ФОТО ПАЦИЕНТА, ПЕРЕПИСКА В МЕССЕНДЖЕРЕ И СЛУЧАЙНАЯ УТЕЧКА
7 ошибок клиники при работе с медицинскими данными

Автор: Асад Юсуфов, Председатель Ассоциации по защите прав в сфере здравоохранения

Утечка персональных данных в клинике почти никогда не начинается со взлома сервера. Обычно она начинается с фотографии.

Врач снимает интересный клинический случай и отправляет коллегам. Администратор пересылает пациенту результаты обследования через привычный мессенджер. Сотрудник фотографирует медицинскую карту на личный телефон. Маркетолог выкладывает в соцсеть снимок «до и после». В презентацию для конференции попадает фрагмент истории болезни, где забыли закрыть дату рождения.

Для сотрудников это рабочая рутина. Для медицинской организации — уже потенциальный инцидент, в котором одновременно затронуты персональные данные, врачебная тайна и иногда изображение гражданина. И цена такой ошибки за последние два года выросла принципиально.

РАЗБЕРЕМ СЕМЬ СИТУАЦИЙ, КОТОРЫЕ ЧАЩЕ ВСЕГО ЗАКАНЧИВАЮТСЯ ПРЕТЕНЗИЕЙ ИЛИ ИСКОМ

1. «Пациент же согласился на лечение» — значит, можно использовать его данные?

Нет. Это самая распространённая ошибка, и она системная: разные правовые режимы воспринимаются как один.

Их как минимум три:

- обработка персональных данных;
- сведения, составляющие врачебную тайну;
- использование изображения гражданина.

А если данные планируется опубликовать в интернете или передать неопределённому кругу лиц, появляется четвёртый самостоятельный режим — персональные данные, разрешённые субъектом для распространения.

Сведения о состоянии здоровья относятся к специальным категориям персональных данных — это прямо установлено ст. 10 Федерального закона от 27.07.2006 № 152-ФЗ.

Статья 13 Федерального закона от 21.11.2011 № 323-ФЗ добавляет ещё более узкий режим: врачебную тайну составляют не только диагноз и результаты обследования, но и сам факт обращения гражданина за медицинской помощью.

Поэтому согласие на медицинское вмешательство, договор на оказание платных услуг и стандартное согласие на обработку персональных данных сами по себе не дают клинике права:

- опубликовать фотографию пациента;
- показать результаты его обследований на конференции;
- разместить клинический случай в социальной сети;
- передать материалы блогеру или журналисту;
- снять пациента в рекламном ролике;
- выложить медицинские документы на сайте.

Для публикации закон предусматривает отдельную конструкцию: согласно ст. 10.1 Закона № 152-ФЗ согласие на обработку персональных данных, разрешённых субъектом для распространения, оформляется отдельно от иных согласий.

Формула «мы же взяли согласие на обработку персональных данных» для публичного кейса юридически недостаточна.

2. Фотография «до и после»: одной галочки в договоре мало

Особенно внимательно я рекомендую относиться к съёмке в стоматологии, пластической хирургии, косметологии, дерматологии, трихологии и эстетической медицине.

Здесь накладываются сразу три правовых слоя.

Первый: изображение гражданина охраняется ст. 152.1 ГК РФ. Правило жёсткое — обнародование и дальнейшее использование допускается только с согласия, кроме прямо предусмотренных законом случаев. Если изображение незаконно распространено в интернете, гражданин вправе требовать удаления и запрета дальнейшего распространения.

Второй: фотография содержит персональные данные.

Третий: контекст публикации раскрывает сведения о здоровье.

Представьте снимок лица с подписью***: «Коррекция последствий неудачной ринопластики. Три месяца после повторной операции».*** ФИО нет. Но лицо позволяет идентифицировать человека, а подпись раскрывает обстоятельства лечения. Простого согласия «на фотографирование» здесь недостаточно.

В документах клиники нужно разграничивать:

1) съёмку для медицинских целей;
2) использование материалов внутри организации;
3) использование в образовательных и научных целях;
4) размещение в интернете и соцсетях;
5) использование в рекламе;
6) обработку и распространение соответствующих персональных данных.

И главное: пациент должен понимать, где именно и с какой целью будет опубликовано его изображение. Абстрактное «в информационных целях» не работает.

Суды последовательно исходят из того, что публикация изображения в социальной сети без предусмотренного ст. 152.1 ГК РФ согласия может быть признана незаконной, а само изображение — подлежащим удалению.

3. «Мы убрали имя пациента» — это ещё не обезличивание

Опасная иллюзия: удалили фамилию — случай стал анонимным. Идентифицировать человека позволяет совокупность сведений:

- возраст;
- город;
- профессия;
- редкое заболевание;
- дата операции или госпитализации;
- конкретный врач;
- фотография части тела;
- обстоятельства травмы;
- фрагмент медицинского документа;
- упоминание родственников.

Для небольшого города и редкого случая этого более чем достаточно.

«47-летний главный бухгалтер крупной компании нашего города поступила к нам 12 августа с осложнением после процедуры в другой клинике».

