Автономная некоммерческая организация

«ЭЛЕКТРОСТАЛЬСКАЯ СТОМАТОЛОГИЧЕСКАЯ ПОЛИКЛИНИКА»

ПРИКАЗ № 12 от 10.01.2018 г.

" Об обеспечении безопасности персональных данных при их обработке в Информационных Системах Персональных Данных»

В соответствии с **Федеральным законом** от 27.07.2006 N 152-ФЗ "О персональных данных", во исполнении части 1 ст.23,ст.24 Конституции Российской Федерации, главы 14 Трудового Кодекса, **постановлением** Правительства Российской Федерации от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами",

ПРИКАЗЫВАЮ:

1. Утвердить:

1.1. Политику в отношении обработки персональных данных в АНО «ЭСП» (Приложение №1 к Приказу).

1.2. Инструкцию пользователя информационной системы персональных данных АНО «ЭСП» (Приложение №2 к приказу).

2. Руководителям структурных подразделений ознакомить под роспись работников с настоящим приказом.

3. Назначить сотрудников подразделений, операторов ЭВМ, выполняющих работы с Информационными системами персональных Данных, ответственными и допущенными к работе.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач АНО «ЭСП» К.С. Горелик

Приложение 1
к приказу Главного врача АНО «ЭСП»
от 10.01.2018 № 12

УТВЕРЖДАЮ
Главный врач АНО «ЭСП»

_____К.С.Горелик

«10» января 2018 г

ПОЛИТИКА
в отношении обработки персональных данных в АНО « Электростальская стоматологическая поликлиника»

1. Общие положения

1.1. Настоящий документ определяет политику АНО «ЭСП» в отношении обработки персональных данных (далее - Политика) в информационных системах персональных данных (далее ИСПДн).

1.2. Политика разработана с учетом требований Конституции Российской Федерации, положений главы 14 Трудового Кодекса Российской Федерации « Защита персональных данных работников», федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», федеральным законом Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», и иных нормативных правовых актов Российской Федерации в области персональных данных.

1.3. Политика является общедоступным документом, декларирующим основы деятельности Оператора при обработке персональных данных

1.4. Настоящая Политика вступает в силу с момента ее утверждения Главным врачом АНО «ЭСП» и действует до замены ее новой Политикой учреждения.

2. Основные понятия, используемые в настоящей Политике

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники (п. 4 ч. 1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»).

Персональные данные - любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных).

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.

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

3. Цели обработки персональных данных

В АНО «ЭСП» производится обработка персональных данных следующих категорий субъектов:

- физические лица (работники), в том числе уволенные, состоящие в трудовых отношениях с юридическим лицом(оператором);

- резиденты и субъекты РФ, обратившиеся за оказанием медицинской помощи в АНО «ЭСП».

Для каждой категории субъектов персональных данных определены цели обработки их персональных данных.

Целями обработки персональных данных работников АНО «ЭСП» являются:

- ведение бухгалтерского и кадрового учета

Целями обработки персональных данных резиденты и субъекты РФ, обратившиеся за оказанием медицинской помощи в АНО «ЭСП» являются:

- ведение и актуализация информации в медицинской информационной системе в части обеспечения регламентных требований информационного взаимодействия в территориальной системе обязательного медицинского страхования; формирование и ведение медицинских регистров;

4. Принципы обработки персональных данных

В своей деятельности АНО «ЭСП» исходит из того, что субъект персональных данных АНО «ЭСП», информирует представителей АНО «ЭСП» об изменении своих персональных данных.

Обработка персональных данных осуществляется на основе следующих принципов:

- обработка персональных данных осуществляется на законной и справедливой основе;
- обработка персональных данных ограничивается достижением конкретных, заранее определённых 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;
- содержание и объем обрабатываемых персональных данных соответствуют заявленным целям обработки;
- при обработке персональных данных обеспечивается точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных;
- хранение персональных данных осуществляется 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.

5. Условия обработки персональных данных

5.1. Обработка персональных данных должна осуществляться на законной основе.

5.2. Условия обработки персональных данных должны соответствовать требованиям **статьи 6** Федерального закона Российской Федерации от 27 июля 2006 года N 152 "О персональных данных".

5.3. Условия обработки персональных данных должны быть обеспечены применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищённости персональных данных.

