів у деяких країнах. Наприклад, у Сполучених Штатах Америки Закон «Патріот» надав правоохоронним органам розширені можливості для моніторингу електронних комунікацій, що, з одного боку, сприяє забезпеченню національної безпеки, а з іншого – створює передумови для порушення прав на приватність громадян. Як зазначають Khang, A., Jadhav, B. та Sayyed, M., сучасним державам необхідно розробляти універсальні правові рамки, які дозволять забезпечити захист медичних даних без шкоди для національної безпеки [4]. Такий баланс є надзвичайно важливим для підтримки довіри громадськості до державних інституцій і медичних установ.

Особливу увагу слід приділити проблемі захисту медичних зображень. Сучасні методи візуалізації, зокрема рентгенівські знімки, комп'ютерна томографія (КТ) та магнітно-резонансна томографія (МРТ), є незамінними для точного діагностування, проте вони містять величезну кількість чутливої інформації. На думку S.A. Tovino (2005), МРТ-знімки, що надають високоточну інформацію про мозкові структури, розкривають деталі мозкової активності, що може порушувати приватність пацієнтів [7]. Подібні проблеми спостерігаються і при використанні дерматологічних зображень, які, завдяки своїй візуальній привабливості, можуть бути використані не лише для медичних цілей, але й для збору генетичних даних або у судових розслідуваннях.

Недостатні заходи безпеки є однією з основних причин витоку медичних даних. Як зазначають Chandawarkar, R. та Nadkarni, P. (2021), зростаюча

кількість кібернападів на медичні установи свідчить про те, що без належного контролю доступу та сучасних технологій шифрування неможливо забезпечити високий рівень захисту інформації [5]. Витік даних може не лише підірвати довіру пацієнтів, але й стати причиною значних юридичних санкцій, що підкреслює необхідність постійного оновлення технологічних рішень.

Окрім технічних аспектів, важливо враховувати і соціально-правові питання. В умовах розширення повноважень державних органів щодо моніторингу комунікацій, питання конфіденційності стають надзвичайно актуальними. Законодавці повинні шукати компроміс між потребами забезпечення національної безпеки та правом громадян на приватність. Як зазначають Khang, A., Jadhav, B. та Sayyed, M., створення універсальних правових рамок, що регламентують використання медичних даних, є одним із головних завдань сучасної юриспруденції [4].

Важливою складовою системи захисту є забезпечення доступу до медичних даних лише для уповноважених осіб. Пацієнти повинні бути впевнені, що їхня інформація використовується виключно за їхньою згодою та відповідно до встановлених юридичних норм. Отримання інформованої та добровільної згоди є ключовим механізмом, який дозволяє знизити ризики витоку інформації. Bobinski, M.A. (2024) підкреслює, що інформована згода є наріжним каменем, завдяки якому пацієнти можуть зберігати свою автономію, а медичні установи – забезпечувати правовий захист своєї діяльності [2]

Застосування штучного інтелекту в аналізі медичних зображень відкриває нові можливості для покращення діагностики та планування лікування, проте одночасно породжує низку ризиків для приватності. Алгоритми ШІ потребують великих обсягів даних, що часто містять чутливу інформацію, тому забезпечення високих стандартів захисту та належних процедур анонімізації є критично важливим. Як зазначають дослідники Khang, A., Jadhav, B. та Sayyed, M. (2024), впровадження сучасних технологій безпеки разом із чіткими правовими регулюваннями дозволить зберегти конфіденційність даних при використанні штучного інтелекту [4].

Розвиток сучасних технологій охорони здоров’я створює

безпрецедентні можливості для порушення конфіденційності, адже детальна медична інформація може бути використана у зловмисних цілях. Водночас, впровадження сучасних методів кібербезпеки, розробка універсальних правових рамок та суворе дотримання етичних норм дозволяють знизити ризики витоку інформації та підтримувати довіру пацієнтів до системи охорони здоров'я. Інформована згода залишається наріжним каменем для забезпечення прав пацієнтів, а баланс між використанням даних для наукових досліджень і захистом приватності є однією з основних складових успішної медичної практики.

