https://doi.org/10.29188/2712-9217-2025-11-4-7-16

Правовой суверенитет личности в цифровом здравоохранении в эпоху искусственного интеллекта

И.А. Шадеркин
ООО «Робоскоп патолоджи», Москва, Россия
Контакт: Шадеркин Игорь Аркадьевич, info@uroweb.ru

Аннотация:

Данное аналитическое исследование посвящено одной из наиболее сложных проблем современного права и биоэтики – вопросу принадлежности медицинских данных в эпоху цифрового здравоохранения и искусственного интеллекта. Автор проводит сравнительный анализ правового регулирования и правоприменительной практики в трех юрисдикциях: Российской Федерации (ФЗ-323, ЕГИСЗ), Европейском Союзе (GDPR) и США (HIPAA, 21st Century Cures Act).
В статье раскрывается фундаментальная дихотомия между правом собственности на материальный носитель (сервер, бумажная карта), которое принадлежит медицинской организации, и правами на информационное содержание, которыми наделен пациент. Установлено, что ни одна из рассматриваемых систем не наделяет пациента абсолютным правом собственности (включая право на уничтожение данных) из-за требований общественной безопасности и юридической защиты врачей.
Исследование показывает различия в подходах – российская модель характеризуется централизацией (ЕГИСЗ) и бюрократизированной процедурой доступа; европейская модель фокусируется на правах личности, но ограничивает «право на забвение» в медицине; американская модель через запрет на блокирование информации и внедрение API (Blue Button 2.0) реализует быстрый технологический доступ к данным.
Проведенный сравнительно-правовой анализ регулирования в РФ, США и ЕС показывает, что ни в одной из рассматриваемых юрисдикций пациент не наделяется абсолютным правом собственности на медицинскую документацию; юридически закреплено разделение, при котором материальный носитель принадлежит медицинской организации, а пациент имеет права лишь на информационное содержание. При этом реализация «права на забвение» в медицинской сфере фактически невозможна из-за приоритета общественной безопасности и жестких требований к архивному хранению и аудиту данных.
Несмотря на различия в механизмах реализации прав — от бюрократической централизации в РФ и акцента на юридической защите в ЕС до технологической открытости через API в США — общим вектором развития становится смена парадигмы.
Реальный «информационный суверенитет» пациента в цифровую эпоху достигается не через попытки получения прав на оригинал документа, а через переход от владения к контролю: технологическую возможность беспрепятственного создания независимых личных цифровых архивов.

Ключевые слова: медицинские данные; права пациента; цифровое здравоохранение; искусственный интеллект; электронная медицинская карта (ЭМК); право собственности на данные; ЕГИСЗ; GDPR; HIPAA; информационный суверенитет; персональные данные; право на доступ; право на забвение; интероперабельность.

Для цитирования: Шадеркин И.А. Правовой суверенитет личности в цифровом здравоохранении в эпоху искусственного интеллекта. Российский журнал телемедицины и электронного здравоохранения 2025;11(4):7-16; https://doi.org/10.29188/2712-9217-2025-11-4-7-16

Legal Sovereignty of the Individual in Digital Healthcare in the Era of Artificial Intelligence
Expert opinion

https://doi.org/10.29188/2712-9217-2025-11-3-7-16

I.A. Shaderkin
Roboskop Pathology LLC, Moscow, Russia

Contact: Igor A. Shaderkin, info@uroweb.ru

Summary:

This analytical study addresses one of the most complex issues in modern law and bioethics: the ownership of medical data in the era of digital healthcare and artificial intelligence. The author conducts a comparative analysis of legal regulations and enforcement practices across three jurisdictions: the Russian Federation (Federal Law 323, EGISZ), the European Union (GDPR), and the USA (HIPAA, 21st Century Cures Act).

The paper reveals the fundamental dichotomy between ownership of the physical medium (server, paper record), which belongs to the medical organization, and rights to the informational content, which are vested in the patient. It is established that no jurisdiction grants the patient absolute property rights (including the right to data destruction) due to public safety requirements and the legal defense needs of physicians.

The study highlights distinct approaches: the Russian model is characterized by centralization (EGISZ) and bureaucratic access procedures ; the European model focuses on individual rights but restricts the «right to be forgotten» in medicine; while the US model, through the ban on «information blocking» and the implementation of APIs (Blue Button 2.0), enables rapid technological access to data.

The comparative legal analysis of regulation in the Russian Federation, the USA, and the EU demonstrates that in none of the jurisdictions examined is the patient granted an absolute right of ownership over medical records; a dichotomy is legally established wherein the physical medium belongs to the medical organization, while the patient holds rights only to the informational content. Furthermore, the implementation of the “right to be forgotten” in the medical sphere is effectively impossible due to the priority of public safety and strict requirements for archival storage and data auditing.

