ООО «ИДЕАЛ»

Утверждаю

Директор А.Н. Кузьмин

01 марта 2021 год

Положение по обработке и защите персональных данных работников и пациентов ООО «Идеал».

1. Общие положения.

1.1. Настоящее положение действует в отношении всех персональных данных, которые Общество с ограниченной ответственностью «ИДЕАЛ» (далее – ООО «ИДЕАЛ», Медицинская организация) может получить от субъектов персональных данных.

1.2. Положение распространяется на персональные данные, полученные как до, так и после утверждения настоящего Положения.

1.3. Действие Положения распространяется на все процессы Медицинской организации, связанные с обработкой персональных данных.

1.4. Целью настоящего Положения является определение порядка обработки персональных данных работников и пациентов ООО «ИДЕАЛ» и иных субъектов персональных данных, персональные данные которых подлежат обработке, на основании полномочий оператора; обеспечение защиты прав и свобод человека и гражданина, в т.ч. работника медицинской организации, при обработке его персональных данных в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.5. Положение обязательно для ознакомления и исполнения всеми лицами, допущенными к обработке персональных данных в информационной системе персональных данных, на материальных носителях ООО «ИДЕАЛ».

1.6. Сотрудники ООО «ИДЕАЛ», допущенные к обработке персональных данных работников, контрагентов и клиентов (пациентов) ООО «ИДЕАЛ», несут персональную ответственность за нарушение положений настоящего Положения, иных локальных нормативных актов ООО «ИДЕАЛ» по вопросам обработки персональных данных, а также законодательства Российской Федерации по вопросам обработки и защиты персональных данных.

1.7. Настоящее Положения действует бессрочно, до его замены, что оформляется отдельным приказом директора ООО «Идеал». Текущая редакция Положения размещается на сайте Медицинской организации в общем доступе.

2. Правовые основания обработки персональных данных.

2.1. ООО «ИДЕАЛ» осуществляет обработку персональных данных работников и клиентов (пациентов) в соответствии с:

- Конституцией Российской Федерации,
- статьями 86-90 Трудового кодекса Российской Федерации,
- Федеральным законом №149-ФЗ от 27.07.2006 «Об информации, информационных технологиях и о защите информации»,
- Указом Президента РФ от 06.03.1997 №188,
- Федеральным законом №323-ФЗ от 21.11.2011 «Об основах охраны здоровья граждан в Российской Федерации»,
- Федеральным законом №152-ФЗ от 27.07.2006 «О персональных данных»,
- Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,
- Постановлением Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»,
- Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,
- Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»,
- Приказом Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»,
- Постановлением Правительства РФ от 04.10.2012 № 1006 «Об утверждении Правил предоставления медицинскими организациями платных медицинских услуг»;
- Приказом Минздравсоцразвития России от 22.11.2004 № 255 «О порядке оказания первичной медико-санитарной помощи гражданам, имеющим право на получение набора социальных услуг»;
- Приказом ФМБА РФ от 30.03.2007 № 88 «О добровольном информированном согласии на медицинское вмешательство»;
- Приказом Министерства здравоохранения РФ от 14.09.2020 № 972н "Об утверждении Порядка выдачи медицинскими организациями справок и медицинских заключений;
- и иных нормативных правовых актов Российской Федерации и нормативных документов уполномоченных органов государственной власти.

3. Термины и определения, используемые в настоящем Положении.

3.1. Для целей настоящего Положения в тексте применяются следующие термины и определения:

- **персональные данные работника**- информация, необходимая ООО «Идеал» в связи с трудовыми отношениями и касающаяся конкретного работника.

- **персональные данные пациента**- информация, полученная медицинской организацией при первоначальном поступлении пациента, при заключении с пациентом договора на оказание медицинских услуг, а также информация, полученная в процессе лечения.

- **врачебная тайна** – соблюдение конфиденциальности информации о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иных сведений, полученных при его обследовании и лечении;

- **оператор в соответствии с данным Положением** -ООО «Идеал», самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными работников и пациентов;

- **обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

- **автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники;

- **распространение персональных данных** - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

- **предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

- **блокирование персональных данных** - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

- **уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

- **обезличивание персональных данных** - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

- **использование персональных данных** - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц;

- **информационная система персональных данных** - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

- **конфиденциальность персональных данных** - обязательное для соблюдения организацией-оператором или иным получившим доступ к персональным данным лицом

требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания;

- **общедоступные персональные данные** - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности;

- н**есанкционированный доступ (несанкционированные действия)** - доступ к информации или действия с информацией, нарушающие правила разграничения доступа, в том числе с использованием штатных средств, предоставляемых информационными системами персональных данных.

