**УТВЕРЖДЕНА**

приказом ГБУЗ ПК «ССМП г. Соликамска»

от \_\_.\_\_.20\_\_ г. № \_

**Политика**

**Государственного бюджетного учреждения здравоохранения Пермского края «Станция скорой медицинской помощи г. Соликамска» в отношении обработки и обеспечения безопасности персональных данных**

**1. Общие положения**

1.1. Настоящая Политика разработана в целях реализации требований законодательства Российской Федерации в области обработки персональных данных субъектов персональных данных и направлена на обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных в Государственном бюджетном учреждении здравоохранения Пермского края «Станция скорой медицинской помощи г. Соликамска» (далее – Организация).

1.2. В политике используются следующие основные понятия:

* персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
* 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;
* 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;
* информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;
* трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

1.3. Политика раскрывает принципы обработки Организацией персональных данных в информационных системах, права и обязанности Организации при обработке персональных данных, права субъектов персональных данных, а также включает перечень мер, применяемых Организацией в целях обеспечения безопасности персональных данных при их обработке.

1.4. Положения Политики распространяются на отношения по обработке и обеспечению безопасности персональных данных, полученных Организацией как до, так и после утверждения Политики, за исключением случаев, когда по причинам правового, организационного и иного характера положения Политики не могут быть распространены на отношения по обработке и обеспечению безопасности персональных данных, полученных до ее утверждения.

1.5. Если в отношениях с Организацией участвуют законные представители субъектов персональных данных, то Организация становится оператором персональных данных лиц, представляющих указанных субъектов. Положения Политики и другие локальные акты Организации распространяются на случаи обработки и обеспечения безопасности персональных данных законных представителей субъектов персональных данных, даже если эти лица в локальных актах прямо не упоминаются, но фактически участвуют в правоотношениях с Организацией.

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

* подтверждение факта обработки персональных данных Организацией;
* правовые основания и цели обработки персональных данных;
* цели и применяемые Организацией способы обработки персональных данных;
* наименование и место нахождения Организации, сведения о лицах (за исключением работников Организации), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с 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 июля 2006 г. N 152-ФЗ "О персональных данных" (далее - Закон 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 оператора, если обработка поручена или будет поручена такому лицу;
* иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

1.7. Субъект персональных данных вправе требовать от оператора 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.

1.8. 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.

1.9. Оператор персональных данных вправе:

* отстаивать свои интересы в суде;
* предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);
* отказывать в предоставлении персональных данных в случаях, предусмотренных законодательством;
* использовать персональные данные субъекта без его согласия в случаях, предусмотренных законодательством.

1.10. При сборе персональных данных, в том числе посредством информационно-телекоммуникационной сети "Интернет", оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации

**2. Цели обработки персональных данных.**

2.1. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

2.2. Цели обработки персональных данных происходят в том числе из анализа правовых актов, регламентирующих деятельность Организации, целей фактически осуществляемой Организацией деятельности, а также деятельности, которая предусмотрена учредительными документами Организации, и конкретных бизнес-процессов в конкретных информационных системах персональных данных (по структурным подразделениям Организации и их процедурам в отношении определенных категорий субъектов персональных данных).

2.3. К целям обработки персональных данных Организации относятся:

* заключение, исполнение и прекращение гражданско-правовых договоров;
* оказание медицинской помощи населению;
* выполнение требований законодательства об основах охраны здоровья граждан;
* организация кадрового учета, обеспечение соблюдения законов, заключение и исполнение обязательств по трудовым и гражданско-правовым договорам;
* ведение кадрового делопроизводства, содействие работникам в трудоустройстве, обучении и продвижении по службе, пользовании льготами;
* исполнение требований налогового законодательства по вопросам исчисления и уплаты налога на доходы физических лиц, взносов во внебюджетные фонды и страховых взносов во внебюджетные фонды, пенсионного законодательства при формировании и передаче в ПФР персонифицированных данных о каждом получателе доходов, которые учитываются при начислении взносов на обязательное пенсионное страхование;
* заполнение первичной статистической документации в соответствии с трудовым, налоговым законодательством и иными федеральными законами.

**3. Правовые основания обработки персональных данных.**

Обработка персональных данных осуществляется на основании:

* согласия субъекта персональных данных на обработку его персональных данных;
* необходимости достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на Организацию функций, полномочий и обязанностей;
* уставные документы Организации;
* договоры, заключаемые между Организацией и субъектом персональных данных.

