

Положение о работе с персональными данными пациентов в ООО «АРТО»

Оглавление:

1. Общие положения
2. Основные термины, понятия и определения
3. Принципы и цели обработки персональных данных
4. Состав персональных данных пациентов
5. Перечень действий с персональными данными и способы их обработки
6. Порядок осуществления операций с персональными данными
7. Ответственность за нарушение норм, регулирующих обработку персональных данных
8. Организация доступа к персональным данным. Пользователи персональных данных.
9. Функции Общества при осуществлении обработки персональных данных
10. Права и обязанности субъектов персональных данных
11. Меры, принимаемые Обществом для обеспечения выполнения обязанностей оператора при обработке персональных данных

1. Общие положения.

1.1. Настоящее Положение о работе с персональными данными в ООО «АРТО» (далее - Положение) определяет основные принципы, цели, условия и способы обработки персональных данных, перечни субъектов и обрабатываемых в ООО «АРТО» (далее – Общество, Клиника, Оператор) персональных данных, функции Общества при обработке персональных данных, права субъектов персональных данных, а также реализуемые в Обществе требования к защите персональных данных.

1.2. Положение разработано с учетом требований законодательных и иных нормативных правовых актов РФ в области обработки персональных данных.

1.3. Положение служит основой для разработки организационно-распорядительных документов Общества, регламентирующих процессы обработки персональных данных, а также меры по обеспечению безопасности персональных данных при их обработке в Обществе.

1.4. Настоящее Положение и изменения к нему утверждаются Генеральным директором Общества и вводятся приказом.

1.5. Настоящее Положение вступает в силу с даты утверждения приказом и действует до утверждения нового положения (или изменений).

2. Основные термины, понятия и определения.

В настоящем Положении используются следующие основные термины, понятия и определения:

- Персональные данные пациента – это любая информация, относящаяся к определенному или определяемому на основании такой информации пациенту, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы. Другая информация, необходимая Клинике в связи с оказанием медицинских услуг;
- Оператор – государственный или муниципальный орган, физическое или юридическое лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, состав персональных данных, а также определяющее цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными ;
- Субъект персональных данных – лицо, обратившееся за медицинской помощью, независимо от наличия у него заболевания и от ее состояния (далее – Пациент);
- Обработка персональных данных – сбор, систематизация, накопление, хранение, уничтожение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение персональных данных пациентов Клиники;
- Конфиденциальность персональных данных – обязательное для соблюдения назначенного ответственного лица, получившего доступ к персональным данным, требование не допускать их распространения без согласия или иного законного основания;
- Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо способом;
- Использование персональных данных – действия (операции) с персональными данными, совершаемые сотрудником Клиники в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПД либо иным образом затрагивающих их права и свободы или права и свободы других лиц;
- Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных субъекта ПД, в том числе их передачи;
- Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных пациентов или в результате которых уничтожаются материальные носители персональных данных пациентов;

- Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному пациенту;
- Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия пациента или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;
- Информация – сведения (сообщения, данные) независимо от формы их представления
- Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

3. Принципы и цели обработки персональных данных.

3.1. Общество, являясь оператором персональных данных, осуществляет обработку персональных данных пациентов Общества.

3.2. Обработка персональных данных в Обществе осуществляется с учетом необходимости обеспечения защиты прав и свобод субъектов персональных данных, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайну, на основе следующих принципов:

- обработка персональных данных осуществляется в Обществе на законной и справедливой основе;
- обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей;
- не допускается обработка персональных данных, несовместимая с целями сбора персональных данных;
- не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;
- обработке подлежат только персональные данные, которые отвечают целям их обработки;
- содержание и объем обрабатываемых персональных данных соответствует заявленным целям обработки. Не допускается избыточность обрабатываемых персональных данных по отношению к заявленным целям их обработки;
- при обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Общество принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных или неточных персональных данных;
- обрабатываемые персональные данные уничтожаются либо обезличиваются по достижению целей обработки или в случае утраты необходимости достижения этих целей, если иное не предусмотрено законодательством Российской Федерации.