6. Права субъектов персональных данных

6.1. Субъект персональных данных, чьи персональные данные обрабатываются в ИСПДн,

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

- подтверждение факта обработки персональных данных;
- правовые основания и цели обработки персональных данных;
- цели и применяемые АНО «ЭСП» способы обработки персональных данных;
-наименование и место нахождения АНО «ЭСП» сведения о лицах (за исключением работников АНО «ЭСП»), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с АНО «ЭСП» или на основании федеральных законов Российской Федерации;
- обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральными законами Российской Федерации;
- сроки обработки персональных данных, в том числе сроки их хранения;
- иные сведения, предусмотренные **Федеральным законом** "О персональных данных" или другими федеральными законами.

6.2. Субъект персональных данных вправе требовать от АНО «ЭСП» 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.

6.3. Субъект персональных данных вправе обжаловать действия или бездействие АНО «ЭСП» в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке.

6.4. 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.

7. ОБЯЗАННОСТИ АНО «ЭСП»

В соответствии с положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» АНО «ЭСП» обязано:

- осуществлять обработку персональных данных с соблюдением правил и принципов, предусмотренных законодательством Российской Федерации;
- принимать необходимые правовые, организационные и технические меры и обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий;
- не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации;
- представлять субъекту персональных данных по его запросу информацию, касающуюся обработки его персональных данных, либо на законных основаниях предоставить отказ в предоставлении данной информации и дать в письменной форме мотивированный ответ, содержащий ссылку на положения Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», являющуюся основанием для такого отказа;
- в случае, если предоставление персональных данных является обязательным в соответствии с законодательством Российской Федерации, разъяснить данному субъекту правовые последствия отказа предоставления таких данных;
- по требованию субъекта персональных данных вносить изменения в обрабатываемые персональные данные или уничтожать их, если такие данные являются неполными, неактуальными, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах;
- в случае выявления неправомерной обработки персональных данных или неточных персональных данных, устранять выявленные нарушения в соответствии с порядком и сроками, указанными в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных»;

8. Реализация требований к защите персональных данных

8.1. Реализация требований к защите персональных данных в АНО «ЭСП» обеспечивается применением организационных и технических мер 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.

8.2. Реализация требований к защите персональных данных в АНО «ЭСП» включает в себя проведение в частности следующих мероприятий:

- определение категории персональных данных, обрабатываемых в ИСПДн;
- определение угроз безопасности персональных данных в ИСПДн;
- определение необходимого уровня защищённости персональных данных на основе анализа угроз безопасности и возможного ущерба субъектам персональных данных при реализации угроз безопасности персональных данных;
- реализация организационных и технических мер по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищённости персональных данных;
- оценка эффективности принимаемых мер по обеспечению безопасности персональных данных;
- учёт машинных носителей персональных данных;
- обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;
- восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- установление правил доступа к персональным данным, обрабатываемым в ИСПДн, а также обеспечение регистрации и учёта всех действий, совершаемых с персональными данными в ИСПДн;
- контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищённости ИСПДн.

9. Заключительные положения

9.1. Настоящая Политика является общедоступной и подлежит размещению на официальном сайте АНО «ЭСП».

9.2. Настоящая Политика подлежит изменению, дополнению в случае принятия новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных.

9.3. Ответственность работников АНО «ЭСП», имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российский Федерации.

Правила
обработки персональных данных в АНО
«Электростальская стоматологическая поликлиника»

1. Общие положения

1.1. Настоящие правила обработки персональных данных устанавливают единый порядок обработки персональных данных в информационных системах персональных данных (далее - ИСПДн) АНО «ЭСП»

1.2. Настоящие правила регламентируют требования к технологии обработки персональных данных и обеспечивают эффективность системы защиты информации, построенной на основе существующей технологии обработки персональных данных.

1.3. Настоящие правила разработаны на основании и в соответствии с требованиями следующих законодательных и нормативных правовых актов Российской Федерации:
- трудовой кодекс Российской Федерации (ст. 65, ст. 85 - 90);
- гражданский кодекс Российской Федерации, Часть 1 (ст. ст. 150, 152, 152.1) от 30.11.1994 N 51-ФЗ;
- федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и защите информации";
- федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - Федеральный закон N 152-ФЗ);
- постановление Правительства Российской Федерации от 21 марта 2012 года N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правыми актами, операторами, являющимися государственными или муниципальными органами;
- постановление Правительства Российской Федерации от 15 сентября 2008 года N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";
- постановление Правительства Российской Федерации от 01 ноября 2012 года N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

1.4. Настоящие правила устанавливают и определяют в АНО «ЭСП»:
- процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных;
- цели обработки персональных данных;
- содержание обрабатываемых персональных данных для каждой цели обработки персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- сроки обработки и хранения обрабатываемых персональных данных;
- порядок уничтожения обработанных персональных данных при достижении целей обработки или при наступлении иных законных оснований.