Сучасна охорона здоров'я повинна спиратися на інтеграцію нормативно-правових, етичних та технологічних підходів, що дозволить ефективно протидіяти новим викликам у сфері захисту медичних даних. Тільки комплексний підхід дозволяє створити систему, здатну оперативно реагувати на кіберзагрози та зберігати високу якість медичної допомоги. Подальші дослідження мають бути спрямовані на розробку ефективних правових та технологічних рішень, що забезпечать належний захист конфіденційності в умовах стрімкої цифровізації охорони здоров'я

Висновок. Підсумовуючи викладене, слід наголосити: медична конфіденційність є системоутворювальною умовою функціонування сучасної охорони здоров'я. Вона захищає автономію пацієнта, забезпечує дієвість інформованої згоди й підтримує гідність особи в ситуаціях, коли вразлива інформація неминуче циркулює між клініками, лабораторіями, страховими компаніями та дослідницькими центрами. Без стійких гарантій приватності зникає готовність пацієнтів довіряти дані навіть для очевидно корисних цілей, що прямо позначається на якості лікування, прогресі науки і суспільній підтримці цифрових інновацій.

Цифровізація медицини створює як потужні можливості, так і безпрецедентні ризики. Електронні медичні записи, складні обміни зображеннями у форматах PACS/DICOM, телемедицина, IoMT та алгоритмічна аналітика розширюють периметр обробки даних, збільшують кількість точок доступу і ускладнюють ланцюги постачання IT-послуг. У

таких умовах класичні декларації про «конфіденційність» уже недостатні: потрібне цілісне поєднання права, етики й інженерії у єдиній операційній моделі, що працює щодня — від робочого місця лікаря до хмарної інфраструктури.

Надійна правова рамка має переходити від формальних процедур до фактичної підзвітності. Це означає документовані ролі контролерів і процесорів, угоди про обробку даних зі сторонніми постачальниками, регулярні оцінки впливу на захист даних (DPIA), чіткі політики строків і цілей зберігання, а також дієві механізми реалізації прав суб'єктів даних — доступ, виправлення, обмеження обробки, відкликання згоди. Особливого значення набуває прозорість: пацієнт має розуміти, хто і з якою метою переглядає його дані, і як він може контролювати цей процес.

Технологічний контур повинен втілювати принципи privacy by design та security by default. Йдеться не лише про шифрування «в спокої» і «в дорозі» чи багатофакторну автентифікацію, а про повний цикл керування даними: мінімізацію збору, псевдонімізацію й анонімізацію з урахуванням ризику повторної ідентифікації, сегментацію мережі, захищене журналювання доступів, системний моніторинг подій безпеки, відстеження походження (provenance) зображень і захист цілісності діагностичного контенту. У сфері медичних зображень це доповнюється контрольованими середовищами обміну, валідацією метаданих та підтримкою відтворюваної трасованості, що зменшує як випадкові помилки, так і навмисні маніпуляції.

Етичний вимір вимагає переосмислення інформованої згоди. Статичні «разові» форми не встигають за динамікою повторних використань даних. Потрібні моделі зрозумілої, контекстної та, де це доречно, «динамічної» згоди, яка робить видимими реальні сценарії використання, ризики та вигоди. Турбота про вразливі групи і запобігання дискримінації мають бути не декларацією, а набором практик — від мінімізації наборів ознак у дослідженнях до незалежного етичного нагляду і регулярних перевірок справедливості алгоритмів.

Організаційна спроможність — ключ до стійкості. Політики залишаться

на папері без навчання персоналу, тестованих планів реагування на інциденти, чітких метрик (SLA з відновлення, MTTD/MTTR для кіберподій), регулярних аудитів і «червоних команд» для виявлення слабких місць. Управління ризиками ланцюга постачання передбачає відбір і сертифікацію підрядників, технічні вимоги до інтеграцій, перевірку географії зберігання та правового режиму транскордонних передач, а також узгоджені стандарти сертифікації інформаційної безпеки.

Штучний інтелект і наука про дані можуть розвиватися без підриву приватності за умови впровадження privacy-preserving підходів. Федеративне навчання, безпечна когортування й агрегація, диференційна приватність, апаратні довірені середовища виконання, синтетичні дані з контрольованою відновлюваністю ідентифікації — це вже не «екзотика», а практичний інструментарій, здатний збалансувати точність моделей і захист пацієнтів. Потрібні також узгоджені протоколи де-персоналізації саме для зображень, які враховують як зміст, так і метадані, що часто несуть ідентифікатори.