**4. Объем и категории обрабатываемых персональных данных, категории субъектов персональных данных.**

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

Организация обрабатывает персональные данные следующих субъектов:

* Физические лица, являющие близкими родственниками сотрудников Организации;
* Физические лица, уволившиеся из Организации;
* Физические лица, являющиеся кандидатами на работу;
* Физические лица, являющиеся работниками Организации;
* Физические лица, обратившиеся в Организацию за медицинской помощью.

Обрабатываемые персональные данные:

* Физические лица, являющиеся работниками Организации:

фамилия, имя, отчество; пол; гражданство; дата и место рождения; адрес места проживания; сведения о регистрации по месту жительства или пребывания; номера телефонов; адрес электронной почты; замещаемая должность; сведения о трудовой деятельности; идентификационный номер налогоплательщика; данные документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета, в том числе в форме электронного документа; данные паспорта или иного удостоверяющего личность документа; данные трудовой книжки; сведения о воинском учете; сведения об образовании; данные водительского удостоверения, доходы, прежние фамилия, имя, отчество, сведения о дисциплинарных взысканиях; сведения, содержащиеся в материалах служебных проверок; сведения о семейном положении; сведения о близких родственниках; номер расчетного счета, данные предварительного медицинского осмотра, психиатрического освидетельствования.

* Физические лица, являющие близкими родственниками сотрудников Организации:

фамилия, имя, отчество; степень родства, дата рождения.

* Физические лица, уволившиеся из Организации:

фамилия, имя, отчество; паспортные данные, адрес проживания, адрес регистрации, гражданство, дата рождения, занимаемая должность, ИНН, информация о трудовой деятельности, квалификация, контактные сведения (номер телефона, электронная почта), место рождения, образование, пол, профессия, сведения о воинском учёте, сведения о переподготовке и повышении квалификации, СНИЛС, состав семьи, социальное положение, специальность.

* Физические лица, являющиеся кандидатами на работу:

фамилия, имя, отчество; паспортные данные, адрес проживания, адрес регистрации, гражданство, дата рождения, информация о трудовой деятельности, квалификация, контактные сведения (номер телефона, электронная почта), место рождения, место учебы, сведения об образовании, профессия, сведения о воинском учёте, сведения о профессиональной переподготовке и повышении квалификации, семейное положение, специальность, должность.

* Физические лица, обратившиеся в Организацию за медицинской помощью:

фамилия, имя, отчество; пол; гражданство; дата и место рождения; адрес места проживания; сведения о регистрации по месту жительства или пребывания; данные трудовой деятельности (учебы); номер телефона; полис ОМС; страховое свидетельство; данные паспорта или иного удостоверяющего личность документа; сведения о законных представителях; сведения о заболеваниях пациента (диагноз).

**5. Порядок и условия обработки персональных данных.**

Обработка персональных данных осуществляется как с использованием средств автоматизации, так и без использования таких средств.

Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Обработке подлежат только персональные данные, которые отвечают целям их обработки. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки.

До начала обработки персональных данных Организация осуществляет уведомление уполномоченного органа по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных. Организация уведомляет уполномоченный орган по защите прав субъектов персональных данных об изменении сведений, поданных ранее, согласно требованиям Федерального закона № 152-ФЗ.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого 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 подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Организация не производит трансграничную передачу персональных данных.

Условием прекращения обработки персональных данных может являться достижение целей обработки персональных данных, истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных, а также выявление неправомерной обработки персональных данных.

Организация вправе поручить обработку персональных данных другому лицу на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта. Лицо, осуществляющее обработку персональных данных по поручению Организации, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Законом о персональных данных, соблюдать конфиденциальность персональных данных, принимать необходимые меры, направленные на обеспечение выполнения обязанностей, предусмотренных Законом о персональных данных.

Организация, получившая доступ к персональным данным, обязана соблюдать конфиденциальность персональных данных - не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

Организация вправе передавать персональные данные органам дознания и следствия, иным уполномоченным органам по основаниям, предусмотренным действующим законодательством Российской Федерации.

Политика является общедоступным документом, декларирующим концептуальные основы деятельности Организации при обработке и обеспечению безопасности персональных данных в информационных системах.

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.

Обработка персональных данных производится на основе соблюдения принципов:

* законности целей и способов обработки персональных данных;
* соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;
* соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;
* достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;
* недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;
* хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки;
* уничтожения по достижении целей обработки персональных данных или в случае утраты необходимости в их достижении.

**6. Порядок и условия обработки биометрических персональных данных.**

К биометрическим персональным данным относятся сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются Организацией для установления личности субъекта персональных данных.

