Приложение № 1
к Приказу № 43 от 09.02.2018г.

Политика в отношении обработки персональных данных в обществе с ограниченной ответственностью "Женская клиника здоровья и красоты"КЛИНИКА21".

1. Общие положения.

1.1. Настоящая Политика в отношении обработки персональных данных, именуемая в дальнейшем «Политика», является основополагающим локальным актом медицинской организации Общество с ограниченной ответственностью «Женская клиника здоровья и красоты «КЛИНИКА21», именуемой в дальнейшем «Медицинская организация», регулирующим вопросы обработки и защиты персональных данных в Медицинской организации.

1.2. Настоящая Политика разработана в соответствии с п.п. 2 п. 1 ст. 18.1 Федерального закона № 152-ФЗ от 27.07.2006 г. «О персональных данных» и предназначена для публичного ознакомления неограниченного круга лиц на официальном веб-сайте Медицинской организации в информационно-телекоммуникационной сети Интернет https://clinic21.ru, в дальнейшем «веб-сайте Медицинской организации», в разделе «Политика в отношении обработки персональных данных» по ссылке https://clinic21.ru/company/document/, а также на информационном стенде (стойке) и в регистратуре Медицинской организации.

1.3. Настоящая Политика разработана в целях реализации требований законодательства в области обработки и защиты персональных данных и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных в Медицинской организации, в том числе защиты прав на неприкосновенность частной жизни, личной, семейной и врачебной тайн.

1.4. Политика распространяется на персональные данные, полученные как до, так и после подписания настоящей Политики.

1.5. Действие настоящей Политики распространяется на все процессы Медицинской организации, в рамках которых осуществляется обработка персональных данных, как с использованием средстве вычислительной техники, в том числе с использованием информационно-телекоммуникационных сетей, так и без использования таких средств.

1.6. Целью настоящей Политики является установление основных принципов и подходов к обработке и обеспечению защиты персональных данных в Медицинской организации, являющейся оператором персональных данных.

1.7. Политика обязательна для ознакомления и исполнения всеми лицами, допущенными к обработке персональных данных в информационной системе персональных данных ООО «Женская клиника здоровья и красоты "КЛИНИКА21».

1.8. Сотрудники ООО «Женская клиника здоровья и красоты "КЛИНИКА21», допущенные к обработке персональных данных работников, контрагентов и клиентов ООО «Женская клиника здоровья и красоты "КЛИНИКА21», несут персональную ответственность за нарушение положений настоящей Политики, иных локальных нормативных актов ООО «Женская клиника здоровья и красоты "КЛИНИКА21» по вопросам обработки персональных данных, а также законодательства Российской Федерации по вопросам обработки и защиты персональных данных.

1.9. Положения настоящей Политики являются основой для разработки локальных актов Медицинской организации, регламентирующих вопросы обработки и защиты персональных данных.

1.10. Положения настоящей Политики действуют бессрочно, до их замены, что оформляется отдельным приказом директора Медицинской организации. Текущая редакция Политики размещается на сайте Медицинской организации в общем доступе.

2. Правовые основания обработки персональных данных.

4.1. Правовыми основаниями обработки персональных данных является совокупность нормативных правовых актов, во исполнение которых и в соответствии с которыми Медицинская организация осуществляет обработку персональных данных, в том числе:

4.1.1. Конституция Российской Федерации;

4.1.2. Трудовой кодекс Российской Федерации;

4.1.3. Налоговый кодекс Российской Федерации;

4.1.4. Гражданский кодекс Российской Федерации,

4.1.5. Федеральный закон от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»,

4.1.6. Закон Российской Федерации от 07.02.1992 г. № 2300-1 «О защите прав потребителей»;

4.1.7. Федеральный Закон от 29.12.2006 № 255-ФЗ "Об обязательном социальном страховании на случай временной нетрудоспособности и в связи с материнством",

4.1.8. Федеральный закон от 21.11.2011 N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации",