Фамилии нет. Но коллеги, знакомые и сотрудники работодателя установят личность за несколько минут.

Юридически оценивать нужно не наличие имени, а возможность отнести информацию к прямо или косвенно определённому лицу. В медицине риск усилен ст. 13 Закона № 323-ФЗ: тайной является и сам факт обращения за помощью.

Поэтому перед публикацией клинического случая правильный вопрос звучит не ***«убрали ли мы ФИО», а «можно ли по оставшейся совокупности идентифицировать пациента».*** Это разные стандарты.

4. Рабочий чат медицинского работника — тоже зона риска

Типичная ситуация. Врач пишет в чат: «Коллеги, посмотрите КТ, что думаете?» — и прикрепляет снимок.

На изображении одновременно видны фамилия, дата рождения, дата исследования, название клиники, иногда номер медкарты.

С медицинской точки зрения цель разумная — коллегиальное обсуждение. С правовой возникает другой вопрос: где именно происходит обработка и кто получает доступ.

Статья 19 Закона № 152-ФЗ обязывает оператора принимать правовые, организационные и технические меры защиты данных от неправомерного или случайного доступа, копирования, предоставления и распространения. Медицинская организация дополнительно связана режимом врачебной тайны.

Важно: закон не запрещает обмен сведениями между медиками. Обработка данных о здоровье допускается в целях установления диагноза и оказания медицинских услуг лицами, профессионально осуществляющими медицинскую деятельность и обязанными хранить врачебную тайну.

Но из этого не следует, что врач вправе выбирать любой удобный канал. Личные телефоны, персональные облака, стихийные чаты и сторонние сервисы без оценки их правового статуса — это неконтролируемая инфраструктура обработки данных.

Информационная безопасность в клинике давно перестала быть задачей одной только IT-службы. Это вопрос юридического управления организацией.

5. Ответ на негативный отзыв, который сам стал нарушением

Самая конфликтная ситуация из моей практики. Пациент публикует: ***«Ужасная клиника, врач поставил неверный диагноз и назначил ненужное лечение».***

У врача возникает естественное желание ответить публично: ***«Вы сами отказались от обследования, у вас были такие-то показатели и хроническое заболевание…»***

Граница переходится в одну строку.

Даже если пациент первым публично рассказал о конфликте, клиника обязана крайне осторожно относиться к раскрытию сведений, которые сам пациент общедоступными не делал. Судебная практика исходит из того, что, отвечая на критику, медицинская организация не вправе раскрывать факт обращения, состояние здоровья, диагноз и иные сведения, составляющие врачебную тайну, если пациент не раскрыл их добровольно для неопределённого круга лиц.

Право на защиту деловой репутации у клиники есть. Но реализовывать его нужно так, чтобы защита репутации не превратилась в самостоятельное нарушение.

Я рекомендую жёстко разделять два контура:

- публичный ответ — нейтральный, без медицинской конкретики, с приглашением к разбору в личном порядке;
- юридическая защита — претензия, адвокатский запрос, обращение к владельцу площадки, судебный процесс, где информация предоставляется в процессуальном порядке.

Социальная сеть — плохое место для изложения истории болезни.

6. Утечка может быть случайной — ответственность от этого не исчезает

Самая опасная реакция руководителя: ***«Базу никто не продавал, сотрудник просто ошибся адресатом».***

Для законодательства о персональных данных «случайно» не означает «без ответственности».

С 30 мая 2025 года административная ответственность по ст. 13.11 КоАП РФ существенно ужесточена. В действующей редакции предусмотрены самостоятельные составы — в том числе за неуведомление Роскомнадзора об инциденте и за действия либо бездействие оператора, повлёкшие неправомерную передачу, предоставление, распространение или доступ к персональным данным.

Для клиник критичны санкции по специальным категориям: если неправомерная передача касается сведений о состоянии здоровья, штраф для юридического лица измеряется не сотнями тысяч, а миллионами рублей. Для биометрии планка ещё выше. При повторных серьёзных нарушениях предусмотрены оборотные штрафы — процент от выручки.

Поэтому «администратор случайно прикрепил к письму Excel со всеми пациентами» — это не внутренняя оплошность сотрудника. Это полноценный инцидент, требующий немедленного юридического и технического реагирования.

7. Главная ошибка после утечки — попытаться её скрыть

Когда инцидент уже произошёл, организации совершают вторую ошибку: сначала разобраться внутри, никуда не сообщая.

Между тем ст. 21 Закона № 152-ФЗ устанавливает специальный порядок действий оператора при установлении факта неправомерной или случайной передачи данных, повлёкшей нарушение прав субъектов. А ст. 13.11 КоАП РФ содержит отдельный состав за невыполнение или несвоевременное выполнение обязанности уведомить уполномоченный орган — с миллионными санкциями для юридических лиц.

Юридически опасна не только сама утечка. Не менее опасно неправильное поведение организации после её обнаружения.

У клиники должен существовать заранее утверждённый алгоритм:

сотрудник обнаружил инцидент → сообщил ответственному → доступ ограничили → зафиксировали обстоятельства → определили состав данных и число затронутых лиц → подключили IT и юриста → выполнили предусмотренные законом уведомления → провели расследование → устранили причину.