3.3. Персональные данные в Обществе обрабатываются в целях:

- в целях оказания медицинских и медико-социальных услуг, обеспечения соблюдения законов и иных нормативных правовых актов при оказании;

- защиты жизни, здоровья или иных жизненно важных интересов субъектов персональных данных;
- исполнения судебных актов, актов других органов или должностных лиц, подлежащих исполнению в соответствии с законодательством Российской Федерации;
- заполнения статистической и иной документации в соответствии с нормативными актами.

3.4. В Обществе осуществляется обработка специальных категорий персональных данных о состоянии здоровья в соответствии с требованиями законодательства, а также с письменного согласия субъектов персональных данных.

3.5. Общество не осуществляет трансграничную передачу персональных данных.

4. Состав персональных данных пациентов.

4.1. В состав персональных данных пациентов Общества входят:

- ФИО, анкетные и биографические данные;
- биометрические и антропометрические данные;
- паспортные данные;
- место рождения, дата рождения
- сведения о социальных льготах;
- семейное положение;
- место работы, специальность;
- адрес фактического проживания, адрес прописки;
- домашний телефон, мобильный телефон;
- ИНН, СНИЛС;
- сведения страхового медицинского полиса ОМС;
- сведения о состоянии здоровья, перенесенных заболеваниях, имеющихся аллергических реакциях, случаях обращения за медицинской помощью, о прохождении углубленных медицинских обследований и медицинских осмотров, заключения и рекомендации врачей, и другую информацию.

4.2. Достоверность персональных данных определяется исходя из их изначального размещения в таких документах, как:

- паспорт или иной источник, удостоверяющий личность;
- свидетельство пенсионного страхования; либо документ, подтверждающий регистрацию в системе индивидуального (персонифицированного) учета, в том числе в форме электронного документа;
- свидетельство о браке;
- справка о наличии социальных льгот;
- физический носитель информации полиса ОМС, СНИЛС, ИНН.

Отдельным приказом руководителя Общества могут быть определены иные документы, которые рассматриваются как носители достоверных персональных данных.

Представление пациентом подложных документов или ложных сведений при оформлении документов для оказания медицинской помощи является основанием для отказа в оказании медицинской помощи.

5. Перечень действий с персональными данными и способы их обработки.

Настоящее Положение устанавливает, что Общество осуществляет следующие операции с персональными данными пациентов:

- сбор;
- запись;
- систематизация;
- накопление;
- хранение;
- уточнение (обновление, изменение);
- извлечение;
- использование;
- передача (распространение, предоставление, доступ);
- обезличивание;
- блокирование;
- удаление;
- уничтожение.

6. Порядок осуществления операций с персональными данными.

6.1. Получение и обработка персональных данных пациентов

Сбор персональных данных осуществляется в пределах установленного объема, необходимого для каждой категории субъектов, с которыми взаимодействует Общество, и не может превышать указанный объем.

Общество обеспечивает защиту персональных данных от неправомерного использования или утраты.

Получение персональных данных (документов, на которых они зафиксированы) осуществляется непосредственно от пациентов при посещении клиники. В случае если предоставление соответствующих данных возможно только от третьих лиц, то пациент должен дать письменное согласие на это.

Общество обязано сообщить пациенту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа пациента дать письменное согласие на их получение.

Общество не имеет право получать и обрабатывать персональные данные пациента о его политических, религиозных и иных убеждениях и частной жизни.

Общество не имеет право получать и обрабатывать персональные данные

пациента о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

Обработка персональных данных в Обществе осуществляется следующими способами:

- неавтоматизированная обработка персональных данных (вручную);
- автоматизированная обработка персональных данных;
- смешанная обработка персональных данных.

6.2. Хранение персональных данных пациентов

Персональные данные пациентов предоставляются Обществу после получения соответствующего информированного согласия пациентов на обработку их персональных данных. Персональные данные пациентов содержатся в информационных системах персональных данных, представляющих собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств. В информационных системах персональные данные могут быть размещены на материальных, в том числе бумажных носителях (медицинская карта пациента, иные медицинские документы).

Работа с информационными системами персональных данных, материальными носителями, в том числе с медицинской документацией, содержащими персональные данные пациентов осуществляется в специально отведённых для этого помещениях.

