



№ 2
№ 48
2019 года

«РАССМОТРЕНО»
Председатель профкома
филиала
(подпись)
(В.П.Карпова)
« » 2019г.

№ 10
филиала
(подпись)
(О.В.Сабасв)
2019г.

ПОЛОЖЕНИЕ

О защите персональных данных пациентов филиала ГАУЗ «РКЦД» «Набережночелнинский противотуберкулезный диспансер»

1. Общие положения

1.1. Настоящее Положение определяет порядок создания, обработки и защиты персональных данных пациентов филиала ГАУЗ «РКЦД» «Набережночелнинский противотуберкулезный диспансер» (далее - Учреждение-оператор).

1.2. Настоящее Положение разработано на основании:

- Конституции РФ от 12 декабря 1993 г. (ст. 2, 17-24, 41);
- часть 1 и 2, часть 4 Гражданского кодекса РФ;
- Указа Президента РФ от 06 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Федерального закона от 02 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;
- Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Федерального закона Российской Федерации от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;
- Постановления Правительства Российской Федерации от 21 марта 2012 г. № 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»;
- Постановления Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

- Постановления Правительства РФ от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Регламентирующих документов ФСТЭК России и ФСБ России об обеспечении безопасности персональных данных:
 - Приказа ФСТЭК России от 18.02.2013 N 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
 - «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК РФ 14 февраля 2008 г.);
 - «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Выписка) (утв. ФСТЭК РФ 15 февраля 2008 г.);
 - Приказа ФСТЭК России от 18.02.2013 N 21 "Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

1.3. Целью настоящего Положения является определение порядка обработки персональных данных пациентов Учреждения-оператора, (согласно Перечня персональных данных, указанных в разделе 3 настоящего Положения); обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а также установление ответственности должностных лиц, имеющих доступ к персональным данным пациентов, за невыполнение требований и норм, регулирующих обработку и защиту персональных данных.

1.4 Персональные данные пациентов относятся к категории конфиденциальной информации. Конфиденциальность, сохранность и защита персональных данных обеспечиваются отнесением их к сфере негосударственной (служебной, профессиональной) тайны.

2. Основные понятия, используемые в настоящем Положении

Для целей настоящего Положения применяются следующие термины и определения:

Оператор – Учреждение-оператор 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.

Пациенты (субъекты персональных данных) — физические лица, обратившиеся к Учреждению-оператору с целью получения медицинского обслуживания, либо состоящие в иных гражданско-правовых отношениях с Учреждением-оператором по вопросам получения медицинских услуг.

Врачебная тайна — соблюдение конфиденциальности информации о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иных сведений, полученных при его обследовании и лечении.

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

Документы, содержащие персональные данные пациента — документы, необходимые для осуществления действий в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг, а также для оформления договорных отношений.

Обработка персональных данных пациента — 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 пациента.

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.

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

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.

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

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

Конфиденциальность персональных данных — операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законодательством.

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

Общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных

данных или на которые в соответствии с Федеральным законодательством не распространяется требование соблюдения конфиденциальности.

Лица, допущенные к персональным данным – работники учреждения, которые в силу своих должностных обязанностей либо занимаемой должности осуществляют обработку персональных данных, либо совершающие действия (операции) с персональными данными.

3. Понятие, состав, цели и сроки обработки персональных данных

3.1. В состав обрабатываемых в Учреждении-оператора персональных данных пациентов могут входить:

- анкетные данные (фамилия, имя, отчество, число, месяц, год рождения), пол, паспортные данные, адрес регистрации, адрес места жительства, должность, место работы пациента (законного представителя, опекуна, попечителя несовершеннолетнего ребенка), сведения об образовании, контактные телефоны, адрес электронной почты, номер страхового свидетельства государственного пенсионного страхования, данные о присвоении ИНН, семейное положение, состав семьи; фамилия, имена, отчества, даты рождения детей; фамилия, имя, отчество, должность и место работы супруга(и), данные об инвалидности, периодических медицинских осмотров, о наличии прививок, сведения о фактах обращения пациентов за оказанием медицинской помощи, состоянии их здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, которые составляют врачебную тайну, сведения о социальных льготах.