4.1.9. Федеральный закон от 29.11.2010 N 326-ФЗ "Об обязательном медицинском страховании в Российской Федерации",

4.1.10. Федеральный закон от 08.02.1998 N 14-ФЗ "Об обществах с ограниченной ответственностью",

4.1.11. Федеральный закон от 06.12.2011 N 402-ФЗ "О бухгалтерском учете",

4.1.12. Постановление Правительства Российской Федерации от 16.04.2012 г. 291 «О лицензировании медицинской деятельности»;

4.1.13. Постановление Правительства Российской Федерации от 04.10.2012 г. № 1006 «Об утверждении Правил предоставления медицинскими организациями платных медицинских услуг»;

4.1.14. Постановление Правительства Российской Федерации от 24.12.2007г. № 922 "Об особенностях исчисления средней заработной платы",

4.1.15. Лицензия Министерства здравоохранения Чувашской Республики на осуществление медицинской деятельности № ЛО-21-01-001919 от 27 августа 2019 года,

4.1.16. Устав ООО "Женская клиника здоровья и красоты"КЛИНИКА21",

4.1.17. Положение о работе с персональными данными ООО "Женская клиника здоровья и красоты"КЛИНИКА21",

4.1.18. Политика в отношении обработки персональных данных в ООО "Женская клиника здоровья и красоты"КЛИНИКА21"

4.1.19. Иные нормативные правовые акты Российской Федерации и нормативные документы уполномоченных органов государственной власти;

4.1.20. Согласие субъектов персональных данных на обработку их персональных данных;

4.1.21. Договоры с контрагентами Медицинской организации.

3. Основные термины и определения, используемые Медицинской организацией при работе с персональными данными.

3.1. Персональные данные — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

3.2. Информация — сведения (сообщения, данные) независимо от формы их представления.

3.3. Оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, 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.

3.4. Субъект персональных данных – физическое лицо: посетитель сайта; Потребитель; Заказчик; поставщик товаров и услуг; работник Медицинской организации, а также иное третье лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных;

3.5. Посетитель сайта – физическое лицо, получающее информацию и документацию, размещенную на веб-сайте Медицинской организации и/или других онлайновых ресурсах Медицинской организации в информационно-телекоммуникационной сети Интернет;

3.6. Потребитель – физическое лицо, имеющее намерение заказать (приобрести) либо заказывающее (приобретающее) платные медицинские услуги - медицинское вмешательство или комплекс медицинских вмешательств, направленных на профилактику, диагностику и лечение заболеваний, медицинскую реабилитацию и имеющих самостоятельное законченное значение в соответствии с договором;

3.7. Заказчик – физическое лицо, имеющее намерение заказать (приобрести) либо заказывающее (приобретающее) платные медицинские услуги - медицинское вмешательство или комплекс медицинских вмешательств, направленных на профилактику, диагностику и лечение заболеваний, медицинскую реабилитацию и имеющих самостоятельное законченное значение в соответствии с договором в пользу потребителя;

3.8. Поставщик товаров и услуг – физическое лицо, с которым сотрудничает Медицинская организация в рамках деятельности;

3.9. Работник– физическое лицо, вступившее в трудовые отношения с Медицинской организацией на основании трудового законодательства и/или иных основаниях, предусмотренных Трудовым Кодексом РФ;

3.10. Обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемые 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.

3.11. Автоматизированная обработка персональных данных — обработка персональных данных с помощью средств вычислительной техники.

3.12. Предоставление персональных данных — действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

3.13. Распространение персональных данных — действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

3.14. Трансграничная передача персональных данных — передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3.15. Блокирование персональных данных — временное прекращение обработки персональных данных (за исключением случаев, когда обработка необходима для уточнения персональных данных).

3.16. 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.