Обработка биометрических персональных данных может осуществляться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, связанных с реализацией международных договоров Российской Федерации о реадмиссии, в связи с осуществлением правосудия и исполнением судебных актов, в связи с проведением обязательной государственной дактилоскопической регистрации, а также в случаях, предусмотренных законодательством Российской Федерации об обороне, о безопасности, о противодействии терроризму, о транспортной безопасности, о противодействии коррупции, об оперативно-розыскной деятельности, о государственной службе, уголовно-исполнительным законодательством Российской Федерации, законодательством Российской Федерации о порядке выезда из Российской Федерации и въезда в Российскую Федерацию, о гражданстве Российской Федерации, законодательством Российской Федерации о нотариате.

Обработка биометрических персональных данных осуществляется Организацией в соответствии с требованиями к защите биометрических персональных данных, установленными в соответствии со статьей 19 Закона о персональных данных.

Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

Под материальным носителем понимается машиночитаемый носитель информации (в том числе магнитный и электронный), на котором осуществляются запись и хранение сведений, характеризующих физиологические особенности человека и на основе которых можно установить его личность.

Организация утверждает порядок передачи материальных носителей уполномоченным лицам.

Материальный носитель должен использоваться в течение срока, установленного Организацией, осуществившей запись биометрических персональных данных на материальный носитель, но не более срока эксплуатации, установленного изготовителем материального носителя.

Организация обязана:

* осуществлять учет количества экземпляров материальных носителей;
* осуществлять присвоение материальному носителю уникального идентификационного номера, позволяющего точно определить оператора, осуществившего запись биометрических персональных данных на материальный носитель.

Технологии хранения биометрических персональных данных вне информационных систем персональных данных должны обеспечивать:

* доступ к информации, содержащейся на материальном носителе, для уполномоченных лиц;
* применение средств электронной подписи или иных информационных технологий, позволяющих сохранить целостность и неизменность биометрических персональных данных, записанных на материальный носитель;
* проверку наличия письменного согласия субъекта персональных данных на обработку его биометрических персональных данных или наличия иных оснований обработки персональных данных, установленных законодательством Российской Федерации в сфере отношений, связанных с обработкой персональных данных.

При хранении биометрических персональных данных вне информационных систем персональных данных должна обеспечиваться регистрация фактов несанкционированной повторной и дополнительной записи информации после ее извлечения из информационной системы персональных данных.

**7. Актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов на доступ к персональным данным**

Организация обязана прекратить обработку персональных данных или обеспечить прекращение обработки персональных данных лицом, действующим по поручению Организации:

* в случае выявления неправомерной обработки персональных данных в срок, не превышающий трех рабочих дней с даты этого выявления. Если обеспечить правомерность обработки персональных данных невозможно, Организация в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязана уничтожить такие персональные данные;
* в случае отзыва субъектом персональных данных согласия на обработку его персональных данных и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва;
* в случае достижения цели обработки персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.В случае отсутствия возможности уничтожения персональных данных в течение указанного срока Организация осуществляет блокирование таких персональных данных и обеспечивает их уничтожение в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами;
* в случае подтверждения факта неточности персональных данных до их уточнения на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов в срок до семи рабочих дней.

В случае установления факта неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, Организация обязана с момента выявления такого инцидента уведомить уполномоченный орган по защите прав субъектов персональных данных:

- в течение двадцати четырех часов о произошедшем инциденте, о предполагаемых причинах, повлекших нарушение прав субъектов персональных данных, и предполагаемом вреде, нанесенном правам субъектов персональных данных, о принятых мерах по устранению последствий соответствующего инцидента, а также предоставить сведения о лице, уполномоченном Организацией на взаимодействие с уполномоченным органом по защите прав субъектов персональных данных, по вопросам, связанным с выявленным инцидентом;

- в течение семидесяти двух часов о результатах внутреннего расследования выявленного инцидента, а также предоставить сведения о лицах, действия которых стали причиной выявленного инцидента (при наличии).

Сведения из пункта 1.6 настоящей политики предоставляются субъекту персональных данных или его представителю Организацией в течение десяти рабочих дней с момента обращения либо получения Организацией запроса субъекта персональных данных или его представителя. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления Организацией в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

В случае обращения субъекта персональных данных к оператору с требованием о прекращении обработки персональных данных оператор в срок, не превышающий десяти рабочих дней с даты получения им соответствующего требования, обязан прекратить их обработку.

Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы, кроме случаев наличия согласия в письменной форме субъекта персональных данных или случаев, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.