3.2. Все персональные сведения о пациентах Учреждение-оператор может получить только от них самих. В случаях, когда Учреждение-оператор может получить необходимые персональные данные пациентов только у третьего лица, оно должно уведомить об этом пациентов и получить от них письменное согласие.

3.3. Учреждение-оператор обязано сообщать пациентам о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа пациентов дать письменное согласие на их получение.

3.4. Персональные данные пациентов являются конфиденциальной информацией и не могут быть использованы учреждением-оператором или любым иным лицом в личных целях.

3.5. Учреждение-оператор разрабатывает меры защиты персональных данных работников и пациентов.

3.6. Информация о персональных данных может содержаться:

- на бумажных носителях;
- на электронных носителях;
- в информационно-телекоммуникационных сетях и иных информационных системах.

3.7. Учреждение-оператор использует следующие способы обработки персональных данных:

- автоматизированная обработка;
- без использования средств автоматизации;
- смешанная обработка (с применением объектов вычислительной техники).

Учреждение-оператор самостоятельно устанавливает способы обработки персональных данных в зависимости от целей такой обработки и материально-технических возможностей учреждения.

При обработке персональных данных с применением объектов вычислительной техники должностные лица, осуществляющие такую обработку (пользователи объектов вычислительной техники), должны быть ознакомлены под роспись с локальными нормативными актами Учреждения-оператора, устанавливающими порядок применения объектов вычислительной техники.

3.8. Персональные данные пациентов Учреждения-оператора могут содержаться в следующих документах:

а) медицинские документы: история болезни пациентов, история родов, история развития новорожденного, материнский паспорт, медицинская карта стационарного больного, медицинская карта пациента, получающего медицинскую помощь в амбулаторных условиях, медицинская карта, обменная карта (медицинские справки, результаты анализов и обследований пациентов, врачебно-консультативное заключение, медицинская карта стационарного больного протоколы заседания ВК, пр.);

б) паспорт здоровья;

в) паспорт или иной документ, удостоверяющий личность;

г) для иностранных граждан: паспорт иностранного гражданина, вид на жительство, разрешение на временное проживание, свидетельство о временном убежище, миграционная карта, отрывной бланк уведомления о прибытии иностранного гражданина в место пребывания;

д) страховое свидетельство государственного пенсионного страхования (СНИЛС), реквизиты полис ОМС (ДМС), миграционная карта, отрывной бланк уведомления о прибытии иностранного гражданина в место пребывания;

е) договор о добровольном медицинском страховании работников правоохранительных органов и других организаций, гарантийное письмо об оплате;

ж) другие документы, несущие персональные данные и не запрещенные на территории РФ.

3.9. Учреждение-оператор осуществляет обработку данных о состоянии здоровья пациентов в целях оказания медицинских услуг, установления медицинского диагноза при этом обработка персональных данных осуществляется лицами, профессионально занимающимися медицинской деятельностью и обязанными в соответствии с законодательством Российской Федерации сохранять врачебную тайну.

3.10. Обработка персональных данных работников и обучающихся осуществляется в целях:

а) обеспечения соблюдения Конституции Российской Федерации, федеральных законов, иных нормативных правовых актов Российской Федерации и реализации уставных задач Учреждения-оператора.

б) медико-профилактических услуг;

в) медицинских и медико-социальных услуг;

г) установления диагноза и т.д.

3.11. Обработка персональных данных необходима для защиты жизни, здоровья и других жизненно важных интересов субъектов.

3.12. Сроки обработки персональных данных:

- Общий срок обработки персональных данных определяется периодом времени, в течение которого ЛПУ осуществляет действия (операции) в отношении персональных данных, обусловленные заявленными целями их обработки, в том числе хранение персональных данных.
- Обработка персональных данных начинается с момента их получения ЛПУ и заканчивается:
 - по достижении заранее заявленных целей обработки;
 - по факту утраты необходимости в достижении заранее заявленных целей обработки.