Доступ к электронным базам данных, содержащим персональные данные пациентов, обеспечивается двухступенчатой системой паролей: на уровне локальной компьютерной сети и на уровне баз данных. Пароли устанавливаются Генеральным директором Общества и сообщаются индивидуально работникам, имеющим доступ к персональным данным.

Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей соблюдаются условия, обеспечивающие сохранность персональных данных и исключают несанкционированный к ним доступ.

Персональные данные клиентов на бумажных носителях, если с них не снят на законном основании режим конфиденциальности, хранятся в специально отведенном кабинете. Ключи от кабинета/шкафов хранятся соответствующего специалиста, допущенного к обработке персональных данных клиентов.

Персональные данные пациентов содержатся в следующих группах документов:

- договор оказания услуг психолога;
- договор оказания медицинских услуг и все приложения к нему;
- договоры о криоконсервации и хранении биоматериала;
- анкета о здоровье;
- медицинская карта;
- информированные согласия на различные виды медицинских манипуляций;
- протоколы фиксации претензий пациента, журналы учета
- акты выполненных работ/оказанных услуг,
- других медицинских документах.

6.3. Использование персональных данных пациентов

Использование персональных данных пациента осуществляется исключительно в целях оказания медицинских и медико-социальных услуг, обеспечения соблюдения законов и иных нормативных правовых актов.

Персональные данные пациентов предоставляются Обществу после получения соответствующего информированного согласия пациентов на обработку их персональных данных.

Согласие на обработку персональных данных может быть отозвано пациентом.

Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.

6.4. Срок обработки и хранения персональных данных.

Срок обработки персональных данных — это период от начала обработки данных до ее прекращения. Срок обработки данных начинается с начала действия договора на оказание медицинских услуг и дачи согласия на обработку.

Дата прекращения обработки персональных данных (за исключением хранения) определяется моментом наступления одного из событий:

- расторгнут Договор на оказание медицинских услуг;
- достигнута цель обработки;
- истек срок действия согласия субъекта или он отозвал согласие на обработку данных;
- обнаружена несанкционированная обработка данных;
- прекращение деятельности Общества.

Общество уничтожает персональные данные пациента, за исключением данных, содержащихся в медицинской карте и иной медицинской документации, в следующие сроки: в течение 30 рабочих дней с момента отзыва согласия на обработку при условии завершения расчетов между клиникой и пациентом.

После истечения нормативных сроков хранения персональные данные стираются с информационных носителей, либо уничтожаются сами носители (в том числе и бумажные) на которых храниться информация.

6.5. Передача и распространение персональных данных пациентов

Передача персональных данных пациента осуществляется с учетом

специфики конкретной информационной системы:

- в цифровой информационной системе (предназначенной для автоматизированной обработки персональных данных) передача данных осуществляется по защищенным каналам связи, а также при задействовании средств криптозащиты;

- в информационной системе на основе бумажных носителей передача данных осуществляется посредством перемещения или копирования содержимого данных носителей при участии пациентов Общества, имеющих доступ к соответствующей информационной системе, который устанавливается отдельным локальным правовым актом.

При передаче персональных данных пациента Общество должно соблюдать следующие требования:

при передаче персональных данных пациент должен дать на это согласие в письменной или электронной форме.

оператор вправе передать информацию, которая относится к персональным данным пациента, без его согласия, если такие сведения нужно передать по запросу государственных органов, в порядке, установленном законодательством. общество не вправе предоставлять персональные данные пациента третьей стороне без письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью пациента, а также в случаях, установленных законодательством.

Согласие на обработку персональных данных, разрешенных пациентом для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

В случае если из предоставленного пациентом согласия на распространение персональных данных не следует, что пациент согласился с распространением персональных данных, такие персональные данные обрабатываются без права распространения.

В согласии на распространение персональных данных пациент вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных работодателем неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц.

Передача (распространение, предоставление, доступ) персональных данных, разрешенных пациентом для распространения, должна быть прекращена в любое время по его требованию. Данное требование должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) пациента, а также перечень персональных данных, обработка которых подлежит прекращению.