3.17. Обезличивание персональных данных — действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

3.18. Информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

3.19. Общедоступные источники персональных данных – справочники. адресные книги, реестры списки, каталоги, другие систематизированные источники открытой информации, содержащие персональные данные, сообщаемые субъектом персональных данных и размещенные, и опубликованные с согласия субъекта персональных данных;

3.20. Информация – сведения (сообщения, данные) независимо от формы их представления;

3.21. Документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.

4. Принципы и цели обработки Медицинской организацией персональных данных.

4.1. Медицинская организация, являясь оператором персональных данных, осуществляет обработку персональных данных принадлежащих:

- работникам Медицинской организации, уволенным работникам Медицинской организации и их близким родственникам, и представителям; соискателям на вакантные должности в Медицинской организации;

- клиентам Медицинской организации – физическим лицам, в том числе потенциальным клиентам, представителям клиентов, уполномоченным представлять клиентов, в том числе посетителям, пользователям сайта Медицинской организации, физическим лицам (населению), персональные данные которых обрабатываются в пределах полномочий, задач медицинского учреждения;

- контрагентам Медицинской организации (физическим и юридическим лицам, их руководителям, работникам партнеров Медицинской организации) с которыми взаимодействуют Медицинская организация и ее работники в рамках своей деятельности, лицам, состоящим в договорных и иных гражданско-правовых отношениях с Медицинской организацией,

- иным третьим лицам, которые прямо или косвенно определены, или определяемы с помощью персональных данных.

4.2. Обработка персональных данных Медицинской организацией осуществляется с учетом необходимости обеспечения защиты прав и свобод работников Медицинской организации, клиентов (пациентов) Медицинской организации 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.

4.3. 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 организацией;
- 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;
- выполнения требований законодательства Российской Федерации о труде, налогообложении, бухгалтерском учете;
- ведения текущего бухгалтерского, налогового, управленческого, финансового, кадрового, статистического учета; формирования и представления отчетности в соответствующие контролирующие органы;
- регулирования трудовых отношений с работниками Медицинской организации;
- 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.

4.4. 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.

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

4.6. Обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медикосоциальных услуг при условии, что обработка персональных данных осуществляется лицом,

профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

4.7. Медицинской организацией осуществляется, в том числе, и обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе (далее - персональные данные, сделанные общедоступными субъектом персональных данных), включая размещение на корпоративном сайте Медицинской организации.

5. Хранение персональных данных.

5.1. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют соответствующие цели их обработки, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки, или в случае утраты необходимости в достижении этих целей.

5.2. Персональные данные субъектов могут обрабатываться как на бумажных носителях, так и в электронном виде.

5.3. Персональные данные на бумажных носителях хранятся в запираемых шкафах или сейфах.

5.4. Персональные данные в электронном виде обрабатываются в компьютерных сетях Медицинской организации и аффилированных с Медицинской организацией организаций.

7. Перечень персональных данных, обрабатываемых в Медицинской организации

7.1. Перечень персональных данных, обрабатываемых в Медицинской организации, определяется в соответствии с законодательством Российской Федерации и локальными нормативными актами Медицинской организации с учетом целей обработки персональных данных, указанных в настоящей Политике.

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

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

- фамилия, имя, отчество; пол; дата рождения; место рождения; гражданство;
- сведения об образовании (включая название образовательного учреждения, специальность, квалификацию);
- семейное положение, сведения о браке, сведения о разводе, сведения о составе семьи; паспортные данные (вид документа, серия и номер документа, орган, выдавший документ, дата выдачи документа);

ИНН, СНИЛС, военный билет;

- адрес регистрации и фактического места жительства;
- сведения о трудовой деятельности; сведения воинского учета;
- ученая степень; ученое звание; почетное звание; сведения о дате защиты и теме диссертации, диплома; сведения о прохождении за последние пять лет повышения квалификации или профессиональной переподготовки или стажировки, способствующие подготовке к решению задач, стоящих перед руководством; сведения о наградах и поощрениях; сведения о привлечении к дисциплинарной, материальной, гражданскоправовой, административной и уголовной ответственности;
- биографические данные; сведения о государственном пенсионном страховании; идентификационный номер налогоплательщика; сведения об отчислениях в Федеральную налоговую службу; сведения об отчислениях в Пенсионный фонд России; сведения о