1.5. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определённых статьёй 3 Федерального закона N 152-ФЗ.

1.6. Правила являются обязательными для исполнения всеми пользователями ИСПДн, имеющими доступ к персональным данным.

1.7. Правила вступают в силу с момента их утверждения и действуют до замены их новыми Правилами.

2. Требования к обработке и защите персональных данных

2.1. При обработке персональных данных необходимо руководствоваться принципами и условиями определёнными нормами главы 2 Федерального закона N 152-ФЗ.

2.2. Права субъектов персональных данных определены в главе 3 Федерального закона N 152-ФЗ.

2.3. При определении обязанностей АНО «ЭСП» при сборе персональных данных и при обращении к нему субъектов персональных данных» АНО «ЭСП» должно руководствоваться главой 4 Федерального закона N 152-ФЗ.

2.4. В АНО «ЭСП» должны приниматься меры направленные на обеспечение выполнения обязанностей, предусмотренных Федеральным законом N 152-ФЗ в частности:
- назначение ответственного за организацию обработки персональных данных;
- издание документов, определяющих политику АНО «ЭСП» 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 в соответствии со статьёй 19 Федерального закона N 152-ФЗ "О персональных данных";
- осуществление внутреннего контроля соответствия обработки персональных данных в соответствии Федеральному закону N 152-ФЗ "О персональных данных" и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике АНО «ЭСП» в отношении обработки персональных данных, локальным актам АНО «ЭСП».
- оценка вреда, который может быть причинён субъектам персональных данных в случае нарушения законодательства Российской Федерации в сфере персональных данных;
- ознакомление пользователей ИСПДн, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных и настоящими Правилами;
- запрещение обработки персональных данных пользователям ИСПДн, не допущенными к их обработке.

2.5. Обработка персональных данных должна осуществляется только при наличии оснований, предусмотренных ст. 6 Федерального закона "О персональных данных".

2.6. При обработке персональных данных должны соблюдаться следующие требования:

- к работе с персональными данными допускаются только пользователи ИСПДн, допущенные соответствующим приказом врача АНО «ЭСП»;

- в целях обеспечения сохранности документов, содержащих персональные данные, все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться пользователями - сотрудниками АНО «ЭСП» осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

2.7. Особенности обработки персональных данных

2.7.1. Машинные носители персональных данных должны подлежать обязательной регистрации и учёту, в соответствии с "Инструкцией по защите машинных носителей информации".

2.7.2. Обработка персональных данных должна осуществляться при условии выполнения требований к защите персональных данных, установленных:
- федеральным законом Российской Федерации от 27 июля 2006 года N 152-ФЗ "О персональных данных";
- постановлением Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";
- постановлением Правительства Российской Федерации от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правыми актами, операторами, являющимися государственными или муниципальными органами";
- приказом ФСТЭК России от 18.02.2013 N 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".

2.7.3. При обработке персональных данных в ИСПДн АНО «ЭСП» должны приниматься правовые, организационные и технические меры или обеспечиваться 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.

3. Цели обработки персональных данных

3.1. Цель обработки персональных данных определяется целями создания и видами деятельности АНО «ЭСП» а именно:
- управления лечебной и профилактической деятельностью системы здравоохранения Московской области;
- регулирования отношений, возникающих в сфере обращения лекарственных средств, в пределах представленных полномочий;
- управления специализированной медицинской помощью;
- исполнения обязательств по договорам с субъектом персональных данных (договоры гражданско-правового характера);
- ведения бухгалтерского и кадрового учёта сотрудников (работников) АНО «ЭСП»;
- формирования, ведения регионального сегмента единой государственной информационной системы здравоохранения.

4. Содержание обрабатываемых персональных данных

4.1. Содержание обрабатываемых персональных данных устанавливается "Перечнем персональных данных, обрабатываемых в АНО «ЭСП» в связи с реализацией служебных или трудовых отношений, а также в связи с оказанием услуг и осуществлением государственных или муниципальных функций".

5. Категории субъектов персональных данных

5.1. В ИСПДн осуществляется обработка специальных категории персональных данных.
5.2. В ИСПДн осуществляется обработка персональных данных субъектов персональных данных, не являющихся сотрудниками оператора.