4. Перечень персональных данных, обрабатываемых в Медицинской организации.

4.1. Перечень персональных данных, обрабатываемых в ООО «ИДЕАЛ», определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами Медицинской организации с учетом целей обработки персональных данных, указанных в настоящем Положении.

4.2. Медицинской организацией обрабатываются следующие персональные данные субъектов персональных данных:

4.2.1.) Персональные данные работников и кандидатов на прием на работу в составе:

- фамилия, имя, отчество;
- дата рождения;
- гражданство;
- номер страхового свидетельства;
- ИНН;
- знание иностранных языков;
- данные об образовании (номер, серия дипломов, год окончания);
- данные о приобретенных специальностях;
- семейное положение;
- данные о членах семьи (степень родства, Ф. И. О., год рождения, паспортные данные, включая прописку и место рождения);
- фактическое место проживания;
- контактная информация;
- данные о военной обязанности;
- данные о текущей трудовой деятельности (дата начала трудовой деятельности, кадровые перемещения, оклады и их изменения, сведения о поощрениях, данные о повышении квалификации и т. п.).

4.2.2.) персональные данные клиентов (пациентов) в составе:

- анкетные данные (фамилия, имя, отчество, число, месяц, год рождения и др.);
- паспортные данные;
- адрес регистрации;
- адрес места жительства;
- данные о состоянии здоровья;
- сведения о социальных льготах;
- иные сведения, необходимые в соответствии с законодательством для оказания медицинской помощи в соответствии с профилем медицинской организации

4.2.3.) Персональные данные контрагентов в составе:

- фамилия, имя, отчество физического лица-уполномоченного представителя контрагента;
- наименование юридического лица;

- ИНН; государственный регистрационный номер (ОГРН, ОГРНИП);
- адрес; контактный телефон;
- номер банковского счета;
- сведения о заключаемом с контрагентом договоре.

4.3. Основанием для обработки персональных данных субъекта, не являющегося работником Медицинской организации или лицом, заключившим с Медицинской организацией договор, является согласие в письменной форме субъекта персональных данных на обработку его персональных данных или добровольное размещение непосредственно субъектом персональных данных своих персональных данных в общедоступных источниках информации, включая корпоративный сайт Медицинской организации.

4.4. Субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе.

4.5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям обработки.

5. Перечень субъектов, персональные данные которых обрабатываются в Медицинской организации.

5.1. Медицинской организацией осуществляется обработка полученных в установленном законом порядке персональных данных принадлежащих:

- работникам Медицинской организации и кандидатам на прием в Медицинскую организацию на работу;
- клиентам (пациентам) Медицинской организации;
- физическим лицам, в том числе потенциальным клиентам, представителям клиентов, уполномоченным представлять клиентов, в том числе пользователям корпоративного сайта Медицинской организации;
- контрагентам Медицинской организации (физическим и юридическим лицам, их уполномоченным представителям, работникам партнеров Медицинской организации) и другим лицам, имеющим договорные отношения с Медицинской организацией, с которыми взаимодействуют работники Медицинской организации в рамках своей деятельности

6. Принципы и цели обработки Медицинской организацией персональных данных.

6.1. ООО «Идеал», являясь оператором персональных данных, осуществляет обработку персональных данных работников Медицинской организации, контрагентов (сотрудничающих в рамках гражданско-правовых договоров), клиентов (пациентов) ООО «ИДЕАЛ», обратившихся с целью получения медицинских услуг.