начислениях и удержаниях; подразделение; должность; табельный номер; сведения трудового договора (номер дата, испытательный срок) график работы; инвалидность;

- сведения о налоговых вычетах сведения о наградах; сведения об отпуске; социальные льготы; данные больничного листа;
- - сведения о дополнительных навыках;
- данные медицинских книжек;
- номер телефона
- фото.

7.2.2.) персональные данные клиентов в составе:

- фамилия, имя, отчество; дата рождения; возраст; пол; СНИЛС; ИНН;
- номер телефона; документ удостоверяющий личность (тип документа, серия, номер дата выдачи, кем выдан);
- гражданство; место работы; место учебы; должность; адрес прописки; адрес проживания;
- полис ОМС, ДМС (серия и номер, дата действия);
- сведения об оплате;
- медицинские сведения (анамнез, диагноз, ранее полученная пациентом медицинская помощь в Клинике и за ее пределами, другие медицинские сведения;
- сведения о об открытых счетах в кредитных организациях, номерах карт в кредитных организациях;
- сведения о состоянии здоровья;
- сведения о состоянии интимной жизни.

7.2.3.) Персональные данные контрагентов в составе:

- фамилия, имя, отчество физического лица;
- наименование юридического лица;
- идентификационный номер налогоплательщика (ИНН); государственный регистрационный номер (ОГРН, ОГРНИП);
- сведения о составе и полномочиях органов управления юридического лица;
- адрес; контактный телефон;
- номер банковского счета;
- сведения о заключаемом с контрагентом договоре.

7.3. 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.

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

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

8. Перечень действий с персональными данными

8.1. При обработке персональных данных Медицинская организация будет осуществлять следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

8.2. Медицинская организация вправе обрабатывать персональные данные посредством внесения их в электронную базу данных включения в списки (реестры) и отчетные формы, предусмотренные документами, регламентирующими порядок ведения и состав данных в учетно-отчетной медицинской документации, а также договором на оказание медицинской помощи по программе ОМС, ДМС между Медицинской организацией и страховой медицинской компанией.

8.3. Медицинская организация имеет право во исполнение своих обязательств на обмен (прием и передачу) персональными данными с медицинскими компаниями, в том числе страховыми, Министерством здравоохранения, Фондом социального страхования, Фондом обязательного медицинского страхования, органом статистической отчетности с использованием машинных носителей информации, по каналам связи и (или) в виде бумажных документов, с соблюдением мер, обеспечивающих их защиту от несанкционированного доступа, без специального уведомления об этом субъекта персональных данных.

8.4. Медицинская организация имеет право на обмен (прием и передачу) персональными данными с третьими лицами, которым в порядке субподряда Медицинской организацией поручено выполнение некоторых медицинских услуг (в том числе с клиническими лабораториями).

9. Условия обработки персональных данных Медицинской организацией.

9.1. Обработка персональных данных в Медицинской организации осуществляется с согласия субъекта персональных данных на обработку его персональных данных, если иное не предусмотрено законодательством Российской Федерации в области персональных данных.

9.2. Медицинская организация без согласия субъекта персональных данных не раскрывает третьим лицам и не распространяет персональные данные, если иное не предусмотрено федеральным законом.

9.3. Медицинская организация вправе поручить обработку персональных данных другому лицу с согласия субъекта персональных данных на основании заключаемого с этим лицом договора. Договор должен содержать перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанность такого лица соблюдать конфиденциальность персональных данных и обеспечивать безопасность персональных данных при их обработке, а также требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона от 27.07.2006 №152 «О персональных данных».