Пациент вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее

разрешенных для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения положений Федерального закона от 27.07.2006 № 152-ФЗ или обратиться с таким требованием в суд. Общество или третье лицо обязано прекратить передачу (распространение, предоставление, доступ) персональных данных в течение трех рабочих дней с момента получения требования пациента или в срок, указанный во вступившем в законную силу решении суда.

6.6. Блокирование и уничтожение персональных данных.

Блокирование персональных данных в Обществе осуществляется с учетом специфики конкретной информационной системы:

- в цифровой информационной системе блокирование данных осуществляется посредством закрытия доступа к файлам при задействовании средств криптозащиты;
- в информационной системе на основе бумажных носителей блокирование данных осуществляется посредством закрытия доступа к соответствующей информационной системе для определенных групп пациентов.

6.7. Уничтожение персональных данных осуществляется с учетом специфики конкретной информационной системы:

- в цифровой информационной системе ликвидация данных осуществляется посредством их удаления с ПК, а также серверов;
- в информационной системе на основе бумажных носителей ликвидация данных осуществляется посредством уничтожения соответствующих носителей с помощью специальных технических средств.

7. Ответственность за нарушение норм, регулирующих обработку персональных данных.

7.1. Лица, виновные в нарушении положений законодательства РФ в области персональных данных при обработке персональных данных пациента, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к административной, гражданско-правовой или уголовной ответственности в порядке, установленном федеральными законами.

7.2. Моральный вред, причиненный пациенту вследствие нарушения его прав, нарушения правил обработки персональных данных, а также несоблюдения требований к защите персональных данных, установленных Федеральным законом от 27.07.2006 N 152-ФЗ, подлежит возмещению в соответствии с законодательством РФ. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных пациентом убытков.

8. Организация доступа к персональным данным. Пользователи персональных данных.

8.1. Доступ к персональным данным пациентов, не требующий подтверждения и не подлежащий ограничению, имеют:

Внутренний доступ (доступ внутри организации):

главный врач;

врачи – к персональным данным пациентов при осуществлении амбулаторного приема, стационарном лечении;

сотрудники регистратур, администраторы;

медсестры;

работники бухгалтерии – к тем данным, которые необходимы для выполнения конкретных функций;

Внешний доступ. Массовые потребители персональных данных вне организации государственные и негосударственные функциональные структуры:

страховые медицинские организации;

аптечные организации;

лаборатории (медико -генетические);

разработчики баз данных и информационных систем клиники;

криобанки биологического материала;

фонд ОМС;

военкоматы;

органы внутренних дел, суда, прокуратуры.

8.2. Доступ к персональным данным пациентов для иных лиц может быть разрешен только отдельным распоряжением руководителя.

8.3. Работники Общества и другие лица, имеющие доступ к персональным данным, обязаны:

- осуществлять операции с персональными данными при соблюдении норм, установленных настоящим Положением, а также действующим законодательством Российской Федерации;

- информировать своего непосредственного руководителя и руководителя Общества о нештатных ситуациях, связанных с операциями с персональными данными;

- обеспечивать конфиденциальность операций с персональными данными;

- обеспечивать сохранность и неизменность персональных данных в случае, если выполняемая задача не предполагает их корректировки или дополнения.

8.4. Персональные данные пациента могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого пациента.

9. Функции Общества при осуществлении обработки персональных данных

Общество при осуществлении обработки персональных данных выполняет следующие функции:

9.1. Принимает меры, необходимые и достаточные для обеспечения выполнения требований законодательства Российской Федерации и локальных нормативных актов Общества в области обработки персональных данных.

9.2. Принимает правовые, организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также иных неправомерных действий в отношении персональных данных.

9.3. Назначает лицо, ответственное за организацию обработки персональных данных в Обществе.

9.4. Издаёт локальные нормативные акты, определяющие политику и вопросы обработки и защиты персональных данных в Обществе.

9.5. Сообщает в установленном порядке субъектам персональных данных или их представителям информацию о наличии персональных данных, относящихся к соответствующим субъектам, предоставляет возможность ознакомления с этими персональными данными при обращении и (или) поступлении запросов указанных субъектов персональных данных или их представителей, если иное не установлено законодательством Российской Федерации.

