

DOI: 10.34015/2523-4552.2025.2.13
УДК 342.721:614.253.84:004.056.5

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
Національної академії наук України
ORCID: 0000-0002-8232-3748

АНАЛІЗ НОРМАТИВНОЇ БАЗИ НІРАА: ЕТИЧНІ ТА ЮРИДИЧНІ АСПЕКТИ КОНФІДЕНЦІЙНОСТІ ТА БЕЗПЕКИ МЕДИЧНОЇ ІНФОРМАЦІЇ У СУЧАСНІЙ ОХОРОНІ ЗДОРОВ'Я

У статті розглядаються нормативно-правові, етичні та практичні аспекти застосування Закону про переносимість та відповідальність страхування здоров'я 1996 року (НІРАА) у контексті сучасних інформаційних технологій охорони здоров'я. Дослідження аналізує основні положення НІРАА, проблематику конфіденційності, безпеки електронних медичних записів (EHR), етичні виклики, пов'язані із забезпеченням інформованої згоди, а також особливості роботи з мультимедійними даними у медичній практиці. Власний аналіз підкріплено даними з низки джерел [1–12]. Результати дослідження дозволяють окреслити перспективи розвитку нормативної бази та практичних заходів для забезпечення конфіденційності та безпеки пацієнтської інформації.

Однією з ключових тем є необхідність інтеграції вимог НІРАА з новітніми технологіями, які використовуються для обробки та зберігання медичних даних, зокрема в таких сферах, як радіологія та клінічна візуалізація. Серед етичних проблем виокремлюються питання, пов'язані з отриманням інформованої згоди пацієнтів, а також захистом їх приватності під час використання мультимедійних даних у медичній практиці.

Автор наголошує на важливості комплексного підходу до впровадження технологій безпеки, який включає не лише технічні, але й організаційні та етичні рішення. У статті наведені рекомендації щодо вдосконалення систем безпеки, підвищення рівня обізнаності медичних працівників і розробки політик для роботи з мультимедійними даними, що відповідають вимогам НІРАА. Зокрема, значну увагу приділено важливості навчання персоналу, розробці внутрішніх політик, що забезпечують захист конфіденційності, а також регулярному аудиту систем безпеки.

Результати дослідження свідчать про те, що ефективна реалізація вимог НІРАА вимагає постійного вдосконалення нормативно-правової бази та технологічних рішень. Перспективи розвитку цієї теми зумовлені необхідністю адаптації до новітніх технологічних змін, що виникають у сфері охорони

здоров'я, зокрема в контексті зростаючого використання штучного інтелекту та автоматизованих систем для забезпечення безпеки медичних даних.

Ключові слова: Відповідність HIPAA, безпека медичних даних, конфіденційність медичної інформації, електронні медичні картки (ЕМК), конфіденційність пацієнта, інформована згода, захист мультимедійних даних, кібербезпека в охороні здоров'я, етичні стандарти в охороні здоров'я, регулювання медичних даних.

Постановка проблеми. Сучасна охорона здоров'я характеризується стрімким впровадженням інформаційних технологій, що дозволяє ефективно зберігати, передавати та обробляти медичну інформацію. Проте з розвитком цифрових технологій зростає й ризик порушення конфіденційності та безпеки даних пацієнтів. Одним із основних нормативних актів, спрямованих на захист чутливої медичної інформації, є Закон про переносимість та відповідальність страхування здоров'я (HIPAA), прийнятий у 1996 році [1]. Водночас сучасна практика охорони здоров'я стикається із численними етичними викликами, зокрема щодо забезпечення інформованої згоди та конфіденційності, що вимагає комплексного підходу до вирішення проблем правового, технічного та етичного характеру.

Актуальність дослідження зумовлена необхідністю інтеграції нормативних положень HIPAA із сучасними технологічними рішеннями, зокрема електронними медичними записами (EHR) та мультимедійними даними, що використовуються для діагностики та лікування пацієнтів. «HIPAA встановлює національні стандарти для захисту конфіденційності та безпеки медичної інформації» [1], що підтверджує важливість аналізу його положень у сучасних умовах.