4. Лица, допущенные к персональным данным.

4.1. Доступ к персональным данным пациентов имеют работники Учреждения-оператора: главный врач, заместители главного врача, главный бухгалтер; заведующие отделений всех структурных подразделений; врачи; средний медицинский персонал; младший медицинский персонал; работники регистратуры, секретарь руководителя, операторы, инженер-программист, обеспечивающие работоспособность аппаратно-программных средств, предназначенных для автоматизированной обработки персональных данных; юрист; работники отдела кадров; работники экономического отдела; работники бухгалтерии, иные лица в силу своих должностных обязанностей.

5. Случаи, когда для обработки персональных данных не требуется согласия субъекта персональных данных

5.1. Обработка персональных данных осуществляется на основании федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия оператора;

5.2. Обработка персональных данных осуществляется в целях исполнения договора, одной из сторон которого является субъект персональных данных;

5.3. Обработка персональных данных осуществляется для статистических или иных научных целей при условии обязательного обезличивания персональных данных;

5.4. Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

5.5. Обработка персональных данных необходима для доставки почтовых отправок организациями почтовой связи, для осуществления операторами электросвязи расчетов с пользователями услуг связи за оказанные услуги связи, а также для рассмотрения претензий пользователей услугами связи.

6. Общие принципы и условия обработки персональных данных пациентов

6.1. Обработка персональных данных пациента осуществляется на основе принципов:

1. Обработка персональных данных должна осуществляться на законной и справедливой основе.
2. Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.
3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
4. Обработке подлежат только персональные данные, которые отвечают целям их обработки.
5. Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.
6. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Учреждение-оператор должно принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
7. 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 № 152-ФЗ, 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 законодательством.

6.2. В целях обеспечения прав и свобод человека и гражданина Учреждение-оператор и его представители при обработке персональных данных пациента обязаны соблюдать следующие общие требования:

Обработка персональных данных пациента может осуществляться исключительно в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг, оформления договорных

отношений с пациентом при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну в соответствии с законодательством Российской Федерации.

□ Все персональные данные пациента следует получать у него самого или у его полномочного представителя. Если персональные данные пациента, возможно, получить только у третьей стороны, то пациент должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие.

□ При определении объема и содержания обрабатываемых персональных данных пациента, Учреждение-оператор должно руководствоваться Конституцией Российской Федерации, Федеральным законом № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», законодательством РФ в сфере защиты персональных данных и обработки информации, Уставом Учреждения-оператора и иными локальными нормативными актами в области защиты персональных данных.

□ Учреждение-оператор не имеет права получать и обрабатывать персональные данные пациента, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, интимной жизни, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ.

□ Запрещается принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении пациента или иным образом затрагивающих его права и законные интересы, за исключением случаев, предусмотренных Федеральным законом № 152-ФЗ.

□ Решение, порождающее юридические последствия в отношении пациента или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме пациента или в случаях, предусмотренных Федеральным законодательством, устанавливающим также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

□ Учреждение-оператор обязано разъяснить пациенту порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты пациентом своих прав и законных интересов.

□ Учреждение-оператор обязано рассмотреть возражение в течение тридцати дней со дня его получения и уведомить пациента о результатах рассмотрения такого возражения.

□ Защита персональных данных пациента от неправомерного их использования или утраты должна быть обеспечена Учреждением-оператором за счет своих средств, в порядке, установленном Федеральным законодательством и другими нормативными документами.

6.3. Учреждение-оператор вправе поручить обработку персональных данных другому лицу с согласия пациента, если иное не предусмотрено Федеральным законом № 152-ФЗ, на основании заключаемого с этим лицом договора, в том числе государственного или муниципального контракта, либо путем принятия государственным или муниципальным органом соответствующего акта (далее — поручение Учреждения-оператора). Лицо, осуществляющее обработку персональных данных по поручению Учреждения-оператора, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом № 152-ФЗ. В поручении Учреждения-оператора должны быть определены перечень действий (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, и цели обработки, должна быть установлена обязанность такого лица соблюдать конфиденциальность персональных

данных и обеспечивать безопасность персональных данных при их обработке, а также должны быть указаны требования к защите обрабатываемых персональных данных в соответствии со статьей 19 Федерального закона № 152-ФЗ.