Если персонал впервые обсуждает, «что делать при утечке», уже после отправки базы постороннему, — системы защиты нет, какой бы толстой ни была папка с политиками.

При этом клинике грозит не только штраф Роскомнадзора.

Нарушение конфиденциальности медицинской информации способно одновременно задействовать четыре вида ответственности:

- **Гражданско-правовая.** Пациент вправе защищать неприкосновенность частной жизни и изображение, требовать удаления информации, прекращения её распространения и компенсации морального вреда.
- **Административная**. Основные составы — ст. 13.11 КоАП РФ, размеры санкций после реформы выросли кратно.
- **Дисциплинарная**. Медицинский работник обязан соблюдать врачебную тайну; нарушение влечёт меры ответственности при соблюдении процедуры, установленной ТК РФ.
- **Уголовная**. Незаконное собирание или распространение сведений о частной жизни при определённых обстоятельствах образует состав ст. 137 УК РФ, а деяние с использованием служебного положения квалифицируется строже. С декабря 2024 года действует также ст. 272.1 УК РФ — об отдельных формах незаконного использования, передачи, сбора или хранения компьютерной информации с персональными данными, полученной незаконным путём.

Не каждая ошибка администратора превращается в уголовное дело. Но воспринимать данные пациентов как вопрос «бумажного согласия на стойке регистрации» сегодня уже невозможно.

Что рекомендуется проверить в клинике прямо сейчас:

Экспресс-аудит я начинаю не с папки «Персональные данные», а с реальных процессов. Прошу показать:

- куда медицинские работники отправляют фотографии исследований;
- используются ли личные телефоны для съёмки медицинской документации;
- через какие сервисы администраторы пересылают пациентам результаты;
- кто имеет доступ к МИС и сохранились ли доступы у уволенных сотрудников;
- куда выгружаются базы пациентов и какие облака используются;
- публикуются ли фотографии «до и после» и на каком основании;
- какие согласия реально подписывает пациент;
- у кого есть доступ к аккаунтам клиники в соцсетях;
- каким образом маркетолог получает фотографии пациентов;
- как клиника реагирует на негативные отзывы;
- существует ли инструкция на случай утечки;
- знает ли рядовой администратор, кому он обязан сообщить об инциденте.

Очень часто документы выглядят почти безупречно. А потом выясняется, что медицинский работник фотографирует историю болезни на личный телефон, администратор отправляет анализы из личного аккаунта, а SMM-специалист хранит снимки пациентов в своём облаке. Главный риск живёт именно в зазоре между локальным актом и реальным поведением сотрудников.

Что необходимо сделать руководителю:

Минимальная система защиты — это не одно «согласие на персональные данные», а несколько уровней.

- **Первое.** Составить карту обработки данных: какие данные клиника получает, откуда, с какой целью, где хранит, кому передаёт и когда уничтожает.
- **Второе.** Отдельно описать работу со специальными категориями — прежде всего со сведениями о состоянии здоровья.
- **Третье.** Установить правила фото- и видеосъёмки пациентов и отдельный порядок использования материалов для обучения, научных публикаций, сайта, соцсетей и рекламы.
- **Четвёртое.** Провести аудит всех мессенджеров, облачных сервисов и каналов передачи медицинской информации.
- **Пятое**. Пересмотреть разграничение доступа сотрудников к МИС и другим информационным системам.
- **Шестое**. Разработать настоящий, а не формальный план реагирования на инцидент.
- **И, наконец, седьмое** — обучить персонал. Потому что самая качественная политика бессмысленна, если администратор не видит проблемы в том, чтобы отправить фотографию паспорта пациента в общий рабочий чат.

Вместо вывода

Медицинские данные сегодня — один из самых юридически чувствительных активов клиники.

База пациентов содержит не просто фамилии и телефоны. Она раскрывает личность человека вместе с состоянием здоровья, диагнозами, операциями, интимными обстоятельствами, психиатрическими диагнозами, репродуктивной информацией. Последствия разглашения здесь несопоставимы с утечкой обычной клиентской базы.

Поэтому защита медицинских данных — не факультативная функция IT-специалиста и не папка, которую один раз собрали перед проверкой. Это элемент корпоративного управления и правовой безопасности организации.

Правило для руководителя я формулирую предельно просто.

Если информация о пациенте выходит за пределы того процесса, ради которого пациент передал её клинике, — остановитесь и ответьте на три вопроса: на каком правовом основании мы это делаем, кто получит доступ и что произойдёт, если эта информация станет публичной.

Иногда трёх вопросов достаточно, чтобы предотвратить утечку, многомиллионный штраф и судебный спор.

А как устроено у вас: медицинские работники и администраторы знают, какие данные пациента категорически нельзя отправлять в обычный рабочий чат?

Материал подготовлен *Ассоциацией по защите прав в сфере здравоохранения по запросу Ассоциации медицинских сестер России.*
Для консультаций и юридического сопровождения — обращайтесь к специалистам Ассоциации.