Despite differences in the mechanisms of rights implementation—ranging from bureaucratic centralization in the Russian Federation and an emphasis on legal protection in the EU to technological openness via APIs in the USA—a paradigm shift is becoming the common vector of development. Real patient “information sovereignty” in the digital age is achieved not through attempts to obtain rights to the original document, but through a transition from ownership to control: the technological ability to seamlessly create independent personal digital archives.

Key words: medical data; patient rights; digital health; artificial intelligence; Electronic Health Records (EHR); data ownership; EGISZ; GDPR; HIPAA; information sovereignty; personal data; right of access; right to be forgotten; interoperability.

For citation: Shaderkin I.A. Digital Health: Legal Sovereignty of the Individual in Digital Healthcare in the Era of Artificial Intelligence. Russian Journal of Telemedicine and E-Health 2025;11(4):7-16; https://doi.org/10.29188/2712-9217-2025-11-4-7-16

ВВЕДЕНИЕ

Вопрос принадлежности медицинской информации является одной из самых сложных и многогранных проблем современного права, биоэтики и организации здравоохранения. Исторически сложившаяся патерналистская модель медицины, где врач выступал единственным хранителем знания и судьбы пациента, в XXI веке столкнулась с концепцией пациент-центрированности и цифровой трансформацией. В эпоху, когда медицинская карта трансформировалась из папки с бумагами в набор записей в распределенных базах данных, понятие «владение» требует фундаментального переосмысления.

Настоящая публикация, выраженная в виде мнения эксперта, представляет собой глубокое аналитическое исследование, направленное на разрешение центрального конфликта: является ли пациент субъектом, обладающим правом собственности на свои медицинские данные, или же он остается пользователем сервиса с ограниченными правами доступа.

Исследование охватывает юридические, технические и правоприменительные аспекты, сравнивая российскую правовую действительность с регуляторными ландшафтами Европейского Союза (GDPR) и Соединенных Штатов Америки (HIPAA).

Актуальность данного анализа обусловлена не только теоретическим интересом, но и практическими последствиями для каждого гражданина. Возможность получить свои данные, передать их другому специалисту для получения «второго мнения», исправить ошибку или потребовать забвения – это не просто бюрократические процедуры, а элементы реализации права на жизнь и здоровье.

В представленной работе детально рассматриваются механизмы реализации этих прав, от подачи заявления в регистратуру районной поликлиники в РФ до использования API-интерфейсов Blue Button 2.0 в системе Medicare в США.

1. Теоретико-правовые основы статуса медицинской документации

1.1. Дихотомия материального носителя и информационного содержания

Для понимания юридической природы медицинской документации необходимо провести четкое разграничение между физическим носителем и информацией как таковой. Это различие является краеугольным камнем во всех рассматриваемых юрисдикциях [1].

Традиционно в гражданском праве право собственности распространяется на материальные объекты (вещи). Медицинская карта пациента (форма 025/у в РФ) как физический объект – пачка бумаги, скрепленная и пронумерованная, или жесткий диск сервера, где хранится база данных, – является собственностью медицинской организации. Клиника несет расходы на приобретение бланков, содержание архивов и серверов. Следовательно, право на «карту» как на вещь принадлежит учреждению.

Однако содержание карты – сведения о состоянии здоровья, диагнозах, результатах анализов – относится к категории нематериальных благ и персональных данных. Здесь возникает коллизия прав:

1. Право медицинской организации (авторское и трудовое). Врач, заполняющий карту, осуществляет интеллектуальную деятельность. Формулировка диагноза, описание анамнеза, эпикриз – это результат профессионального труда.
2. Право пациента (личное неимущественное). Информация касается непосредственно личности пациента, его физиологической и социальной сущности. Согласно Конституции РФ и международным конвенциям, каждый имеет право на неприкосновенность частной жизни и ознакомление с документами, затрагивающими его права.

Анализ показывает, что ни одна современная правовая система не наделяет пациента абсолютным правом собственности на медицинскую карту в том же смысле, в каком он владеет недвижимостью или автомобилем [2, 3]. Вместо этого законодатель конструирует сложный комплекс прав, включающий право доступа, копирования, исправления и ограничения обработки, но редко – право полного изъятия оригинала [4].

1.2. Медицинские данные как особая категория персональных данных

В теории информационного права медицинские данные выделяются в специальную категорию, требующую повышенного уровня защиты.