6.4. Лицо, осуществляющее обработку персональных данных по поручению Учреждения-оператора, не обязано получать согласие пациента на обработку его персональных данных.

6.5. В случае если Учреждение-оператор поручает обработку персональных данных другому лицу, ответственность перед пациентом за действия указанного лица несет Учреждение-оператор. Лицо, осуществляющее обработку персональных данных по поручению Учреждения-оператора, несет ответственность перед Учреждением-оператором.

7. Получение персональных данных пациента

7.1. Получение персональных данных преимущественно осуществляется путем представления их самим пациентом, на основании его письменного согласия за исключением случаев прямо предусмотренных действующим законодательством РФ.

7.2. Документы, содержащие персональные данные, создаются путём:

- а) копирования оригиналов (паспорт, свидетельство ИНН, свидетельство государственного пенсионного страхования, страховой медицинский полис др.);
- б) внесения сведений в учётные формы (на бумажных и электронных носителях);
- в) получения оригиналов необходимых документов.

В случаях, предусмотренных Федеральным законодательством, обработка персональных данных осуществляется только с согласия пациента в письменной форме. (Равнозначным содержащему собственноручную подпись пациента согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с Федеральным законом № 152-ФЗ электронной подписью. Согласие пациента в письменной форме на обработку его персональных данных должно включать в себя, в частности:

1. фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
2. фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
3. наименование или фамилию, имя, отчество и адрес Учреждения-оператора, получающего согласие субъекта персональных данных;
4. цель обработки персональных данных;
5. перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

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

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

8. срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено Федеральным законодательством;

9. подпись субъекта персональных данных.

Для обработки персональных данных, содержащихся в согласии в письменной форме пациента на обработку его персональных данных, дополнительное согласие не требуется.

7.3. В случае недееспособности пациента, не достижения пациентом возраста 15 лет, смерти пациента, в других случаях согласие на обработку его персональных данных дает в письменной форме его законный представитель.

7.4. В случае необходимости проверки персональных данных пациента Учреждение-оператор заблаговременно должно сообщить об этом пациенту, о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа пациента дать письменное согласие на их получение. Учреждение-оператор при обработке персональных данных пациентов обязано принимать необходимые правовые, организационные и технические меры или обеспечивать 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.

8. Хранение и использование персональных данных пациентов

8.1. Информация персонального характера пациента хранится и обрабатывается с соблюдением требований действующего Российского законодательства о защите персональных данных.

8.2. Порядок хранения документов, содержащих персональные данные пациентов осуществлять в соответствии с:

- Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

8.3. Обработка персональных данных пациентов осуществляется смешанным путем:

- неавтоматизированным способом обработки персональных данных;
- автоматизированным способом обработки персональных данных (с помощью ПЭВМ и специальных программных продуктов).

8.4. Персональные данные пациентов хранятся на бумажных носителях и в электронном виде.

8.5. Хранение содержащих персональные данные пациентов и оконченных производством документов, содержащих персональные данные пациентов, осуществляется во внутренних помещениях Учреждения-оператора, а также в помещениях Учреждения-оператора, предназначенных для хранения отработанной документации.

8.6. Возможна передача персональных данных пациентов по внутренней сети организации с использованием технических и программных средств защиты информации, с доступом только для работников Учреждения-оператора, допущенных к работе с персональными данными пациентов и только в объеме, необходимом данным работникам для выполнения своих должностных обязанностей.

8.7. Хранение персональных данных пациентов осуществляется не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении.

Хранение документов, содержащих персональные данные пациентов, осуществляется в течение установленных действующими нормативными актами сроков хранения данных документов. По истечении установленных сроков хранения документы подлежат уничтожению.

8.8. Учреждение-оператор обеспечивает ограничение доступа к персональным данным пациентов лицам, не уполномоченным Федеральным законодательством, либо работодателем для получения соответствующих сведений.