6. Сроки обработки и хранения обрабатываемых персональных данных

6.1. 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.
6.2. 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.
6.3. Основания для прекращения обработки персональных данных и сроки их уничтожения определены в частях 3, 4, 5 статьи 21 Федерального закона "О персональных данных".
6.4. Основанием (условием) прекращения обработки персональных данных также является ликвидация АНО «ЭСП»
6.5. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в частях 3, 4, 5 статьи 21 Федерального закона N 152-ФЗ, должно осуществляться блокирование таких персональных данных или обеспечиваться их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению АНО «ЭСП» и обеспечиваться уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами).

7. Порядок уничтожения персональных данных

7.1. При уничтожении материальных носителей содержащих персональные данные должно быть исключено ознакомление с ними посторонних лиц, неполное или случайное их уничтожение.

7.2. При необходимости уничтожения части персональных данных уничтожается материальный носитель с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

7.3. Уничтожение части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе.

7.4. Уничтожение персональных данных осуществляется в соответствии с требованиями "Инструкции по защите машинных носителей информации".

8. Ответственность за нарушения при обработке персональных данных

8.1. Лица, виновные в нарушении требований к обработке персональных данных, установленным Федеральным законом N 152-ФЗ, несут предусмотренную законодательством Российской Федерации ответственность.

9. Заключительные положения

9.1. Сотрудники АНО «ЭСП», определённые приказом главного врача, как пользователи ИСПДн должны ознакомиться с настоящими правилами обработки персональных данных.

9.2. Обязанность доводить до сведения сотрудников АНО «ЭСП» нормативные правовые акты в сфере персональных данных, локальные акты по вопросам обработки и защиты персональных данных, требования к защите персональных данных лежит на ответственном за организацию обработки персональных данных.

Правила работы с запросами субъектов персональных данных в АНО «Электростальская стоматологическая поликлиника»

1. Общие положения

1.1.Настоящими Правилами определяется порядок учета (регистрации), рассмотрения запросов субъектов персональных даны, их представителей, государственных (муниципальных) и правоохранительных органов.

1.2. Настоящие Правила разработаны в соответствии Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон), постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», специальными требованиями и рекомендациями по технической защите конфиденциальной информации, утвержденными приказом Гостехкомиссии России от 30.08.2002 № 282.

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

1) подтверждение факта обработки персональных данных;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые способы обработки персональных данных;

4) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

5) сроки обработки персональных данных, в том числе сроки их хранения;

6)порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

7) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению АНО «ЭСП», если обработка поручена или будет поручена такому лицу;

8) иные сведения, предусмотренные Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» или другими федеральными законами.

Субъект персональных данных вправе требовать 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.

Представитель субъекта персональных данных - лицо, действующее от имени субъекта персональных данных в силу полномочия, основанного на доверенности, указании закона, либо акте уполномоченного на то государственного органа или органа местного самоуправления.

Персональные данные не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает работника от взятых им обязательств по неразглашению сведений ограниченного распространения.

2. Порядок регистрации и рассмотрения запросов

2.1. Ведение делопроизводства по запросам осуществляется непосредственно в АНО «ЭСП». Все поступившие запросы регистрируются в «Журнале входящей корреспонденции» в день их поступления. На запросе проставляется штамп, в котором указывается входящий номер и дата регистрации.

2.2. Запрос прочитывается, проверяется на повторность, при необходимости сверяется с находящейся в архиве предыдущей перепиской. Если запрашиваемая информация ранее предоставлялась, авторам таких запросов направляется сообщение о том, что запрашиваемая информация предоставлялась ранее, с указанием номера и даты исходящего документа.

Повторный запрос наряду с необходимыми сведениями должен содержать обоснование направления повторного запроса.

2.3. При личном обращении субъекта персональных данных или его законного представителя заполняется форма запроса (приложение 1) или принимается запрос в произвольной форме.

Необходимые сведения о субъекте ПДн, которые должны присутствовать в подаваемом запросе:

− Фамилия, Имя и Отчество субъекта ПДн;

- копия основного документа, удостоверяющего личность, сведения о дате выдачи указанного документа и выдавшем его органе;

− адрес места жительства;

- собственноручная подпись субъекта персональных данных или его законного представителя.

2.4. Анонимные запросы не рассматриваются. Под анонимным понимается запрос, в котором не указаны фамилия, имя и отчество гражданина, направившего запрос, либо наименование организации (юридического лица), общественного объединения. Такие запросы подшиваются в дело без направления ответа заявителю.

2.5. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

3. Сроки рассмотрения и уточнения запросов

3.1. Запрос подлежит рассмотрению в тридцатидневный срок со дня его регистрации в АНО «ЭСП», если иное не предусмотрено законодательством Российской Федерации.