6.2. Обработка персональных данных Медицинской организацией осуществляется с учетом необходимости обеспечения защиты прав и свобод работников, клиентов (пациентов) и других субъектов персональных данных, в том числе защиты права на неприкосновенность частной жизни, личную и семейную тайну, врачебную тайну на основе следующих принципов:

- обработка персональных данных осуществляется 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 обеспечиваются точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Медицинской организацией принимаются необходимые меры либо обеспечивается их принятие по удалению или уточнению неполных или неточных персональных данных;

- хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем того требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

- обрабатываемые персональные данные уничтожаются либо обезличиваются по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

6.3. Персональные данные обрабатываются Медицинской организацией в следующих целях:

- обеспечения соблюдения Конституции Российской Федерации, законодательных и иных нормативных правовых актов Российской Федерации, локальных нормативных актов Медицинской организации;

- осуществления функций, полномочий и обязанностей, возложенных законодательством Российской Федерации на Медицинскую организацию, в том числе по предоставлению персональных данных в органы государственной власти, в Пенсионный фонд Российской Федерации, в Фонд социального страхования Российской Федерации, в Федеральный фонд обязательного медицинского страхования, в органы статистики, а также в иные государственные органы;

- ведения текущего бухгалтерского, налогового, управленческого, финансового, кадрового, статистического учета; формирования и представления отчетности в соответствующие контролирующие органы;

- защиты жизни, здоровья или иных жизненно важных интересов субъектов персональных данных;

- подготовки, заключения, исполнения и прекращения договоров с контрагентами, клиентами (пациентами) Медицинской организации;

- исполнения судебных актов, актов других органов или должностных лиц, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

- осуществления прав и законных интересов Медицинской организации в рамках осуществления видов деятельности, предусмотренных Уставом и иными локальными нормативными актами Медицинской организации, или третьих лиц либо достижения общественно значимых целей;

- в иных законных целях.

6.4. Обработка Медицинской организацией персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем.

6.5. Обработка персональных данных необходима для информационного обеспечения Медицинской организации и клиентов (пациентов).

6.6. Обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

7. Сбор, обработка и хранение персональных данных работников.

7.1 Сбор, обработка и хранение персональных данных работников. Порядок получения персональных данных.

7.1.1. Все персональные данные работника Медицинской организации следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо работодателя должно сообщить работнику Медицинской организации о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

7.1.2. Работодатель не имеет права получать и обрабатывать персональные данные работника Медицинской организации о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

Обработка указанных персональных данных работников работодателем возможна без согласия субъекта персональных данных только в случаях, поименованных в Федеральном законе от 27.07.2006 № 152-ФЗ "О персональных данных"

7.1.3. В остальных случаях работодатель вправе обрабатывать персональные данные работников только с их письменного согласия.

7.1.4. Письменное согласие работника на обработку своих персональных данных должно включать в себя:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта персональных данных.

7.2. Порядок обработки, передачи и хранения персональных данных.

7.2.1. Работник Медицинской организации предоставляет работнику отдела кадров Медицинской организации достоверные сведения о себе. Работник отдела кадров Медицинской организации проверяет достоверность сведений, сверяя данные, предоставленные работником, с имеющимися у работника документами.

7.2.2. В соответствии со главой 14 Трудового кодекса РФ в целях обеспечения прав и свобод человека и гражданина директор ООО «Идеал» (Работодатель) и его представители при обработке персональных данных работника должны соблюдать следующие общие требования:

7.2.2.1. Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

7.2.2.2. При определении объема и содержания, обрабатываемых персональных данных Работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

7.2.2.3. При принятии решений, затрагивающих интересы работника, Работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

7.2.2.4. Защита персональных данных работника от неправомерного их использования или утраты обеспечивается Работодателем за счет его средств в порядке, установленном федеральным законом.

7.2.2.5. Работники и их представители должны быть ознакомлены под расписку с документами Работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

7.2.2.6. Во всех случаях отказ работника от своих прав на сохранение и защиту тайны недействителен.

7.3. Хранение и использование персональных данных работников:

7.3.1. Персональные данные работников обрабатываются и хранятся в отделе кадров.

7.3.2. Персональные данные работников могут быть получены, проходить дальнейшую обработку и передаваться на хранение как на бумажных носителях, так и в электронном виде - локальной компьютерной сети и компьютерной программе.

7.3.2. При получении персональных данных не от работника (за исключением случаев, если персональные данные были предоставлены работодателю на основании федерального закона или если персональные данные являются общедоступными) работодатель до начала обработки таких персональных данных обязан предоставить работнику следующую информацию:

- наименование (фамилия, имя, отчество) и адрес оператора или его представителя;
- цель обработки персональных данных и ее правовое основание;
- предполагаемые пользователи персональных данных;
- установленные Федеральным закономот 27.07.2006 № 152-ФЗ "О персональных данных" права субъекта персональных данных.

8. Сбор, обработка и хранение персональных данных клиентов (пациентов).