Аналіз останніх досліджень і публікацій. Для комплексного аналізу дослідження було використано публічно доступні джерела, які висвітлюють різноманітні аспекти застосування HIPAA у медичній практиці. До їх числа належать офіційні матеріали Центру з контролю та профілактики захворювань (CDC) [1], аналітичні статті з AINSP, що розглядають критичні питання інформованої згоди та етики охорони здоров'я [2, 4], а також матеріали, присвячені конфіденційності, безпеці електронних медичних записів та специфічним аспектам роботи з мультимедійними даними [3, 5–8, 10–12].

Методологічною основою дослідження є якісний аналіз нормативних документів, публікацій та аналітичних матеріалів з питань етики та безпеки інформації в охороні здоров'я. Особлива увага приділяється інтеграції даних з різних джерел з метою формування узагальненого бачення проблематики, а також аналізу практичних кейсів порушення HIPAA [12]. До того ж, дослідження здійснюється із застосуванням порівняльного аналізу підходів до забезпечення конфіденційності пацієнтської інформації у різних галузях медицини, зокрема в радіології [5] та роботі з клінічними зображеннями [9, 11].

Постановка завдання. Метою статті є аналіз та виявлення особли-

ностей нормативно-правових, етичних та практичних аспектів застосування Закону про переносимість та відповідальність страхування здоров'я 1996 року (HIPAA) у контексті сучасних інформаційних технологій охорони здоров'я.

Виклад основного матеріалу.

Основні положення HIPAA та їх вплив на охорону здоров'я.

HIPAA є комплексним нормативним актом, який спрямований на забезпечення захисту конфіденційності та безпеки медичної інформації. Основні положення HIPAA охоплюють стандарти для обробки, зберігання та передачі електронних медичних записів, а також встановлюють обов'язки для суб'єктів охорони здоров'я щодо захисту персональних даних. Як зазначено на офіційному сайті CDC, «HIPAA встановлює національні стандарти для захисту конфіденційності та безпеки медичної інформації» [1]. Ці положення є важливими з точки зору як юридичної відповідальності, так і етичних норм, що регулюють відносини між пацієнтом та медичним закладом.

Одним із ключових елементів HIPAA є зобов'язання суб'єктів охорони здоров'я впроваджувати ефективні заходи для захисту даних. Ці заходи охоплюють не лише технічні аспекти, такі як шифрування даних та контроль доступу, але й організаційні заходи, спрямовані на забезпечення відповідності нормативним вимогам. Наприклад, у матеріалі з Zenarmor зазначено, що «безпека електронних медичних записів (EHR) є критично важливою для запобігання несанкціонованому доступу до конфіденційної інформації» [7]. Такий підхід дозволяє не лише захистити дані, але й забезпе-

чити довіру пацієнтів до системи охорони здоров'я.

Етичні аспекти інформованої згоди та конфіденційності.

Однією з основних етичних проблем у сучасній охороні здоров'я є забезпечення інформованої згоди пацієнтів. За даними АІНСР, «інформована згода є ключовим етичним принципом, що забезпечує право пацієнтів на отримання повної інформації про методи лікування та можливі ризики» [2]. Водночас, інтеграція інноваційних технологій у медичну практику ставить нові виклики перед традиційними підходами до отримання згоди. У комплексному дослідженні, опублікованому АІНСР, наголошується, що «забезпечення інформованої згоди має враховувати не лише юридичні аспекти, але й морально-етичні вимоги сучасного суспільства» [4].

Етичний вимір забезпечення конфіденційності даних передбачає не лише захист інформації від несанкціонованого доступу, але й повагу до гідності та приватності пацієнта. Як підкреслено у публікації на сайті Standards of Care, «конфіденційність є одним із основних принципів надання якісної медичної допомоги» [3]. Таким чином, дотримання норм HIPAA тісно пов'язане з етичними стандартами, що регулюють відносини між медичними працівниками та пацієнтами.

Конфіденційність у сфері радіології та обробці клінічних зображень.

Особливу увагу до питань конфіденційності слід приділяти у галузі радіології, де пацієнтські дані використовуються для діагностики та лікування за допомогою високотехнологічних методів візуалізації.

Матеріал з RadiologyInfo підкреслює, що «захист конфіденційності пацієнтів є критично важливим у радіологічній практиці, оскільки передача зображень та інших медичних даних пов'язана з ризиком їх неправомірного використання» [5]. Проте, незважаючи на високі вимоги до захисту даних, випадки порушень конфіденційності не є рідкістю, що вимагає постійного вдосконалення систем безпеки.