8.9. Доступ к персональным данным пациентов имеют только работники Учреждения-оператора, подписавшие обязательство о неразглашении конфиденциальной информации. Персональные данные выдаются, в объеме, необходимом для выполнения своих должностных обязанностей.

8.10. Ответственными за организацию и осуществление хранения персональных данных пациентов Учреждения-оператора являются руководители структурных подразделений.

8.11. Контроль за обеспечением безопасности персональных данных при их обработке в информационных системах персональных данных в соответствии с требованиями законодательства РФ возлагается на руководителей структурных подразделений.

8.12. Требования к помещениям, в которых производится обработка персональных данных:

8.12.1. Размещение оборудования информационных систем персональных данных, специального оборудования и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

8.12.2. Помещения, в которых располагаются технические средства информационных систем персональных данных или хранятся носители персональных данных, должны соответствовать требованиям пожарной безопасности, установленным действующим законодательством Российской Федерации.

8.12.3. Определение уровня специального оборудования помещения осуществляется специально создаваемой комиссией. По результатам определения

класса и обследования помещения на предмет его соответствия такому классу составляются акты.

8.12.4. Кроме указанных мер по специальному оборудованию и охране помещений, в которых устанавливаются криптографические средства защиты информации или осуществляется их хранение, реализуются дополнительные требования, определяемые методическими документами Федеральной службы безопасности России.

9. Защита персональных данных пациентов

9.1. Учреждение-оператор при обработке персональных данных пациентов обязано принимать необходимые правовые, организационные и технические меры или обеспечивать 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.

9.2. Обеспечение безопасности персональных данных пациентов достигается, в частности:

1. определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;
2. 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 защищенности персональных данных;
3. применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
4. оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;
5. учетом машинных носителей персональных данных;
6. обнаружением фактов несанкционированного доступа к персональным данным и принятием мер;
7. восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
8. установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9. контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

9.3. Для обеспечения безопасности персональных данных пациентов при неавтоматизированной обработке предпринимаются следующие меры:

9.3.1. Определяются места хранения персональных данных (согласно настоящего Положения), которые оснащаются следующими средствами защиты:

- В кабинетах, где осуществляется хранение документов, содержащих персональные данные пациентов, имеются сейфы, шкафы, стеллажи, тумбы.
- Дополнительно кабинеты, где осуществляется хранение документов, содержащих персональные данные пациентов, оборудованы замками и системой пожарной сигнализации.

9.3.2. Все действия при неавтоматизированной обработке персональных данных пациентов осуществляются только должностными лицами Учреждения-оператора, допущенных к персональным данным, и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.

9.3.3. При обработке персональных данных на материальных носителях не допускается фиксация на одном материальном носителе тех данных, цели обработки которых заведомо не совместимы.

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если не имеется возможности осуществлять их отдельно, должны быть приняты следующие меры:

1. при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) только копия;
2. при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

Уничтожение или обезличивание 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 (удаление).

Персональные данные пациентов, содержащиеся на материальных носителях, уничтожаются по Акту об уничтожении персональных данных.

Эти правила применяются также в случае, если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя — путем фиксации на том же материальном носителе сведений о вносимых в них изменениях, либо путем изготовления нового материального носителя с уточненными персональными данными.

9.3.4. Обработка персональных данных осуществляется с соблюдением порядка, предусмотренного Постановлением Правительства от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

9.4. Для обеспечения безопасности персональных данных пациентов при автоматизированной обработке предпринимаются следующие меры:

9.4.1. Все действия при автоматизированной обработке персональных данных пациентов осуществляются только должностными лицами, допущенных к персональным данным, и только в объеме, необходимом данным лицам для выполнения своей трудовой функции.

9.4.2. Персональные компьютеры, имеющие доступ к базам хранения персональных данных пациентов, защищены паролями доступа. Пароли устанавливаются работниками отдела АСУП и сообщаются индивидуально работнику, допущенному к работе с персональными данными и осуществляющему обработку персональных данных пациентов на данном ПК.