8.1. В целях обеспечения прав и свобод человека и гражданина лица, участвующие в обработке персональных данных пациента, обязаны соблюдать следующие общие требования:

- обработка персональных данных пациента может осуществляться лицами, имеющими допуск исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, контроля количества и качества выполняемой работы;

- при определении объема и содержания обрабатываемых персональных данных пациента лица, участвующие в процессе обработки, должны руководствоваться Конституцией РФ, Федеральным законом РФ от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федеральным закономот 27.07.2006 № 152-ФЗ "О персональных данных"- все персональные данные пациента следует получать у него самого или у его представителя, полномочия которого следуют из закона (законный представитель) либо должны быть подтверждены нотариально.

8.2. Если персональные данные пациента возможно получить только у третьей стороны, то пациент должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Указанный пункт имеет отношение только к пациентам, достигшим совершеннолетия.

8.3.Работник Медицинскойорганизации должен 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.

8.4. Защита персональных данных пациента от неправомерного их использования или утраты должна быть обеспечена Медицинскойорганизацией за счет своих средств в порядке, установленном федеральным законом.

8.5. Пациенты и их представители должны быть ознакомлены под роспись с документами Медицинской организации, устанавливающими порядок обработки персональных данных пациента, а также об их правах и обязанностях в этой области.

8.6. Обработка, передача и хранение персональных данных пациента:

8.6.1. Все действия по обработке персональных данных пациента осуществляются только работниками Медицинскойорганизации.Допуск к работе с персональными данными пациентаосуществляется на основании приказа директора Медицинской организации в котором утвержден перечень должностей.

Обработка персональных данных осуществляется только в объеме, необходимом данным лицам для оказания медицинской услуги.

8.6.2. Поскольку сведения о пациентах содержат в том числе специальную категорию персональных данных, то обработка персональных данных осуществляется с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

4) цель обработки персональных данных;

5) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

6) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

8) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;

9) подпись субъекта персональных данных.

8.7. Этапность получения и обработки персональных данных пациента.

8.7.1. При первичном посещении Медицинскойорганизациипациентом информация заносится в базу данных в регистратуре. На этом этапе регистратор отмечает паспортные данные, контактный телефон, место работы и должность, Ф.И.О специалиста к которому желает попасть пациент. Оформляется амбулаторная карта, которая является основным документом, содержащим персональные данные пациента, в которой фиксируются выше перечисленные персональные данные. Информация о пациенте хранится как на электронном, так и на бумажном носителе информации о персональных данных. Регистратор не вправе получать информацию о состоянии здоровья пациента. Ответственным на данном этапе хранения персональных данных является регистратор, фиксирующий персональные данные.

8.7.2. Амбулаторная карта передается врачу. Врач собирает информацию о состоянии здоровья пациента, фиксирует в амбулаторную карту. Ответственным за неразглашения информации о состоянии здоровья является врач. При передаче персональных данных пациента врач должен соблюдать следующие требования:

- не сообщать персональные данные третьей стороне без письменного согласия пациента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью пациента, а также в случаях, установленных федеральным законом;

- не сообщать персональные данные пациента в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные пациента, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные пациента, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными пациента в порядке, установленном федеральными законами;

- разрешать доступ к персональным данным пациента только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные пациента, которые необходимы для выполнения конкретных функций.

8.7.3. По окончании приема медицинская карта сдается врачом-специалистом в регистратуру Медицинскойорганизации.

8.7.4. После получения медицинских услуг носитель, содержащий персональные данные о состоянии здоровья, диагнозе, проведенном лечении и рекомендациях хранится в регистратуре медицинского центра.

8.8. Все меры конфиденциальности при сборе, обработке и хранении персональных данных пациента распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.

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

8.10. С работниками, ответственными за хранение персональных данных, а также с работниками, владеющими персональными данными в силу своих должностных обязанностей, заключаются Соглашения о неразглашении персональных данных пациентов. Экземпляр Соглашения хранится в отделе кадров. В должностные инструкции данных работников включается пункт об обязанности сохранения врачебной тайны.

8.11. Автоматизированная обработка и хранение персональных данных пациентов допускаются только после выполнения всех основных мероприятий по защите информации.

8.12. Журналы и другие формы медицинской документации, находящиеся в обработке и содержащие персональные данные пациентов, оформляются и хранятся в подразделениях медицинского центра в соответствии с требованиями действующих локальных приказов.