3.2. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, уполномоченные сотрудники АНО «ЭСП» обязаны внести в них необходимые изменения.

3.3. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, уполномоченные сотрудники АНО «ЭСП» обязаны уничтожить такие персональные данные (акт об уничтожении ПДн, уведомление об уничтожении).

3.4. В срок, не превышающий трех рабочих дней с даты выявления неправомерной обработки персональных данных, обязаны прекратить неправомерную обработку персональных данных. В случае, если обеспечить правомерность обработки персональных данных невозможно в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязаны уничтожить такие персональные данные или обеспечить их уничтожение.

3.5. В случае поступления Запроса о предоставлении информации в правоохранительные органы. Предоставление сведений, составляющих ПДн, без согласия гражданина или его законного представителя допускается по запросу органов дознания и следствия, и суда в связи с проведением расследования или судебным разбирательством(ФЗ РФ от 21 ноября 2011 г. N 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации")

В соответствии с п.4 ч.1 ст.13 ФЗ «О полиции» полиция по мотивированному запросу уполномоченных должностных лиц вправе запрашивать и получать на безвозмездной основе необходимые сведения, справки и документы, а также их копии. При этом запрос полиции может быть направлен только в рамках следующих мероприятий:

1) расследование уголовного дела или дела об административном правонарушении;

2) проведение проверки зарегистрированных в установленном порядке заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях, разрешение которых отнесено к компетенции полиции;

3) проведение оперативно-розыскных мероприятий.

Полиция также вправе требовать от организации предоставления образцов и каталогов своей продукции, технической и технологической документации и других информационных материалов, необходимых для производства экспертиз (п.17 ч.1 ст.13 ФЗ «О полиции»).

При этом запрос полиции должен быть оформлен надлежащим образом (в письменной форме, на официальном бланке, с указанием наименования подразделения полиции, исходящего номера и даты документа, фамилии и должности лица, направившего запрос, а также с указанием цели и правового основания затребования информации).

Согласно ч.4 ст.13 ФЗ «О полиции» запросы уполномоченных должностных лиц полиции обязательны для исполнения в сроки, указанные в запросе, но не позднее одного месяца с момента вручения запроса.

4. Подготовка и направление ответов на запросы

4.1. Если запрос оформлен в соответствии с требованиями законодательства, он принимается к обработке и передается в тот же день руководителю АНО «ЭСП» либо лицу, его замещающему, который определяет порядок и сроки их рассмотрения, дает по каждому из них письменное указание исполнителям.

Руководитель АНО «ЭСП» его заместители при рассмотрении и разрешении запроса обязаны:

- внимательно разобраться в их существе, в случае необходимости истребовать дополнительные материалы;
- принимать законные, обоснованные и мотивированные решения и обеспечивать своевременное и качественное их исполнение;
- сообщать в письменной форме заявителям о решениях, принятых по их запросам, со ссылками на законодательство Российской Федерации, а в случае отклонения запроса - разъяснять также порядок обжалования принятого решения.

4.2. Ответственные исполнители запросов несут ответственность за соблюдение сроков предоставление в канцелярию АНО «ЭСП» информации по вопросам своего ведения и ее достоверность.

4.3. На основании имеющейся либо представленной ответственными исполнителями информации по запросу, канцелярия АНО «ЭСП» готовит проект ответа (приложение 2).

4.4. Ответы на запросы печатаются на бланке АНО «ЭСП» установленной формы. В ответах обязательно указывается номер и дата поступившего запроса.

4.5. Ответ на запрос подписывается руководителем АНО «ЭСП» с указанием ответственного исполнителя запроса и регистрируется в « Журнале исходящей корреспонденции».

4.6. Ответ на запрос предоставляется способом, указанным в запросе (по почте, по электронной почте, либо по факсу). Если способ предоставления информации в запросе не определен, то она представляется по одному из указанных каналов связи. При этом по электронной почте направляется электронный образ документа, полученный путем сканирования оригинала ответа. Оригинал документа подшивается в дело.

4.7. Если запрашиваемая информация о деятельности АНО «ЭСП» опубликована в средствах массовой информации либо размещена на официальных сайтах в сети Интернет, в ответе на запрос указывается только название, дата выхода и номер средства массовой информации или электронный адрес официального сайта.

4.8. Запрос считается исполненным, если рассмотрены все поставленные в нем вопросы, приняты необходимые меры и даны исчерпывающие ответы заявителю.

На контроль берутся все запросы.