9.6. Прекращает обработку и уничтожает персональные данные в случаях, предусмотренных законодательством Российской Федерации.

9.7. Совершает иные действия, предусмотренные законодательством Российской Федерации в области обработки персональных данных.

10. Права и обязанности субъектов персональных данных.

Субъекты персональных данных имеют право на:

10.1. Полную информацию об их персональных данных, обрабатываемых в Обществе.

10.2. Доступ к своим персональным данным, включая право на бесплатное получение копии любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных законодательством Российской Федерации.

10.3. Уточнение своих персональных данных, их блокирование или уничтожение в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки.

10.4. Отзыв согласия на обработку персональных данных.

10.5. Принятие предусмотренных законодательством Российской Федерации мер по защите своих прав.

10.6. Обжалование действия или бездействия Общества, осуществляемого с нарушением требований законодательства Российской Федерации в области персональных данных, в уполномоченный орган по защите прав субъектов персональных данных или суд.

10.7. Получение сведений о наименовании и месте нахождения оператора, сведения о лицах (за исключением пациентов оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона.

10.8. Требование прекратить в любое время передачу (распространение, предоставление, доступ) персональных данных, разрешенных для распространения. Требование оформляется в письменном виде. Оно должно включать в себя фамилию, имя, отчество (при наличии), контактную информацию (номер телефона, адрес электронной почты или почтовый адрес) пациента, а также перечень персональных данных, обработка которых подлежит прекращению.

10.9. Определение своих представителей для защиты своих персональных данных;

10.10. Сохранение и защиту своей личной жизни и семейной тайны.

10.11. Пациент обязан передавать комплекс достоверных, документированных персональных данных, а также своевременно сообщать об изменениях своих персональных данных.

10.12. Пациент ставит клинику в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в медицинской документации на основании представленных документов.

11. Меры, принимаемые Обществом для обеспечения выполнения обязанностей оператора при обработке персональных данных.

11.1. Меры, необходимые и достаточные для обеспечения выполнения Обществом обязанностей оператора, предусмотренных законодательством Российской Федерации в области обработки персональных данных, включают:

- назначение лица, ответственного за организацию обработки персональных данных в Обществе;
- принятие локальных нормативных актов и иных документов в области обработки и защиты персональных данных;
- проведение методической работы с работниками Общества, занимающими должности, включенные на основании приказа Общества в перечень должностей структурных подразделений Общества, при замещении которых осуществляется обработка персональных данных;
- получение согласий субъектов персональных данных на обработку персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации;
- установление запрета на передачу персональных данных по открытым каналам связи, вычислительным сетям вне пределов контролируемой зоны, сети Интернет без применения установленных в Обществе мер по обеспечению

безопасности персональных данных (за исключение общедоступных и (или) обезличенных персональных данных);

- хранение материальных носителей персональных данных с соблюдением условий, обеспечивающих их сохранность и исключающих несанкционированный доступ к ним;

11.2. Меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных устанавливаются в соответствии с требованиями законодательных и иных нормативных правовых актов Российской Федерации, локальных нормативных актов Общества, регламентирующих вопросы обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных Общества.

11.3. Лицо, ответственное за организацию обработки персональных данных и назначаемое приказом Общества, получает указания от руководства Общества и подотчетно ему.

11.4. Лицо, ответственное за организацию обработки персональных данных, в частности, обязано организовывать:

- внутренний контроль за соблюдением работниками Общества законодательства Российской Федерации в области обработки персональных данных, в том числе требований к защите персональных данных;

- доведение до сведения пациентов Общества положений законодательства Российской Федерации, локальных нормативных актов Общества в области обработки персональных данных, в том числе требований к защите персональных данных;

- контроль за приемом и обработкой обращений и запросов субъектов персональных данных или их представителей.

12. Изменения и дополнения к Положению утверждаются приказом по Обществу.

13. Любые обращения, касающиеся обработки ПДн, направляются на электронную почту: lime877@yandex.ru, либо на почтовый адрес: 105062, г.Москва, Подсосенский переулок дом 3