- В Российской Федерации ФЗ-152 «О персональных данных» относит сведения о состоянии здоровья к специальным категориям персональных данных, обработка которых допускается только с письменного согласия субъекта, за исключением медико-профилактических целей [5].
- В Евросоюзе – статья 9 GDPR запрещает обработку данных о здоровье по умолчанию, вводя исчерпывающий перечень исключений [6].
- В США – HIPAA Privacy Rule вводит понятие PHI (Protected Health Information), которое охватывает любую информацию в медицинской карте, позволяющую идентифицировать личность [1, 6].

Возникает парадокс – чем более чувствительна информация, тем сложнее пациенту реализовать полное право собственности на нее. Государство, стремясь защитить эти данные, накладывает строгие ограничения на их оборот, хранение и удаление, что часто интерпретируется пациентами как ограничение их свободы распоряжения собственной информацией.

2. Российская Федерация. Законодательное регулирование и правоприменительная практика

2.1. Нормативный ландшафт

В России правовой статус пациента и его данных регулируется многоуровневой системой нормативных актов. Базовым фундаментом является статья 41 Конституции РФ (право на охрану здоровья) и статья 24 (обязанность органов власти и организаций обеспечить каждому возможность ознакомления с документами). ▸▸

Основным отраслевым законом является Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации». Статья 22 данного закона – «Информация о состоянии здоровья» – является ключевой для нашего исследования [5].

Закон гласит: «Каждый имеет право получить в доступной для него форме имеющуюся в медицинской организации информацию о состоянии своего здоровья». Формулировка «получить информацию» принципиально отличается от «получить документ». Законодатель закрепил за пациентом право знать, что написано в карте, но оставил оригинал документа в ведении медицинской организации.

Это решение продиктовано необходимостью обеспечения преемственности лечебного процесса и юридической защиты врачей. Медицинская карта является основным доказательством в спорах о качестве оказания медицинской помощи. Изъятие оригинала пациентом лишило бы клинику возможности защитить себя в суде в случае претензий, а также нарушило бы требования к статистическому учету.

2.2. Процедура доступа и получения копий – анализ Приказов № 1050н и № 789н

Реализация декларативного права, прописанного в законе, осуществляется через жестко регламентированные подзаконные акты Минздрава России. Именно здесь кроются основные бюрократические барьеры для пациента.

Порядок ознакомления – Приказ Минздрава РФ № 1050н

Приказ от 12.11.2021 № 1050н устанавливает процедуру ознакомления пациента с оригиналами медицинской документации [7].

- Механизм. Пациент подает письменный запрос. Клиника обязана предоставить возможность ознакомления в специально отведенном помещении под контролем сотрудников.
- Ограничение – вынос оригинала карты за пределы этого помещения запрещен. Это подтверждает тезис о том, что вещественное право на карту остается у клиники.
- Цифровой аспект – если документация ведется в электронном виде, клиника обязана предоставить заверенную копию. Термин «заверенная копия» подразумевает, что юридическая сила оригинала остается за электронной записью в базе данных (МИС) клиники, а пациенту выдается производный документ.

Сроки и форматы выдачи (Приказ Минздрава РФ № 789н).

Приказ от 31.07.2020 № 789н регулирует выдачу копий и выписок. Анализ сроков показывает значительный разрыв между цифровыми ожиданиями пациентов и нормативной реальностью [8].

- Максимальный срок подготовки документов составляет 30 дней с момента регистрации запроса. Этот срок синхронизирован с ФЗ-59 «О порядке рассмотрения обращений граждан».
- Для пациентов, находящихся в стационаре, выписки и копии должны предоставляться в течение суток (24 часов) [9].

Аналитический вывод. 30-дневный срок для амбулаторного звена является архаичным в эпоху мгновенной передачи данных. Он создает искусственный барьер для пациентов, желающих получить «второе мнение» или сменить клинику. Фактически, клиника может легально удерживать информацию в течение месяца, что может быть критично для динамики заболевания. Это демонстрирует, что в балансе интересов «удобство администрирования клиники» против «оперативность доступа пациента» российский законодатель пока склоняется к первому.

2.3. Право на удаление и «забвение»

Может ли российский пациент, руководствуясь правом собственности на свои данные, потребовать удалить историю болезни?

Анализ законодательства дает однозначный ответ: нет.

В отличие от сферы интернет-поиска, где действует «право на забвение» (ст. 10.3 ФЗ «Об информации...»), в медицине действуют императивные нормы архивного дела [10].

- Сроки хранения. Приказы Минздрава и перечни типовых архивных документов устанавливают длительные сроки хране-

ния медицинской документации: 25 лет для амбулаторных карт, 50 лет для историй болезни стационара, 25 лет для стоматологических карт и т.д.