5. Ответственность и контроль

5.1. Ответственность за корректировку, проверку и пересмотр настоящих Правил несет, начальник службы безопасности, начальник отдела по защите информации .

5.2. Ответственность за правильное применение настоящих Правил несут руководители структурных подразделений.

5.3. Для проверки фактов, изложенных в запросах, при необходимости организуются служебные проверки в соответствии с законодательством Российской Федерации.

5.4. По результатам служебной проверки составляется мотивированное заключение, которое должно содержать объективный анализ собранных материалов. Если при проверке выявлены факты совершения административного правонарушения или состава преступления информация передается незамедлительно в правоохранительные органы. Результаты служебной проверки докладываются руководителю АНО «ЭСП».

5.5. Контроль за обеспечением доступа к информации осуществляет руководитель АНО «ЭСП».

5.6. Текущий контроль за правомерными ответами на запросы осуществляется лицом, ответственным за организацию обработки персональных данных в АНО «ЭСП»

5.7. Нарушение установленных Правил рассмотрения запросов влечет в отношении виновных должностных лиц дисциплинарную, административную, гражданскую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение 1
*к «*Правилам работы с запросами субъектов персональных данных
АНО «ЭСП»

Главному врачу АНО «ЭСП»
К.С. Горелик

от _____
(указать, если законный представитель субъекта ПДн)
_____
адрес: _____
_____
паспорт _____№_____ выдан _____
_____
_____

ЗАПРОС.

В соответствии со статьей 14 закона «О персональных данных», я имею право получить от вас сведения о наличии моих персональных данных. Прошу вас предоставить мне следующую информацию:
_____
_____
Ответ на настоящий запрос прошу выдать
_____
(способ предоставления информации по запросу)
в предусмотренный законом срок.

С уважением, _____
(подпись)

«_____ » _____ 20_____

Приложение 2
*к «*Правилам работы с запросами субъектов персональных данных
в АНО «ЭСП»

_____
(наименование организации;

_____
(ФИО субъекта ПДн от кого запрос)

На Ваш запрос №_____ от « » _____ 20_____ г. администрация АНО «ЭСП» относительно обработки запрашиваемых персональных данных сообщает следующее_____
_____
_____

Главный врач АНО «ЭСП» К.С. Горелик

Правила
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. Общие положения

1.1. Настоящие правила определяют основания, форму и порядок осуществления в АНО «ЭСП» внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных и политике в отношении обработки персональных данных.

1.2. Настоящие правила разработаны в соответствии с:

- **Федеральным законом** Российской Федерации от 27.07.2006 N 152-ФЗ "О персональных данных" (далее - Федеральный закон N 152-ФЗ);
- **постановлением** Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" (далее - постановление Правительства N 1119);
- **постановлением** Правительства Российской Федерации от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правыми актами, операторами, являющимися государственными или муниципальными органами" (далее - постановление Правительства N 211).

1.3. Основные понятия и термины, используемые в настоящих правилах, применяются в значениях, определённых **статьёй 3** Федерального закона N 152-ФЗ.

2. Основание проведения контроля и сроки

2.1. Основанием для проведения внутреннего контроля являются требования **Федерального закона** N 152-ФЗ (**часть 1, статья 18.1**), постановление Правительства N 1119 (**п. 17**) и постановление Правительства N 211 (**п. 1 д**).

2.2. Внутренний контроль осуществляется путём проведения периодических проверок и контроля выполнения требований, установленных нормативными правовыми актами Российской Федерации в сфере персональных данных, а также локальных актов АНО «ЭСП» устанавливающих порядок обработки и защиты персональных данных при их обработке в информационных системах АНО «ЭСП».

2.3. Периодические проверки проводятся не реже 1 раза в три года.

3. Порядок проведения контроля

3.1. Контроль выполнения требований к защите персональных данных проводит Комиссия, назначенная приказом главного врача АНО «ЭСП» или на договорной основе юридическое лицо (индивидуальный предприниматель), имеющее лицензию на осуществление деятельности по технической защите конфиденциальной информации.

3.2. Состав Комиссии - не менее 3-х человек, включая ответственного за организацию обработки персональных данных. Все члены комиссии при принятии решения обладают равными правами.