9.4. В случае, когда Медицинская организация на основании договора передает или поручает обработку персональных данных другому юридическому лицу или индивидуальному предпринимателю, существенным условием договора должна быть обязанность обеспечения указанным лицом условий конфиденциальности и обеспечения безопасности персональных данных при их передаче или обработке.

9.5. При передаче персональных данных третьим лицам в соответствии с заключенными договорами Медицинская организация обеспечивает обязательное выполнение требований законодательства РФ и нормативных актов Медицинской организации в области персональных данных.

10. Обеспечение защиты персональных данных при их обработке Медицинской организацией

10.1. Медицинская организация принимает меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом от 27.07.2006 №152 «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 от 27.07.2006 №152 «О персональных данных», Постановлением Правительства от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Приказом ФСТЭК 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» и другими нормативными правовыми актами, если иное не предусмотрено федеральными законами. К таким мерам могут, в частности, относиться:

– назначение в Медицинской организации ответственного за организацию обработки персональных данных;

– издание Медицинской организацией документов, определяющих политику оператора 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 «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Клиники в отношении обработки персональных данных, локальным актам оператора;

– оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона от 27.07.2006 №152 «О персональных данных», соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных»;

– 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 Медицинской организации в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

10.2. Медицинская организация при обработке персональных данных принимает необходимые правовые, организационные и технические меры или обеспечивает их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

10.3. Обеспечение безопасности персональных данных достигается, в частности:

– определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее ИСПДн);

– применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

– оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн;

– учетом машинных носителей персональных данных;

– обнаружением фактов несанкционированного доступа к персональным данным и принятием необходимых мер;

– восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– установлением правил доступа к персональным данным, обрабатываемых в ИСПДн, а также обеспечением регистрации доступа к персональным данным в ИСПДн;

– контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности ИСПДн.

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

11.1. 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.

11.2. 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.

11.3. 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.

11.4. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

– подтверждение факта обработки персональных данных Медицинской организацией;

– правовые основания и цели обработки персональных данных;

– цели и применяемые Медицинской организацией способы обработки персональных данных;

– наименование и место нахождения Медицинской организации, сведения о лицах (за исключением работников Медицинской организации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Медицинской организацией или на основании федерального закона;

– обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок

представления таких данных не предусмотрен федеральным законом;

– сроки обработки персональных данных, в том числе сроки их хранения;

– порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 №152 «О персональных данных»;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Клиники, если обработка поручена или будет поручена такому лицу.

11.5. Если субъект персональных данных считает, что Медицинская организация осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27.07.2006 №152 «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.

11.6. 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.

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. Уничтожение персональных данных производится в соответствии с актуальными внутренними процессами Медицинской организации.

13. Доступ сотрудников Медицинской организации к персональным данным

13.1. Доступ к персональным данным предоставляется только тем работникам Медицинской организации, которым он необходим для исполнения их непосредственных должностных обязанностей.

13.2. 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.

14. Ответственность Медицинской организации и её сотрудников

14.1. Работники Медицинской организации, виновные в нарушении нормативных правовых актов и локальных нормативных актов Медицинской организации, регулирующих процессы обработки и защиты персональных данных, могут быть привлечены к дисциплинарной, материальной, гражданско-правовой, административной, уголовной ответственности в порядке, установленном действующим законодательством Российской Федерации.

15. Заключительные положения.

15.1. Настоящая Политика является общедоступным документом и размещается на сайте Клиники по адресу https://clinic21.ru/.

15.2. Пересмотр положений настоящей Политики 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 руководства Клиники.

В случае неисполнения положений настоящей Политики Медицинская организация несет ответственность в соответствии действующим законодательством Российской Федерации.

15.4. Граждане, чьи персональные данные обрабатываются Клиникой, могут направлять вопросы по обработке своих персональных данных в Клинику по адресу: Чувашская Республика, город Чебоксары, улица Сельская, дом 39, помещение 2.

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.