Питання обробки клінічних зображень також викликає значний інтерес з точки зору етики. За даними Avant, «використання клінічних зображень для діагностики, навчання та досліджень вимагає ретельного дотримання принципів конфіденційності, оскільки навіть незначні порушення можуть призвести до розголошення особистої інформації пацієнтів» [9]. Додатково, статті з NetSec News та Compliance Home наголошують на необхідності впровадження строгих заходів щодо забезпечення безпеки при зберіганні та передачі фотографій, аудіо- та відеоматеріалів, пов'язаних з медичною документацією [10, 11]. Таке інтегроване бачення дозволяє не лише мінімізувати ризики, але й забезпечити високу якість надання медичної допомоги.

Безпека електронних медичних записів (EHR).

Запровадження електронних медичних записів сприяє оптимізації роботи медичних закладів, проте одночасно підвищує ризики витоку конфіденційної інформації. Як зазначено в журналі етики Американської медичної асоціації, «електронні медичні записи, незважаючи на зручність їх використання, є однією з найбільш уразливих точок для по-

тенційних кіберзлочинців» [8]. Тому забезпечення їх безпеки стає однією з головних задач сучасних медичних установ.

За даними Zenarmor, «ефективна система безпеки EHR повинна включати багаторівневі заходи, зокрема шифрування, автентифікацію користувачів та регулярний моніторинг системних активностей» [7]. Такий комплексний підхід дозволяє знизити ймовірність несанкціонованого доступу до медичних даних, що є особливо важливим в умовах зростання кількості кіберзагроз. Водночас, практика показує, що недотримання вимог HIPAA щодо безпеки електронних даних може призвести до значних штрафних санкцій та втрати довіри з боку пацієнтів.

Мультимедійні дані та виклики HIPAA.

Окрім традиційних текстових даних, сучасні медичні установи активно використовують мультимедійні дані, зокрема фотографії, аудіо- та відеозаписи, для документування клінічних випадків та комунікації між медичними працівниками. У блозі PaloBox зазначено, що «забезпечення HIPAA-відповідності для фотографій, аудіо та відеоматеріалів є критичним завданням, оскільки ці дані часто містять конфіденційну інформацію про пацієнтів» [6]. Проблематика полягає у тому, що традиційні методи захисту даних можуть бути недостатніми для забезпечення безпеки мультимедійних файлів, що вимагає розробки спеціалізованих рішень.

Дослідження показують, що навіть незначні помилки у використанні або зберіганні мультимедійних даних можуть призвести до серйозних порушень конфіденцій-

ності. Як підкреслюється в аналітичних матеріалах з Compliance Home, «порушення НІРАА при роботі з мультимедійними даними можуть виникнути як через людський фактор, так і через недосконалість технологічних рішень» [11]. Ці виклики вимагають від медичних установ впровадження комплексних стратегій захисту, які враховують специфіку кожного типу даних.

Приклади порушень НІРАА та їх юридичні наслідки.

Аналіз практичних кейсів порушення НІРАА дозволяє виявити типові слабкі місця систем захисту медичної інформації. Стаття на eTactics наводить численні приклади порушень, які варіюються від несанкціонованого доступу до електронних медичних записів до неправильного використання мультимедійних даних [12]. Ці приклади свідчать про те, що навіть невеликі недоліки у впровадженні заходів безпеки можуть мати серйозні юридичні наслідки, включаючи штрафні санкції, адміністративні розслідування та втрату довіри пацієнтів.

Юридичний аналіз показує, що основною причиною порушень є як людський фактор, так і недосконалість технічних систем. «Порушення НІРАА часто виникають через недостатнє навчання персоналу та відсутність комплексних заходів безпеки, що підтверджується численними кейсами з практики» [12]. Такий висновок підкреслює необхідність інтеграції юридичних, технічних та організаційних рішень для забезпечення належного захисту медичних даних.

Інтеграція юридичних та етичних підходів: синергетичний ефект.