3.3. Комиссия при проведении проверки обязана:

провести анализ реализации мер, направленных на обеспечение выполнения АНО «ЭСП» обязанностей, предусмотренных **Федеральным законом** N 152-ФЗ (**статья 18.1**, **статья 19**);

провести анализ выполнения АНО «ЭСП» **требований** по определению и обеспечению уровня защищённости персональных данных, утверждённых **постановлением** Правительства N 1119;

провести анализ выполнения АНО «ЭСП» **требований**, утверждённых **постановлением** Правительства N 211;

провести анализ выполнения АНО «ЭСП» принятых локальных актов по вопросам обработки и защиты персональных данных;

провести анализ реализации АНО «ЭСП» **организационных и технических мер** по обеспечению безопасности персональных данных, утверждённых **приказом** ФСТЭК России от

18.02.2013 N 21 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных";
провести анализ состава оборудования, программных средств, включая средства защиты информаций, входящих в состав информационных систем персональных данных АНО «ЭСП» (далее - ИСПДн) на соответствие Техническому паспорту ИСПДн;
своевременно и в полной мере исполнять предоставленные полномочия по предупреждению, выявлению и пресечению нарушений требований к защите персональных данных, установленных законодательными и нормативными правовыми актами Российской Федерации.

3.4. Комиссия при проведении проверки вправе:
запрашивать и получать необходимые документы (сведения) для достижения целей проведения внутреннего контроля;
получать временный доступ к ресурсам ИСПДн в части касающейся её полномочий;
принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований к защите персональных данных;
вносить главному врачу АНО «ЭСП» предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении требований к защите персональных данных, установленных законодательными и нормативными правовыми актами Российской Федерации.

3.5. При проведении проверки члены Комиссии не вправе:
требовать представления документов и сведений, не относящихся к предмету проверки;
распространять информацию и сведения конфиденциального характера, полученные при проведении проверки.

3.6. По результатам проверки составляется Акт проверки, который подписывается членами комиссии и представляется главному врачу АНО «ЭСП» для принятия соответствующего решения.

3.7. В Акте отражаются сведения о результатах проверки, в том числе о выявленных нарушениях требований законодательных и нормативных правовых актов Российской Федерации в области защиты персональных данных, об их характере и о лицах, допустивших указанные нарушения, а также меры, необходимые для устранения выявленных нарушений.

3.8. Акт должен содержать заключение о соответствии или несоответствии обработки персональных данных требованиям к защите персональных данных установленным **Федеральным законом** Российской Федерации от 27.07.2006 N 152-ФЗ "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами, а также локальным актам АНО «ЭСП» по вопросам обработки и защиты персональных данных.

4. Заключительные положения

4.1. Сотрудники, определённые приказом главного врача АНО «ЭСП» как пользователи, участвующие в обработке персональных данных, должны ознакомиться с настоящими правилами проведения внутреннего контроля.

4.2. Обязанность доводить до сведения работников АНО «ЭСП» правила внутреннего контроля лежит на ответственном за организацию обработки персональных данных.

Правила
обработки персональных данных без использования средств автоматизации

1. Введение

1.1. Настоящие правила определяют порядок действий работников АНО «ЭСП» при обработке персональных данных, осуществляемой без использования средств автоматизации.

1.2. Ответственность за организацию выполнения требований настоящих правил несёт ответственный за организацию обработки персональных данных.

1.3. Все работники (служащие) АНО «ЭСП», участвующие в обработке персональных данных без использования средств автоматизации должны быть ознакомлены с настоящими правилами под роспись в листе ознакомлений.

2. Обособление персональных данных

2.1. С целью организации обработки и защиты персональных данных от несанкционированного доступа, персональные данные, обрабатываемые без использования средств автоматизации фиксируются отдельно от другой информации на отдельных носителях информации.

3. Разделение и уничтожение персональных данных

3.1. С целью обеспечения целостности, доступности и конфиденциальности персональных данных, обрабатываемых без средств автоматизации, в АНО «ЭСП» осуществляют процедуры разделения и уничтожения персональных данных.

3.2. Процедура разделения персональных данных производится в следующих случаях:
- изменилась категория части персональных данных, расположенных на одном материальном носителе. Цели обработки изменённой категории несовместимы с целями остальной части персональных данных;
- необходимо использовать или распространить часть персональных данных, находящихся на одном материальном носителе, независимо от остальных персональных данных;
- необходимо блокировать или уничтожить часть персональных данных, находящихся на одном материальном носителе.

3.3. Процедура разделения заключается в копировании требуемой части персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, на новый материальный носитель с последующим уничтожением персональных данных на исходном материальном носителе и использованием персональных данных на новом носителе по назначению.

3.4. Уничтожение персональных данных, находящихся на определённом материальном носителе, осуществляется способом, исключающим восстановление уничтоженных персональных данных и изменения в доступности, целостности и конфиденциальности других персональных данных, находящихся на этом же материальном носителе.