Прочие документы, используемые при оказании медицинской помощи и содержащие персональные данные пациентов (акты, направления, договоры, квитанции и пр.), после оформления передаются работнику, допущенному к работе с персональными данными, в должностные обязанности которого входит обработка этих данных.

Хранение оконченных производством документов, содержащих персональные данные пациентов, осуществляется в архиве Медицинской организации.

8.13. Помещения, в которых хранятся персональные данные пациента, должны быть оборудованы надежными замками.

8.14. Проведение уборки помещения должно производиться в присутствии ответственного лица.

9. Обязанности медицинской организации по хранению и защите персональных данных работников и пациентов

9.1. Медицинская организация обязана за свой счет обеспечить защиту персональных данных работников и пациентов от неправомерного использования или утраты в порядке, установленном законодательством РФ.

9.2. Медицинская организация обязана принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным закономот 27.07.2006 № 152-ФЗ "О персональных данных"и принятыми в соответствии с ним нормативными правовыми актами. Медицинская организация самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. К таким мерам могут, в частности, относиться:

- назначение ответственного за организацию обработки персональных данных;
- издание документов, определяющих его политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;
- осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;
- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;
- ознакомление работников медицинской организации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении

обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

9.3. Медицинская организация обязана ознакомить работников и их представителей с настоящим Положением и их правами в области защиты персональных данных под расписку.

9.4. Медицинская организация обязана осуществлять передачу персональных данных работников и пациентов только в соответствии с настоящим Положением и законодательством РФ.

9.5. Медицинская организация обязана предоставлять персональные данные работников и пациентов только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей, в соответствии с настоящим Положением и законодательством РФ.

9.6. Медицинская организация не вправе получать и обрабатывать персональные данные работников и пациентов о их политических, религиозных и иных убеждениях и частной жизни.

В случаях, непосредственно связанных с вопросами трудовых отношений, медицинская организация вправе получать и обрабатывать персональные данные работников о их личной жизни, только с письменного согласия работников.

9.7. Медицинская организация не имеет права получать и обрабатывать персональные данные работников о их членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных законодательством РФ.

9.8. Медицинская организация не вправе предоставлять персональные данные работников и пациентов в коммерческих целях без их письменного согласия.

9.9. Медицинская организация обязана обеспечить работникам и пациентам свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных законодательством.

9.10. Медицинская организация обязана по требованию работников и пациентов предоставить им полную информацию о их персональных данных и обработке этих данных.

10. Право субъекта персональных данных на доступ к его персональным данным.

10.1. Субъект персональных данных вправе требовать от Медицинской организации уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

10.2. Сведения предоставляются субъекту персональных данных или его представителю Медицинской организацией при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Медицинской организацией (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Медицинской организацией, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации Федерального закона от 06.04.2011 № 63-ФЗ "Об электронной подписи".

10.3 Медицинская организация вправе отказать субъекту персональных данных в выполнении повторного запроса. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Медицинской организации.

10.4. Если субъект персональных данных считает, что Медицинская организация осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Медицинской организации в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

10.5. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

11. Доступ к персональным данным работников и клиентов (пациентов).

11.1. Доступ к персональным данным предоставляется только тем работникам Медицинской организации, которые указаны в перечне должностей, утвержденных приказом директора Медицинской организации, для исполнения их непосредственных должностных обязанностей.

11.2. Сведения о субъекте персональных данных могут быть предоставлены другой организации только с письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления субъекта персональных данных.

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

11.4. Работник Медицинской организации допускается к обработке персональных данных только после ознакомления с действующими нормативными правовыми актами, регламентирующими обработку персональных данных, локальными нормативными актами Медицинской организации, регламентирующими обработку персональных данных, и после подписания обязательства о неразглашении информации, содержащей персональные данные.

12. Уничтожение персональных данных.

12.1. В случае достижения целей обработки персональных данных Медицинская организация прекращает их обработку и уничтожает персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено соглашением между Медицинской организацией и субъектом персональных данных.

12.2. В случае отзыва субъектом персональных данных согласия на обработку своих персональных данных Медицинской организацией последняя прекращает их обработку, если иное не предусмотрено соглашением между Медицинской организацией и субъектом персональных данных, либо если Медицинская организация вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных действующим законодательством, регулирующим процессы обработки персональных данных.