- Обязанность клиники. Уничтожение документов до истечения этих сроков является административным правонарушением и нарушением лицензионных требований. Даже если пациент отзывает согласие на обработку персональных данных (по ФЗ-152), клиника вправе продолжить обработку данных, необходимых для «осуществления медицинской деятельности» и «выполнения возложенных законодательством функций» (п. 2 ч. 2 ст. 10 ФЗ-152).

Таким образом, пациент в РФ лишен права на удаление своего медицинского прошлого. Это обосновывается публичным интересом (эпидемиологический учет) и интересами правосудия (возможность расследования врачебных ошибок спустя годы) [11].

2.4. Цифровой контур здравоохранения. ЕГИСЗ и роль частных клиник

Внедрение Единой государственной информационной системы в сфере здравоохранения (ЕГИСЗ) фундаментально меняет ландшафт владения данными. Государство централизует сбор информации, создавая «супер-архив», независимый от воли конкретной клиники или пациента.

Обязательность передачи данных частными клиниками

В 2024-2025 годах завершился период неопределенности относительно обязанности частных медицинских организаций передавать данные в ЕГИСЗ. Распространенное мнение о существовании отсрочки до 2027 года является юридическим заблуждением (мифом), активно опровергаемым экспертами и регуляторами [12].

Лицензионные требования (Постановление Правительства РФ № 852) императивно обязывают все медицинские организации, независимо от формы собственности, вносить сведения в ЕГИСЗ. Неисполнение этого требования влечет штрафы и риск приостановки лицензии [12, 13].

Для пациента это означает потерю «приватности через изоляцию». Раньше пациент мог лечиться в частной клинике, рассчитывая, что информация останется только в ее стенах. Теперь данные о диагнозах и приемах в частном секторе агрегируются в государственном профиле пациента, доступном врачам государственных учреждений (с согласия) и ведомствам.

Реализация на портале Госуслуг

Портал Госуслуг выступает «витриной» ЕГИСЗ для пациента. Функционал «Мое здоровье» позволяет скачивать электронные медицинские документы (СЭМД).

Технический анализ форматов выгрузки [14]:

1. PDF. Человекочитаемый формат. Предназначен для печати и личного архива.

2. XML. Машиночитаемый формат. Предназначен для обмена между информационными системами.

3. SIG (ЭЦП). Файл отсоединенной электронной подписи. Гарантирует неизменность и авторство документа.

Наличие XML-формата теоретически обеспечивает интероперабельность (переносимость) данных. Однако на текущем этапе экосистема приложений, способных загрузить и визуализировать этот XML для пациента (по аналогии с Apple Health), в России развита слабо. Пациент получает файл, который он не может прочитать без специальных средств, что снижает практическую ценность владения данными.

2.5. Судебная практика и защита интересов

Вопрос владения данными становится критическим в судебных спорах. Практика показывает, что отсутствие у пациента копий медицинской документации часто делает невозможным доказательство врачебной ошибки.

В российских судах ходатайства пациентов об истребовании оригиналов карт часто удовлетворяются, но клиники нередко заявляют об «утере» документации. Внедрение ЕГИСЗ и электронных медицинских карт (ЭМК) решает эту проблему: электронный след невозможно «потерять» так же легко, как бумажную папку. ⏩

3. Международный опыт. Европейский Союз (GDPR)

3.1. Концепция GDPR: Контроль над данными вместо владения

Европейский подход, закрепленный в General Data Protection Regulation (GDPR), смещает акцент с вещественного права на права человека. Регламент не использует термин «собственность», но наделяет субъекта данных беспрецедентным объемом прав контроля [6].

3.2. Ключевые права пациента в контексте медицинских данных

Право доступа (Article 15)

Пациент имеет право получить подтверждение факта обработки данных и копию всех персональных данных. В отличие от РФ, предоставление первой копии должно быть бесплатным. Срок ответа – «без неоправданной задержки», но не позднее одного месяца (с возможностью продления еще на два в сложных случаях) [15].

Право на переносимость (Article 20 Data Portability)

Это новаторское право позволяет пациенту получить свои данные в «структурированном, универсальном и машиночитаемом формате» и передать их другому врачу. Это прямой шаг к реализации концепции владения: пациент может «забрать» свой цифровой профиль из одной клиники и «загрузить» его в другую. Это коррелирует с российским XML-форматом, но в ЕС стандарты интероперабельности (HL7 FHIR) внедряются более системно.

Право на удаление («право на забвение», Article 17)

Самый обсуждаемый аспект GDPR – статья 17 «Right to Erasure». Может ли европеец удалить свою медкарту? Анализ исключений показывает, что в медицине это право практически не работает [16].

Пункт 3 статьи 17 прямо блокирует удаление, если обработка необходима:

- Для целей профилактической или профессиональной медицины (диагностика, лечение).
- В интересах общественного здравоохранения.
- Для установления, осуществления или защиты правовых притязаний.