9.4.3. Иные меры, предусмотренные Положением по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

9.4.4. Обработка персональных данных осуществляется с соблюдением порядка, предусмотренного Постановлением Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

9.5. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, в соответствии с Приказами по архивному делу, или продлевается на основании заключения экспертной комиссии Учреждения-оператора, если иное не определено законодательством РФ.

10. Передача персональных данных пациентов третьим лицам

10.1. Передача персональных данных пациентов третьим лицам осуществляется Учреждением-оператором только с письменного согласия пациента, с подтверждающей визой Главного врача либо заместителя главного врача по медицинской части, за исключением случаев, если:

1. передача необходима для защиты жизни и здоровья пациента, либо других лиц, и получение его согласия невозможно;
2. в целях обследования и лечения пациента, не способного из-за своего состояния выразить свою волю;
3. в случаях, предусмотренных ст.13 ФЗ-323 Об основах охраны здоровья граждан, в том числе по запросу органов дознания, следствия, прокуратуры и суда в связи с

проведением расследования или судебным разбирательством, в соответствии с Законом об оперативно-розыскной деятельности;

4. в случае оказания помощи несовершеннолетнему в возрасте до 15 лет, для информирования его родителей или законных представителей;

5. при наличии оснований, позволяющих полагать, что права и интересы пациента могут быть нарушены противоправными действиями других лиц;

6. в иных случаях, прямо предусмотренных Федеральным законодательством.

Лица, которым в установленном Федеральным законом №152-ФЗ порядке переданы сведения, составляющие персональные данные пациента, несут дисциплинарную, административную или уголовную ответственность за разглашение в соответствии с законодательством Российской Федерации.

10.2. Передача персональных данных пациента третьим лицам осуществляется на основании запроса третьего лица с разрешающей визой главного врача (заведующего поликлиникой) при условии соблюдения требований, предусмотренных п. 7.1 настоящего Положения.

В случае если лицо, обратившееся с запросом, не уполномочено Федеральным законодательством на получение персональных данных пациента, либо отсутствует письменное согласие пациента на передачу его персональных данных, Учреждение-оператор обязано отказать в предоставлении персональных данных. В данном случае лицу, обратившемуся с запросом, выдается мотивированный отказ в предоставлении персональных данных в письменной форме, копия отказа хранится у Учреждения-оператора.

11. Общедоступные источники персональных данных пациентов

11.1. Включение персональных данных пациента в общедоступные источники персональных данных возможно только при наличии его письменного согласия.

11.2. При обезличивании персональных данных согласие пациента на включение персональных данных в общедоступные источники персональных данных не требуется.

11.3. Сведения о пациентах могут быть исключены из общедоступных источников персональных данных по требованию самого пациента, либо по решению суда или иных уполномоченных государственных органов.

12. Права и обязанности пациента в области защиты его персональных данных

12.1. В целях обеспечения защиты персональных данных, хранящихся у Учреждения-оператора, пациенты имеют право на:

- полную информацию о составе и содержимом их персональных данных, а также способе обработки этих данных;
- свободный доступ к своим персональным данным.

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

1. подтверждение факта обработки персональных данных Учреждением-оператором;
2. правовые основания и цели обработки персональных данных;
3. цели и применяемые Учреждением-оператором способы обработки персональных данных;
4. наименование и место нахождения Учреждения-оператора, сведения о лицах (за исключением работников Учреждения-оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Учреждением-оператором или на основании Федерального закона № 152-ФЗ;
5. обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом № 152-ФЗ;
6. сроки обработки персональных данных, в том числе сроки их хранения;
7. порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;
8. информацию об осуществленной или о предполагаемой трансграничной передаче данных;
9. наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Учреждения-оператора, если обработка поручена или будет поручена такому лицу;
10. иные сведения, предусмотренные Федеральным законом № 152-ФЗ или Федеральным законодательством.