Окрім технічних аспектів захисту даних, інтеграція юридичних та етичних підходів дозволяє забезпечити більш комплексний захист пацієнтської інформації. Етичні принципи, зокрема забезпечення інформованої згоди та поваги до конфіденційності, тісно переплітаються з юридичними вимогами НІРАА. Як відзначається в літературі, «забезпечення конфіденційності та дотримання норм інформованої згоди є ключовими складовими етичного підходу в охороні здоров'я» [2, 4]. Цей синергетичний ефект дозволяє не лише уникнути юридичних наслідків, але й сприяє формуванню довіри між пацієнтами та медичними установами.

Інтеграція підходів проявляється, зокрема, у впровадженні комплексних політик безпеки, що враховують як технічні, так і організаційні заходи. Сучасні медичні установи дедалі частіше застосовують системи навчання персоналу, що розглядають етичні аспекти використання інформаційних технологій поряд із технічними вимогами НІРАА. Такий підхід сприяє створенню корпоративної культури, де захист даних розглядається як невід'ємна частина загальної місії установи.

Практичні рекомендації для медичних установ.

На основі проведеного аналізу можна сформулювати низку практичних рекомендацій, спрямованих на підвищення рівня захисту конфіденційності та безпеки медичної інформації:

Вдосконалення технічних заходів безпеки. Медичним установам рекомендується впроваджувати сучасні методи захисту електронних

медичних записів, зокрема використання шифрування, багатофакторної автентифікації та регулярного моніторингу системних активностей [7, 8]. Такі заходи дозволяють знизити ризики несанкціонованого доступу до конфіденційної інформації.

Підвищення рівня обізнаності персоналу. Регулярні тренінги та навчальні програми, що охоплюють як юридичні аспекти НІРАА, так і етичні вимоги щодо інформованої згоди та конфіденційності, сприятимуть зниженню числа порушень, зумовлених людським фактором [12].

Розробка політик щодо роботи з мультимедійними даними. Оскільки зображення, аудіо- та відеоматеріали стають невід'ємною частиною медичної документації, необхідно розробити окремі інструкції та політики щодо їх зберігання, передачі та обробки, що відповідають вимогам НІРАА [6, 10, 11]. Особлива увага має бути приділена захисту даних під час використання мобільних пристроїв та хмарних сервісів.

Інтеграція етичних стандартів у щоденну практику. Медичні установи повинні розробити та впровадити внутрішні політики, що забезпечують прозорість отримання інформованої згоди та гарантують повагу до приватності пацієнтів. Це дозволить не лише уникнути юридичних наслідків, але й зміцнити довіру пацієнтів до системи охорони здоров'я [2, 4, 3].

Постійний аудит та оновлення систем безпеки. Регулярні аудити інформаційних систем допоможуть виявити потенційні вразливості та своєчасно впровадити необхідні оновлення, що забезпечить постійне вдосконалення рівня захисту даних

[7, 8]. Такий підхід є критично важливим в умовах стрімкого розвитку кіберзагроз.

Обговорення перспектив розвитку теми.

У майбутньому можна очікувати подальше удосконалення нормативно-правової бази, що регулює питання конфіденційності та безпеки медичної інформації. Інноваційні технології, зокрема штучний інтелект та машинне навчання, можуть стати важливими інструментами для автоматизації процесів захисту даних. Проте з їх впровадженням виникають нові етичні та юридичні виклики, що потребують комплексного підходу.

Водночас інтеграція технологічних рішень із суворими етичними стандартами створює можливості для формування нової парадигми охорони здоров'я, де права пацієнтів та ефективність медичних послуг знаходяться у балансі. Наприклад, застосування технологій для аналізу великих обсягів даних може сприяти підвищенню якості діагностики, проте одночасно вимагає вдосконалення заходів захисту конфіденційної інформації. «Необхідність збереження конфіденційності пацієнтів в умовах цифровізації охорони здоров'я вимагає синергії між технологічними рішеннями та етичними нормами» [2, 4].

Крім того, зростаюча кількість випадків порушень НІРАА свідчить про необхідність розробки більш гнучких та адаптивних систем контролю, які зможуть своєчасно реагувати на нові виклики кібербезпеки. Досвід окремих медичних установ, що впровадили комплексні системи захисту, може бути використаний як модель для розробки універсальних

стандартів, що враховують специфіку роботи з різними типами даних [11, 12]. Це дозволить знизити ризики та підвищити рівень довіри пацієнтів до системи охорони здоров'я.