Врачебная практика в странах ЕС тесно связана со страхованием профессиональной ответственности. Врачи обязаны хранить записи для защиты от потенциальных исков. Поскольку сроки исковой давности могут исчисляться десятилетиями (особенно в педиатрии), клиники легально отказывают пациентам в удалении основных медицинских записей [17]. Удалению могут подлежать лишь вспомогательные данные (например, контакты для маркетинговых рассылок), но не клиническая история.

4. Международный опыт. США (HIPAA и Cures Act)

4.1. HIPAA. Приватность без права собственности

В США регулирование базируется на Health Insurance Portability and Accountability Act (HIPAA) 1996 года. Важно понимать: HIPAA – это федеральный стандарт приватности и безопасности, но он ***не устанавливает право собственности*** на записи. Вопрос собственности решается на уровне штатов.

- В большинстве штатов (Флорида, Техас, Джорджия и др.) законы прямо указывают, что медицинские записи являются собственностью госпиталя или врача. Только в штате Нью-Гэмпшир закон (N.H. Rev. Stat. Ann. § 332-I:1) декларирует, что информация в медицинской записи является собственностью пациента [3].
- HIPAA Privacy Rule дает пациенту право на доступ к «определенному набору записей», который включает медицинские и биллинговые записи, используемые для принятия решений о пациенте [18].

4.2. Невозможность удаления и Audit Trails

В США концепция «удаления» медицинской записи противоречит требованиям HIPAA Security Rule и стандартам аккредитации.

Системы электронных медицинских карт (EHR) обязаны вести Audit Trails (аудиторский след). Любое действие – создание, просмотр, редактирование, «удаление» – фиксируется в логе [19, 20].

Если врач «удаляет» ошибочный диагноз, система лишь скрывает его из текущего вида, но сохраняет в базе данных с пометкой о деактивации. Это обеспечивает целостность данных для судебных разбирательств. Таким образом, технически и юридически американский пациент не может «стереть» информацию, он может лишь потребовать внести поправку, которая будет прикреплена к оригинальной (ошибочной) записи [18].

4.3. Революция доступа

В 2016 г. был принят 21st Century Cures Act, который ввел запрет на «блокирование информации». Это радикально изменило баланс сил.

- Провайдеры (клиники, разработчики ПО) не имеют права препятствовать доступу, обмену или использованию электронной медицинской информации (EHI).
- Закон обязал использовать открытые стандартизированные API. Это означает, что пациент имеет право подключить любое стороннее приложение (например, фитнес-трекер или агрегатор данных) к базе данных своего госпиталя и скачать свои данные.

5. Технологическая реализация и форматы данных

5.1. Blue Button 2.0 и стандарт FHIR

Наиболее передовой опыт реализации прав пациента на данные демонстрирует программа Blue Button 2.0, запущенная Centers for Medicare & Medicaid Services (CMS) в США.

- Технология. Система построена на стандарте HL7 FHIR (Fast Healthcare Interoperability Resources) и протоколе авторизации OAuth 2.0 [21].
- Механизм. Пациент (бенефициар Medicare) авторизуется на портале и дает разрешение стороннему приложению на доступ к своим данным.
- Формат данных. Данные передаются в формате JSON (JavaScript Object Notation). В отличие от российского PDF или тяжеловесного XML, JSON легко обрабатывается веб-приложениями и мобильными устройствами.
- Объем данных. Через API доступны ресурсы Patient (демография), Coverage (страховка) и ExplanationOfBenefit (детализация оказанных услуг, диагнозы, стоимость) [22].

Эта модель (Data-as-a-Service) фактически решает проблему собственности через технологию: пациенту не нужно владеть сервером клиники, если он владеет ключом доступа (токеном), позволяющим в любой момент забрать данные в удобном виде.

5.2. Сравнение форматов РФ и США

В России пациент получает «слепок» данных на момент запроса. В США через API пациент создает «живой поток» данных. Российский подход (файловый обмен) надежнее с точки зрения архивного хранения, но американский (API) дает больше возможностей для управления здоровьем в реальном времени (табл 1, 2). ▸▸

Таблица 1. Сравнение форматов РФ и США
Table 1. Comparison of Russian and USA formats

Характеристика Characteristics	Россия (Госуслуги / ЕГИСЗ)/Russia (Gosuslugi / Unified State Health Information System)	США (Blue Button 2.0 / CMS) USA (Blue Button 2.0 / CMS)
Основной формат	PDF (визуальный) + XML (структурированный, сложный)	JSON (структурированный, веб-ориентированный)
Стандарт обмена	СЭМД (на базе HL7 CDA)	HL7 FHIR R4
Механизм доступа	Скачивание файла (архив.zip)	API (прямое подключение приложений)
Аутентификация	ЕСИА (Госуслуги)	OAuth 2.0 (MyMedicare.gov)
Интероперабельность	Низкая для пациента (сложно использовать файл XML)	Высокая (экосистема из тысяч приложений)

6. Сравнительный анализ

6.1. Сводная таблица правовых режимов

В таблице 2 представлено сравнение ключевых параметров владения и управления данными в трех юрисдикциях.