12.3. В случае выявления неправомерной обработки персональных данных Медицинская организация предпринимает меры по уничтожению этих персональных данных в срок, не превышающий трех рабочих дней со дня выявления неправомерной обработки персональных данных.

12.4. В случае если обеспечить правомерность обработки персональных данных невозможно, Медицинская организация в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязана уничтожить такие персональные данные или обеспечить их уничтожение. В случае отсутствия

возможности уничтожения персональных данных в течение указанного срока, Медицинская организация осуществляет блокирование таких персональных данных и обеспечивает их уничтожение в срок, не превышающий 6 месяцев со дня выявления неправомерной обработки персональных данных, если иной срок не установлен действующим законодательством или иными нормативными правовыми актами, регулирующими процессы обработки персональных данных.

12.5. В случае обращения субъекта персональных данных с заявлением об уничтожении его персональных данных, Медицинская организация обязана прекратить обработку или обеспечить прекращение обработки персональных данных данного субъекта и уничтожить указанные в заявлении персональные данные в срок, не превышающий тридцати дней с момента подачи субъектом персональных данных соответствующего заявления, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Медицинской организацией и субъектом персональных данных.

12.6. Персональные данные на бумажных носителях уничтожаются с помощью средств, гарантирующих невозможность восстановления носителя.

12.7. Уничтожение информации с машиночитаемых носителей персональных данных производится способом, исключающим возможность использования и восстановления информации.

12.8. По факту уничтожения персональных данных Медицинской организацией составляется акт, который подписывается директором Медицинской организации или иным лицом, на которого соответствующим приказом возложены обязанности. Заверенная копия указанного акта выдается субъекту персональных данных.

13. Ответственность за нарушение норм, регулирующихобработку и защиту персональных данных.

Персональная ответственность - одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы.

13.1. Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

13.2. Каждый сотрудник, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

13.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут в соответствии с федеральными законами ответственность:

- дисциплинарную (замечание, выговор, увольнение);
- административную (предупреждение или административный штраф);
- гражданско-правовую (возмещение причиненного убытка);
- уголовной ответственности.

14. Заключительные положения.

14.1. Настоящее Положение вступает в силу с момента его утверждения и вводится в действие приказом руководителя Медицинской организации.

14.2. Настоящее Положение распространяется на всех клиентов (пациентов), обращающихся за медицинской помощью в Медицинскую организацию, а так же сотрудников Медицинской организации, имеющих доступ и осуществляющих перечень действий с персональными данными пациентов.

14.3. В обязанности работников, осуществляющих первичный сбор персональных данных пациента входит их информирование о возможности ознакомление с настоящим положением, и обязательное получение согласия пациента на обработку его персональных данных.

14.4. Настоящее Положение является общедоступным документом и размещается на сайте Медицинской организации.

14.5. Пересмотр положений настоящей документа проводится в следующих случаях:

- при изменении законодательства Российской Федерации в области обработки и защиты персональных данных;
- при изменении целей обработки персональных данных, структуры информационных и/или телекоммуникационных систем (или введении новых);
- при вводе в действие новых технологий обработки персональных данных (в т. ч. передачи, хранения);
- при появлении необходимости в изменении процесса обработки персональных данных;
- по результатам контроля выполнения требований по обработке и защите персональных данных;
- по решению руководителя Медицинской организации. В случае неисполнения - пунктов настоящего ПоложенияМедицинская организация несет ответственность в соответствии действующим законодательством Российской Федерации.

14.6. Граждане, чьи персональные данные обрабатываются Медицинской организацией, могут направлять вопросы по обработке своих персональных данных в Медицинскую организацию по адресу: Чувашская Республика,г. Алатырь, ул. Стрелецкая, д. 107. При этом в тексте запроса в целях идентификации гражданина необходимо указать:

- фамилию, имя, отчество гражданина или его законного представителя, осуществляющего запрос;
- номер основного документа, удостоверяющего личность гражданина (или его законного представителя), сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие в отношениях с Медицинской организацией (например, номер договора, фамилию, имя, отчество пациента), либо сведения, иным способом подтверждающие факт обработки персональных данных Медицинской организацией;
- подпись гражданина (или его законного представителя). Если запрос отправляется в электронном виде через сайт Медицинской организации, то он должен быть оформлен в виде электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.