3.5. Процедуры разделения и уничтожения персональных данных контролирует ответственный за организацию обработки персональных данных.

4. Управление доступом к персональным данным

4.1. В целях обеспечения доступа к персональным данным, обрабатываемым без использования средств автоматизации в АНО «ЭСП» утверждается Перечень мест хранения материальных носителей персональных данных.

4.2. Места хранения материальных носителей персональных данных должны исключать несанкционированный доступ к ним.

4.3. В Перечне мест хранения материальных носителей персональных данных указываются категории персональных данных которые находятся в каждом хранилище, также

перечень лиц, имеющих доступ к персональным данных находящимся в хранилище, а также Ф.И.О. ответственного за хранилище.

4.4. Форма Перечня мест хранения материальных носителей персональных данных приведена в **Приложении** к настоящим Правилам.

4.5. Ведение перечня, его актуализацию и сохранность обеспечивает ответственный за организацию обработки персональных данных.

5. Нормативные и правовые документы

5.1. **Федеральный закон** от 27 июля 2006 г. N 152-ФЗ "О персональных данных".

5.2. **Постановление** Правительства Российской Федерации от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".

Приложение
к «Правилам обработки персональных данных без использования средств автоматизации»

Перечень
мест хранения материальных носителей персональных данных

N п/п	Место расположение хранилища (номер комнаты, шкафа (сейфа))	Категория персональных данных	Перечень лиц, допущенных к хранилищу	Ф.И.О. ответственного за хранилище

Ответственный за организацию обработки персональных данных:

_____ _____ _____
(подпись) (Ф.И.О.) (дата)

Инструкция
ответственного за организацию обработки персональных данных

1. Общие положения

1.1. Настоящая Инструкция определяет права, обязанности, задачи, функции ответственного за организацию обработки персональных данных (далее - ПДн) при их обработке в информационных системах персональных данных (далее - ИСПДн) АНО «ЭСП» .

1.2. Ответственный за организацию обработки персональных данных получает указания непосредственно от главного врача АНО «ЭСП» , и подотчётен ему.

2. Обязанности ответственного за организацию обработки ПДн

2.1. Знать и выполнять требования законодательства РФ и локальных актов АНО «ЭСП», устанавливающих правила обработки и защиты персональных данных.

2.2. При эксплуатации ИСПДн ответственный за организацию обработки персональных данных обязан:

- Контролировать выполнение и принимать меры к выполнению требований организационно-распорядительной документации (далее - ОРД) регламентирующей порядок обработки персональных данных;
- Планировать, координировать и контролировать действия администратора безопасности и системных администраторов при выполнении работ, предусмотренных организационно-распорядительной документацией по защите персональных данных и документами, определяющими политику АНО «ЭСП» в отношении обработки персональных данных;
- Организовать обучение и контроль знания пользователями ИСПДн правил обработки и защиты персональных данных;
- Контролировать изменения в конфигурации ИСПДн и последствия этих изменений. Организовывать работы по восстановлению конфигурации ИСПДн и её системе защиты;
- Контролировать уровень защищённости персональных данных, обрабатываемых в ИСПДн. Организовывать работы по доработке системы защиты персональных данных с целью обеспечения установленного уровня защищённости ПДн, обрабатываемых в ИСПДн.

3. Права ответственного за организацию обработки ПДн

3.1. Издавать распоряжения по АНО «ЭСП» в части реализации мер по защите ПДн, обрабатываемых в ИСПДн, и мер по организации обработки ПДн.

3.2. Привлекать к действиям, связанным с защитой и обработкой ПДн всех пользователей ИСПДн, а также сотрудников АНО «ЭСП», не являющихся пользователями ИСПДн.

3.3. Вносить предложения по организации и материальному обеспечению работ по защите ПДн, обрабатываемых в ИСПДн АНО «ЭСП».

3.4. Принимать решение об изменениях в базовой конфигурации ИСПДн и её системе защиты, если при этом не требуется переаттестация ИСПДн на соответствие требованиям безопасности персональных данных.

4. Ответственность

4.1. На ответственного за организацию обработки персональных данных возлагается ответственность:

- за организацию соблюдение режима конфиденциальности персональных данных;
- за правильность понимания и полноту выполнения задач, функций, прав и обязанностей, возложенных на него по организации защиты и организации обработки ПДн;
- за соблюдение требований локальных актов по вопросам обработки и защиты ПДн.

4.2. Ответственный за организацию обработки персональных данных несёт ответственность, предусмотренную законодательством Российской Федерации.