6.2. Анализ проблемы собственности

Проведенное исследование выявляет фундаментальную проблему: ***ни в одной из рассматриваемых систем пациент не является полноправным собственником своих медицинских данных в классическом понимании гражданского права***. Он не имеет права распоряжения своими данными вплоть до уничтожения.

Причины этого универсальны и не зависят от политического режима той или иной страны:

1. **Доказательная природа медицины.** Медицинская запись – это юридический документ, подтверждающий действия врача. Его уничтожение нарушает право врача на защиту.
2. **Общественный интерес.** Данные о здоровье населения являются национальным достоянием, необходимым для планирования системы здравоохранения, борьбы с эпидемиями и научных исследований. Индивидуальное право на приватность уступает коллективному праву на безопасность.
3. **Финансовый контроль.** В страховых моделях (ОМС в РФ, Medicare в США) записи являются основанием для оплаты счетов. Их удаление сделало бы невозможным финансовый аудит.

Таким образом, вместо *собственности* (владения вещью) современные правовые системы предлагают пациенту модель *информационного суверенитета* или *опекунства*, где пациент управляет правами доступа, но не физическим уничтожением информации.

Отвечая на прямой запрос пользователя:

1. Является ли пациент владельцем медицинских данных?

- Юридически – нет. Оригинал медицинской карты (как бумажной, так и записи в базе данных) принадлежит медицинской организации.
- Фактически – пациент обладает обширными правами *пользования* и *распоряжения копиями* этих данных, но не правом владения источником.

2. Может ли он их потребовать?

- Да. И в России, и за рубежом право на получение копий гарантировано законом (ст. 22 323-ФЗ в РФ, Art. 15 GDPR в ЕС, HIPAA в США). Отказ в выдаче копий является правонарушением.

3. Может ли сохранять у себя?

- Да. Пациент вправе создавать личный архив на основе полученных копий. В РФ это реализуется через скачивание документов с Госуслуг, в США – через приложения, подключенные к Blue Button.

4. Сравнение опыта.

- Российская модель характеризуется вы-

Таблица 2. Сводная таблица правовых режимов владения данными пациентов
Table 2. Summary table of legal regimes for ownership of patient data

Параметр	Россия (РФ)	Евросоюз (GDPR)	США (HIPAA/Cures Act)
Владелец оригинала	Медицинская организация (как создатель документа и владелец носителя).	Контроллер данных (клиника), но права субъекта превалируют.	Провайдер (врач/клиника) в большинстве штатов.
Право требовать данные	Да, право на информацию (ст. 22 323-ФЗ).	Да, право доступа (Art. 15 GDPR).	Да, право доступа и копирования (HIPAA Privacy Rule).
Срок предоставления	До **30 дней** (амбулаторно), 24 часа (стационар).	До **1 месяца** (с возможностью продления).	**30 дней** (с возможностью продления на 30 дней).
Право на удаление	**Отсутствует.** Императивные сроки архивного хранения (25-50 лет).	**Ограничено.** Практически не применяется к медкартам из-за исключений (Art. 17(3)).	**Отсутствует.** Требование целостности и аудиторского следа (Audit Trails).
Переносимость	Реализуется через XML на Госуслугах, но экосистема слабая.	Закреплено законодательно (Art. 20), но техническая реализация варьируется.	Высокая. Information Blocking Rule обязывает использовать открытые API (FHIR).
Исправление ошибок	Возможно при доказанной недостоверности.	Право на исправление (Art. 16) – базовое право.	Право на поправку (Right to Amend). Врач может отказать, но обязан сохранить запрос.

сокой централизацией (ЕГИСЗ) и жестким государственным контролем. Пациент получает доступ через «единое окно» (Госуслуги), но процедура бюрократизирована (срок 30 дней).

- Американская модель (HIPAA/Blue Button) ориентирована на рыночные механизмы и технологическую открытость (API). Она предоставляет более гибкие инструменты доступа, но фрагментирована из-за множества частных провайдеров.
- Европейская модель (GDPR) ставит во главу угла права человека, предлагая самые сильные юридические гарантии защиты, но сталкивается с теми же ограничениями в части удаления данных, что и другие юрисдикции, из-за приоритета медицинской безопасности.