Висновки. У дослідженні було проведено комплексний аналіз нормативних, юридичних та етичних аспектів застосування НІРАА у сучасній охороні здоров'я. Розглянуто основні положення НІРАА, що регулюють захист конфіденційної медичної інформації, а також окреслено основні етичні виклики, пов'язані з забезпеченням інформованої згоди та дотриманням принципів конфіденційності. Аналіз літературних джерел та практичних кейсів свідчить про необхідність інтеграції технічних заходів безпеки з етичними та організаційними підходами, що сприятиме формуванню більш надійної системи захисту пацієнтської інформації.

Зокрема, впровадження сучасних технологій для захисту електронних медичних записів, розробка спеціалізованих політик для роботи з мультимедійними даними та регулярне навчання персоналу є основними кроками для зниження ризиків порушень НІРАА. Водночас інтеграція етичних стандартів у щоденну практику дозволить забезпечити не лише юридичну відповідальність, але й зміцнення довіри між пацієнтами та медичними установами.

Перспективи розвитку теми включають подальшу адаптацію нормативно-правової бази до умов стрімкого розвитку інформаційних технологій, розробку нових методів кібербезпеки з використанням штучного інтелекту та інтеграцію технологічних рішень із загальними

етичними стандартами охорони здоров'я. Цей підхід сприятиме формуванню універсальної системи захисту, що зможе оперативно реагувати на нові виклики та забезпечувати високий рівень конфіденційності та безпеки медичної інформації.

Перспективи для подальших досліджень. Подальші дослідження мають зосередитись на наступних напрямках:

1) Аналіз впливу новітніх технологій на правову відповідальність у сфері охорони здоров'я. Вивчення випадків застосування штучного інтелекту та автоматизованих систем захисту дозволить розробити нові моделі забезпечення конфіденційності.

2) Розробка інтегрованих систем навчання персоналу. Поглиблений аналіз потреб медичних установ щодо підвищення обізнаності співробітників у питаннях безпеки даних допоможе сформувати рекомендації для створення ефективних програм навчання.

3) Вивчення міжнародного досвіду регулювання захисту медичної інформації. Порівняльний аналіз нормативних актів інших країн може сприяти удосконаленню вітчизняної системи охорони здоров'я та розробці нових підходів до забезпечення безпеки даних.

4) Оцінка ефективності сучасних технологічних рішень у запобіганні порушенням НІРАА. Проведення емпіричних досліджень та аналіз практичних кейсів дозволить визначити оптимальні стратегії для впровадження систем захисту інформації.

З огляду на вищезазначене, інтеграція юридичних, етичних та тех-

нологічних аспектів у систему охорони здоров'я є критично важливою для забезпечення високих стандартів якості медичних послуг. Результати дослідження свідчать про те, що комплексний підхід до захисту медичної інформації сприяє не лише зниженню ризиків кіберзагроз, але й підвищує довіру пацієнтів до системи охорони здоров'я.

Підсумовуючи, можна стверджувати, що нормативна база HIPAA відіграє вирішальну роль у забезпеченні конфіденційності та безпеки медичної інформації. Сучасні виклики цифрової ери вимагають постійного вдосконалення як технічних, так і організаційних заходів, а також інтеграції етичних принципів у щоденну практику медичних установ. Реалізація запропонованих рекомендацій може стати основою для

формування єдиної системи захисту, здатної оперативно реагувати на нові загрози та забезпечувати високий рівень довіри між пацієнтами та медичними закладами.

Зважаючи на стрімкий розвиток технологій та постійні зміни в нормативно-правовому полі, подальші дослідження повинні бути спрямовані на адаптацію існуючих підходів до сучасних умов. Тільки комплексний підхід, що об'єднує юридичні, етичні та технічні аспекти, дозволить забезпечити ефективний захист медичної інформації у майбутньому. «Успіх будь-якої системи охорони здоров'я значною мірою залежить від здатності інтегрувати інноваційні технології із строгими етичними нормами, що гарантують повагу до прав пацієнтів» [2, 4].