Сведения должны быть предоставлены пациенту Учреждением-оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

Сведения предоставляются пациенту или его законному представителю Учреждением-оператором при обращении, либо при получении запроса пациента или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность пациента или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие пациента в отношениях с Учреждением-оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Учреждением-оператором, подпись пациента или его законного представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации. *(Форма запроса в Приложении № 1 к настоящему Положению).*

В случае если сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления пациенту по его запросу, пациент вправе обратиться

повторно к Учреждению-оператору или направить ему повторный запрос в целях получения сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен Федеральным законодательством, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Пациент вправе требовать от Учреждения-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.

12.2. В случае выявления неправомерной обработки персональных данных при обращении пациента или его законного представителя, либо по запросу пациента или его законного представителя, либо уполномоченного органа по защите прав субъектов персональных данных, Учреждение-оператор обязано осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении пациента или его законного представителя, либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных, Учреждение-оператор обязано осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы пациента или третьих лиц.

12.3. В случае подтверждения факта неточности персональных данных Учреждение-оператор на основании сведений, представленных пациентом или его законным представителем, либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязано уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

12.4. В случае выявления неправомерной обработки персональных данных, осуществляемой Учреждением-оператором (или лицом, действующим по поручению Учреждения-оператора), Учреждение-оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Учреждения-оператора. В случае если обеспечить правомерность обработки персональных данных невозможно, Учреждение-оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязано уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение-оператор обязано уведомить пациента или его законного представителя, а в случае, если обращение пациента или его представителя либо запрос уполномоченного органа по защите прав

субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

12.5. В случае достижения цели обработки персональных данных Учреждение-оператор обязано прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является пациент, иным соглашением между Учреждением-оператором и пациентом, либо если Учреждение-оператор не вправе осуществлять обработку персональных данных без согласия пациента на основаниях, предусмотренных Федеральным законом № 152-ФЗ или Федеральным законодательством.

12.6. В случае отзыва пациентом согласия на обработку его персональных данных Учреждение-оператор обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Учреждением-оператором и пациентом, либо если Учреждение-оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 152-ФЗ или Федеральным законодательством. *(Форма отзыва согласия на обработку персональных данных в Приложении № 2.)*

12.7. В случае отсутствия возможности уничтожения персональных данных в течение указанного срока, Учреждение-оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения-оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен Федеральным законодательством.

12.8. Для своевременной и полной реализации своих прав, пациент обязан предоставить Учреждению-оператору достоверные персональные данные.

13. Право на обжалование действий или бездействия Учреждения-оператора

13.1. Если пациент или его законный представитель считает, что Учреждение-оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона № 152-ФЗ или иным образом нарушает его права и свободы, он вправе обжаловать действия или бездействие Учреждения-оператора в уполномоченный орган по защите прав субъектов персональных данных (Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере информационных технологий и связи) или в судебном порядке.

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

Моральный вред, причиненный пациенту вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом № 152-ФЗ, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом № 152-ФЗ, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

14. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных пациентов

14.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных пациента, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с Федеральным законодательством.

14.2. Работники Учреждения-оператора, допущенные к обработке персональных данных пациентов, за разглашение полученной в ходе своей трудовой деятельности информации, несут дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

15. Заключительные положения

15.1. Настоящее Положение вступает в силу с даты его утверждения.

15.2. При необходимости приведения настоящего Положения в соответствие с вновь принятыми законодательными актами, изменения вносятся на основании Приказа главного врача.

15.3. Настоящее Положение распространяется на всех пациентов Учреждения-оператора, а также работников Учреждения-оператора, имеющих доступ и осуществляющих перечень действий с персональными данными пациентов.

Пациенты Учреждения-оператора, а так же их законные представители имеют право, ознакомиться с настоящим Положением.

15.4. В обязанности работников, осуществляющих первичный сбор персональных данных пациента, входит получение согласия пациента на обработку его персональных данных под личную подпись.

15.5. Документы, определяющие политику в отношении обработки персональных данных пациентов, размещены на официальном сайте или информационном стенде Учреждения-оператора в течение 10 дней после их утверждения.