ВЫВОДЫ

На основании проведенного сравнительно-правового анализа регулирования в Российской Федерации, Европейском Союзе и США можно сформулировать следующие ключевые заключения относительно прав пациента на медицинские данные:

1. Иллюзия абсолютного права собственности

Ни одна из рассмотренных юрисдикций не наделяет пациента абсолютным правом собственности на медицинскую документацию в классическом гражданско-правовом смысле. Юридически закреплена фундаментальная дихотомия: право собственности на материальный носитель (сервер, бумажная карта) принадлежит медицинской организации, тогда как пациент наделен правами на информационное содержание.

2. Невозможность «цифрового забвения» в медицине

Требование удаления медицинских данных («право на забвение») фактически нереализуемо ни в одной из систем из-за приоритета общественной безопасности и юридической защиты врачей.

- В РФ это ограничено императивными нормами архивного хранения (до 25–50 лет).
- В США – требованиями к ведению аудиторского следа (Audit Trails), который фиксирует все изменения без возможности физического стирания.
- В ЕС – исключениями ст. 17 GDPR, связанными с целями профилактической медицины и защиты правовых притязаний.

3. Различия в механизмах реализации суверенитета

Реализация прав пациента варьируется от бюрократических до технологических моделей:

- Российская модель характеризуется высокой централизацией (ЕГИСЗ) и бюрократизированной процедурой доступа (срок ожидания до 30 дней), что создает барьеры для оперативного управления здоровьем.
- Европейская модель (GDPR) фокусируется на защите прав личности и юридической возможности переноса данных, однако техническая интероперабельность все еще находится в стадии развития.
- Американская модель (HIPAA/Cures Act) через законодательный запрет на «блокирование информации» и внедрение открытых API (Blue Button 2.0) обеспечивает наиболее быстрый технологический доступ к данным в реальном времени.

4. Смена парадигмы: от владения к контролю

Реальный «информационный суверенитет» пациента в цифровую эпоху достигается не через попытки получить права на оригинал документа, а через технологическую возможность беспрепятственного получения полных цифровых копий. В условиях, когда юридическое удаление данных из систем клиник невозможно, единственной эффективной стратегией защиты интересов пациента становится создание независимого личного цифрового архива (в форматах XML, PDF или через API-агрегаторы).

ЛИТЕРАТУРА

1. Chiruvella V, Guddati AK. Ethical Issues in Patient Data Ownership. *Interact J Med Res* 2021;10(2):e22269. https://doi.org/10.2196/22269

2. International Journal for Research in Applied Science and Engineering Technology (IJRASET). Preserving Privacy and Security: A Comparative Study of Health Data Regulations – GDPR vs. HIPAA