Список використаних джерел

1. CDC. Health Insurance Portability and Accountability Act of 1996 (HIPAA). URL: <https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html> (дата звернення: 01.02.2025).
2. AIHCP. Healthcare Ethics – Critical Issues in Informed Consent. URL: <https://aihcp.net/2024/07/09/healthcare-ethics-critical-issues-in-informed-consent/> (дата звернення: 01.02.2025).
3. Standards of Care. Confidentiality and HIPAA. URL: <https://www.standardsofcare.org/understanding-care/confidentiality-and-hipaa/> (дата звернення: 01.02.2025).
4. AIHCP. Health Care Ethics and Informed Consent: A Comprehensive Guide. URL: <https://aihcp.net/2024/10/14/health-care-ethics-and-informed-consent-a-comprehensive-guide/> (дата звернення: 01.02.2025).
5. RadiologyInfo. Patient Privacy. URL: <https://www.radiologyinfo.org/en/info/article-patient-privacy> (дата звернення: 01.02.2025).
6. Paubox. HIPAA Compliance for Photos, Audio and Video Recordings. URL: <https://www.paubox.com/blog/hipaa-compliance-for-photos-audio-and-video-recordings> (дата звернення: 01.02.2025).
7. Zenarmor. What is EHR Security. URL: <https://www.zenarmor.com/docs/network-security-tutorials/what-is-ehr-security> (дата звернення: 01.02.2025).
8. AMA Journal of Ethics. Electronic Health Records: Privacy, Confidentiality and Security. URL: <https://journalofethics.ama-assn.org/article/electronic-health-records-privacy-confidentiality-and-security/2012-09> (дата звернення: 01.02.2025).

9. Avant. Clinical Images: A Snapshot of the Issues. URL: <https://avant.org.au/resources/clinical-images-a-snapshot-of-the-issues> (дата звернення: 01.02.2025).
10. NetSec News. HIPAA Pictures. URL: <https://www.netsec.news/hipaa-pictures/> (дата звернення: 01.02.2025).
11. Compliance Home. HIPAA Compliance Photos. URL: <https://www.compliancehome.com/hipaa-compliance-photos/> (дата звернення: 01.02.2025).
12. eTactics. HIPAA Violation Examples. URL: <https://etactics.com/blog/hipaa-violation-examples> (дата звернення: 01.02.2025).

Olena Ponomaryova, *Candidate of Legal Sciences, Senior Researcher, Senior Research Fellow at the Department of Intellectual Property and Human Rights in Healthcare Institute of Intellectual Property, National Academy of Legal Sciences of Ukraine*

ORCID: 0000-0002-8232-3748

Analysis of the HIPAA regulatory framework: ethical and legal aspects of confidentiality and security of medical information in modern healthcare

The article examines the legal, ethical, and practical aspects of implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in the context of modern healthcare information technologies. The study analyzes the key provisions of HIPAA, the issues of confidentiality, the security of electronic health records (EHR), ethical challenges related to obtaining informed consent, and the peculiarities of working with multimedia data in medical practice. The author's analysis is supported by data from a range of sources [1-12]. The research findings outline the prospects for the development of the regulatory framework and practical measures to ensure the confidentiality and security of patient information.

One of the key themes is the need to integrate HIPAA requirements with modern technologies used for processing and storing medical data, particularly in areas such as radiology and clinical imaging. Among the ethical issues, the article highlights the challenges related to obtaining informed consent from patients and protecting their privacy when using multimedia data in medical practice.

The author emphasizes the importance of a comprehensive approach to implementing security technologies, which includes not only technical but also organizational and ethical solutions. The article provides recommendations for improving security systems, raising awareness among medical professionals, and developing policies for working with multimedia data that comply with HIPAA requirements. Special attention is given to the importance of staff training, the development of internal policies to protect confidentiality, and regular security system audits.

The findings of the study indicate that effective implementation of HIPAA requirements requires continuous improvement of the regulatory framework and

technological solutions. The prospects for the development of this topic are driven by the need to adapt to new technological changes emerging in the healthcare sector, particularly in the context of the growing use of artificial intelligence and automated systems to ensure the security of medical data.

Keywords: *HIPAA compliance, healthcare data security, medical information privacy, electronic health records (EHR), patient confidentiality, informed consent, multimedia data protection, cybersecurity in healthcare, ethical standards in healthcare, medical data regulations.*