Важливо розуміти обмеження й зони невизначеності. Не існує абсолютної анонімізації для всіх сценаріїв; ризик повторної ідентифікації залежить від контексту, суміжних джерел і технічного прогресу. Тому управління ризиком має бути циклічним і доказовим: емпіричні дослідження ефективності методів знеособлення, регулярний перегляд політик з урахуванням нових загроз, пілотні впровадження з незалежною оцінкою, публікація агрегованих звітів прозорості для суспільства.

З практичної точки зору, запропонована в статті «дорожня карта» є інструментом негайної дії: класифікація чутливості зображень і пов’язаних метаданих, політика життєвого циклу даних, рольовий контроль доступу з принципом найменших привілеїв, обов’язкове журналювання і регулярний аналіз логів, технічні контролі для PACS/DICOM, процедура оцінки і відбору сторонніх постачальників, впровадження приватність-орієнтованих підходів у робочі процеси ШІ. Такі кроки зменшують імовірність інцидентів, пом’якшують їх наслідки і, що не менш важливо, відновлюють довіру пацієнтів.

Політичні та регуляторні наслідки також очевидні. Уніфікація вимог і міжвідомча координація, підтримка сертифікаційних програм, інвестування у кіберстійкість медичних закладів та в публічну просвіту з цифрової грамотності створюють умови, за яких приватність не конфліктує з інноваціями, а доповнює їх. Мета — не зупинити обіг даних, а зробити його керованим, передбачуваним і соціально прийнятним.

Отже, медична конфіденційність — не «гальмо прогресу», а його передумова. Інтеграція нормативно-правових, етичних і технологічних підходів формує практичну архітектуру довіри, у межах якої можлива одночасно висока якість медичної допомоги, швидка наукова еволюція та захист прав пацієнтів. Подальші дослідження мають зосередитися на вимірюванні реальних ризиків де-ідентифікації в медичних зображеннях, оптимізації приватність-зберігаючих методів для клінічних задач, розробці стандартів прозорості для алгоритмічних систем і створенні масштабованих, відтворюваних практик впровадження. Лише комплексний, доказовий і пацієнт-центричний підхід дозволить системі охорони здоров’я впевнено відповідати на нові кіберзагрози й водночас зберігати людяність медицини у добу стрімкої цифровізації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Allen, A.L. Privacy and Medicine URL: https://scholarship.law.upenn.edu/faculty_scholarship/3006/ (дата звернення: 1 лютого 2025).

2. Bobinski, M.A. Autonomy and Privacy: Protecting Patients from Their Physicians URL:University of Pittsburgh Law Review, 2024, Vol. 55, No. 2. – Доступно за посиланням: https://pubmed.ncbi.nlm.nih.gov/11659957/ (дата звернення: 1 лютого 2025).

3. Cohen, J., Ezer, T. Human Rights in Patient Care: A Theoretical and Practical Framework URL:Health and Human Rights, 2016, Vol. 15, No. 2. – Доступно за посиланням: https://pubmed.ncbi.nlm.nih.gov/24421170/ (дата звернення: 1 лютого 2025).

4. Khang, A., Jadhav, B., Sayyed, M. Role of Cutting-Edge Technologies and Deep Learning Frameworks in the Digital Healthcare Sector URL:Advances in Medical Diagnosis, Treatment, and Care (AMDTC) Book Series, 2024. – С. 1–22. – DOI: 10.4018/979-8-3693-3218-4.ch001.

5. Chandawarkar, R., Nadkarni, P. Safe Clinical Photography: Best Practice Guidelines for Risk Management and Mitigation URL:Archives of Plastic Surgery, 2021, Vol. 48, No. 3. – С. 295–304. – DOI: 10.5999/aps.2021.00262.

6. Pillai, A.S. Utilizing Deep Learning in Medical Image Analysis for Enhanced Diagnostic Accuracy and Patient Care: Challenges, Opportunities, and Ethical Implications URL:Journal of Deep Learning in Genomic Data Analysis, 2021, Vol. 1, No. 1. – С. 1–17.

7. Tovino, S.A. The Confidentiality and Privacy Implications of Functional Magnetic Resonance Imaging URL:Journal of Law, Medicine & Ethics, 2005, Vol. 33, No. 4. – С. 844–850. – DOI: 10.1111/j.1748-720x.2005.tb00550.x.