ЛИТЕРАТУРА

[Internet]. 2023 [cited 2026 Jan 2]. Available from: https://www.ijraset.com/research-paper/health-data-regulations-gdpr-vs-hipaa
3. Health Information & the Law. Who Owns Medical Records: 50 State Comparison [Internet]. [cited 2026 Jan 2]. Available from: http://www.healthinfolaw.org/comparative-analysis/who-owns-medical-records-50-state-comparison
4. American Academy of Ophthalmology. Medical Record Ownership and Access [Internet]. 2014 [cited 2025 Dec 2]. Available from: https://www.aao.org/eyenet/article/medical-record-ownership-and-access
5. Российская Федерация. Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» (ред. от 23.07.2025). Ст. 22 [Электронный ресурс]. [цитировано 2026 Янв 2]. Доступно по ссылке: https://www.consultant.ru/document/cons_doc_LAW_121895/d2872d82b3b26ca307971f590ce02dd37f71cafc/
6. Censinet. GDPR vs. HIPAA: Key Differences for Healthcare [Internet]. [cited 2026 Jan 2]. Available from: https://www.censinet.com/perspectives/gdpr-vs-hipaa-key-differences-for-healthcare
7. Министерство здравоохранения Российской Федерации. Приказ от 12.11.2021 № 1050н «Об утверждении Порядка ознакомления пациента либо его законного представителя с медицинской документацией, отражающей состояние здоровья пациента» [Электронный ресурс]. [цитировано 2026 Янв 2]. Доступно по ссылке: http://publication.pravo.gov.ru/Document/View/0001202111260035?index=4
8. Министерство здравоохранения Российской Федерации. Приказ от 31.07.2020 № 789н «Об утверждении порядка и сроков предоставления медицинских документов (их копий) и выписок из них» [Электронный ресурс]. [цитировано 2026 Янв 2]. Доступно по ссылке: https://www.consultant.ru/law/hotdocs/64775.html
9. Medline.su. Об утверждении порядка и сроков предоставления медицинских документов (их копий) и выписок из них [Электронный ресурс]. [цитировано 2026 Янв 2]. Доступно по ссылке: https://medline.su/upload/ob-utverzhdenii-poryadka-i-srokov-predostavleniya-medicinskih-dokumentov-ih-kopij-i-vypisok-iz-nih.pdf
10. Российская Федерация. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (ред. от 24.06.2025). Ст. 10.3 [Электронный ресурс]. [цитировано 2026 Янв 2]. Доступно по ссылке: https://www.consultant.ru/document/cons_doc_LAW_61798/9c2fa12a6b57079c46dbaf3e8af279177d22b87e/
11. Министерство здравоохранения Российской Федерации. Приказ от 07.09.2020 № 947н «Об утверждении Порядка организации системы документооборота в сфере охраны здоровья...». V. Хранение электронных медицинских документов [Электронный ресурс]. [цитировано 2026 Янв 2]. Доступно по ссылке: https://www.consultant.ru/document/cons_doc_LAW_373853/fc8f3189e4f5ad84c953415a9c917867b50f4350/
12. ЕГИСЗ Медицина. Нет отсрочки до 2027 года: клиники должны передавать данные в ЕГИСЗ [Электронный ресурс]. 2024 [цитировано 2026 Янв 2]. Доступно по ссылке: https://egiszmed.ru/blog/kliniki-dolzhny-peredavat-dannye-v-egisz/
13. Директору Клиники. Передача данных в ЕГИСЗ: отсрочки до 2027 года нет. Что делать клиникам? [Электронный ресурс]. [цитировано 2026 Янв 2]. Доступно по ссылке: https://www.dirklinik.ru/news/1607-peredacha-dannyh-v-egisz-otsrochki-do-2027-goda-net-chto-delat-klinikam
14. Госуслуги. Что содержит скачанный архив электронного медицинского документа с подписью [Электронный ресурс]. [цитировано 2026 Янв 2]. Доступно по ссылке: https://www.gosuslugi.ru/help/faq/medical_docs/104158
15. GDPR.eu. Everything you need to know about the "Right to be forgotten" [Internet]. [cited 2025 Dec 2]. Available from: https://gdpr.eu/right-to-be-forgotten/
16. Information Commissioner's Office (ICO). Right to erasure [Internet]. [cited 2025 Dec 2]. Available from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-erasure/
17. Incision Indemnity. GDPR 'Right To Be Forgotten' – Am I Required To Destroy Medical Records? [Internet]. [cited 2025 Dec 2]. Available from: https://incisionindemnity.com/news-resources/gdpr-right-to-be-forgotten/
18. U.S. Department of Health and Human Services (HHS). Audit Protocol [Internet]. [cited 2025 Dec 2]. Available from: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html
19. U.S. Department of Health and Human Services (HHS). Individuals' Right under HIPAA to Access their Health Information [Internet]. [cited 2026 Jan 2]. Available from: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html
20. Compliancy Group. What Are HIPAA Audit Trail and Audit Log Requirements? [Internet]. [cited 2026 Jan 2]. Available from: https://compliancy-group.com/hipaa-audit-log-requirements/
21. Centers for Medicare & Medicaid Services (CMS). API Documentation [Internet]. Blue Button API; [cited 2026 Jan 2]. Available from: https://bluebutton.cms.gov/api-documentation/
22. Centers for Medicare & Medicaid Services (CMS). Understanding the Data [Internet]. Blue Button API; [cited 2026 Jan 2]. Available from: https://bluebutton.cms.gov/data/understanding-the-data/

Сведения об авторе:

Шадеркин И.А. – к.м.н., уролог, генеральный директор ООО «Робоскоп патолоджи», Москва, Россия, РИНЦ Author ID 695560, https://orcid.org/0000-0001-8669-2674

Вклад автора:

Шадеркин И.А. – определение научного интереса, литературный обзор, написание текста, 100%

Конфликт интересов: Автор заявляет об отсутствии конфликта интересов.

Финансирование: Опубликовано без спонсорской поддержки.

Статья поступила: 26.10.25

Рецензирование: 19.11.25

Результаты рецензирования: 06.12.25

Принята к публикации: 10.12.25

Information about author:

Shaderkin I.A. – Ph.D., urologist, CEO of Roboscope Pathology LLC, Moscow, Russia, RSCI Author ID 695560, https://orcid.org/0000-0001-8669-2674

Author Contribution:

Shaderkin I.A. – identification of scientific interest, literature review, text writing, 100%

Conflict of interest. The author declare no conflict of interest.

Financing. Published without sponsorship.

Received: 26.10.25

Reviewing: 19.11.25

Review results: 06.12.25

Accepted for publication: 10.12.25