Приложение №12 к Приказу № 89
от 09 января 2018г.

ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ
ГБУЗ РМ «РЕСПУБЛИКАНСКАЯ КЛИНИЧЕСКАЯ БОЛЬНИЦА №1»

Саранск

СОДЕРЖАНИЕ

1.Общие положения.....3
2.Основные понятия, используемые в настоящем Положении.....5
3.Общие принципы и условия обработки персональных данных.....6
4.Получение персональных данных граждан.....8
5.Хранение и использование персональных данных граждан.....9
6.Передача персональных данных граждан третьим лицам.....10
7.Общедоступные источники персональных данных.....11
8.Обеспечение безопасности персональных данных при их обработке в ИСПДН.....11
8.1.Методы и способы защиты информации в информационных системах Учреждения. 11
8.2.Основные мероприятия по организации обеспечения безопасности персональных данных. 12
8.3.Этапы осуществления мероприятий по организации обеспечения безопасности персональных данных. 12
8.4.Обязанности сотрудников Учреждения при обработке персональных данных. 13
9.Порядок обработки персональных данных без использования средств вычислительной техники.....14
10.Права и обязанности гражданина в области защиты его персональных данных.....15
11.Ответственность за нарушение законодательства об охране ПДн.....18
Приложение 1.....19
Приложение 2.....20
Приложение 3.....21
Приложение 4.....22
Приложение 5.....23
Приложение 6.....25

1. Общие положения.

1.1. Настоящее Положение разработано в соответствии с Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным Постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119, и устанавливающими методы и способы защиты информации, применяемые для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (далее — информационные системы) Государственного бюджетного учреждения здравоохранения Республики Мордовия «Республиканская клиническая больница №1» (далее – Учреждение), а также определяет порядок создания, обработки и защиты персональных данных.

1.2. Основанием для разработки данного локального нормативного акта являются:

−Конституция Российской Федерации от 12 декабря 1993 г. (ст. 2, 17-24, 41);

−часть 1 и 2, часть 4 Гражданского кодекса Российской Федерации;

−Закон Российской Федерации от 28 июня 1991 г. № 1499-1 (ред. от 29 декабря 2006 г.) «О медицинском страховании граждан в Российской Федерации»;

−Указ Президента Российской Федерации от 06 марта 1997 г. № 188 (ред. от 23 сентября 2005 г.) «Об утверждении перечня сведений конфиденциального характера»;

−Федеральный закон Российской Федерации от 17 сентября 1998 г. № 157-ФЗ (ред. от 24 июля 2010 г.) «Об иммунопрофилактике инфекционных болезней»;

−Федеральный закон Российской Федерации от 30 марта 1999 г. № 52-ФЗ «О санитарно-эпидемиологическом благополучии населения» (ред. от 30 декабря 2008 г.);

−Федеральный закон Российской Федерации от 02 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации»;

−Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

−Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

−Федеральный закон Российской Федерации от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

−Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

−Постановление Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

−Приказ главного врача ГБУЗ РМ «Республиканская больница №1» от «28» ноября 2012 г. № 76 - од «О защите персональных данных»;

−Регламентирующие документы ФСТЭК России и ФСБ России об обеспечении безопасности персональных данных:

- Приказ ФСТЭК РФ от 05 февраля 2010 г. № 58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных» (Зарегистрировано в Минюсте РФ 19 февраля 2010 г. № 16456);
- «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК РФ 14 февраля 2008 г.);
- Приказ ФСТЭК РФ № 55, ФСБ РФ № 86, Мининформсвязи РФ № 20 от 13 февраля 2008 г. «Об утверждении Порядка проведения классификации информационных систем персональных данных» (Зарегистрировано в Минюсте

РФ 03 апреля 2008 г. № 11462);

- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК РФ 15 февраля 2008 г.);

1.3. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах, информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации и без использования таковых, а также гарантии их защиты и ответственность за нарушение норм, регулирующих обработку и защиту персональных данных.

1.4. Цель настоящего Положения – защита персональных данных, обрабатываемых в информационных системах персональных данных Учреждения, а также персональных данных работников Учреждения от несанкционированного доступа. Персональные данные являются конфиденциальной, строго охраняемой информацией. Конфиденциальность, сохранность и защита персональных данных обеспечиваются отнесением их к сфере негосударственной (служебной, профессиональной) тайны.

1.5. Общее руководство, координацию работ, организацию применения технических средств защиты и текущий контроль деятельности по защите персональных данных в Учреждении выполняет сотрудник, назначенный приказом Главного врача Учреждения.

1.6. Настоящее Положение распространяется на сведения конфиденциального характера, содержащиеся в Перечне персональных данных, утвержденном приказом. Положение вступает в силу с момента его утверждения приказом Главного врача Учреждения и действует без ограничения срока.

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

1.8. Настоящее Положение распространяется на всех субъектов, ПДн которых обрабатываются в Учреждении, а также работников Учреждения, имеющих доступ и осуществляющих перечень действий с персональными данными граждан.

1.9. Работники Учреждения подлежат ознакомлению с данным документом в порядке, предусмотренном Приказом Главного врача Учреждения, под личную подпись.

1.10. В обязанности работников, осуществляющих первичный сбор персональных данных граждан, входит получение согласия гражданина на обработку его персональных данных под личную подпись.

1.11. В настоящем Положении не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну, а также вопросы применения криптографических методов и способов защиты информации.

2. Основные понятия, используемые в настоящем Положении.

Автоматизированная обработка ПДн – обработка ПДн с помощью средств вычислительной техники.

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Администратор безопасности – субъект доступа, ответственный за защиту АС от несанкционированного доступа к информации.

Блокирование ПДн – временное прекращение сбора, систематизации, накопления, использования, распространения ПДн, в том числе их передачи.

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.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таких средств.

Конфиденциальность ПДн – обязательное для соблюдения оператором или иным получившим доступ к ПДн лицом требование не допускать их распространение без согласия субъекта ПДн или наличия иного законного основания.

Неавтоматизированная обработка ПДн – обработка персональных данных (использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных), осуществляемая без использования средств вычислительной техники.

Несанкционированный доступ к информации (НСД) – доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Обезличивание ПДн – действия, в результате которых невозможно определить принадлежность ПДн конкретному субъекту ПДн.

Обработка информации – совокупность операций сбора, накопления, ввода-вывода, приема-передачи, записи, хранения, регистрации, уничтожения, преобразования и отображения, осуществляемых над информацией.

Обработка ПДн – действия (операции) с ПДн, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПДн.

Общедоступные ПДн – ПДн, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПДн или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Объект защиты информации – информация, носитель информации или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.

Организационно-технические мероприятия по обеспечению защиты информации – совокупность действий, направленных на применение организационных мер и программно-технических способов защиты информации на объекте информатизации.

Персональные данные (ПДн) – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

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

Распространение ПДн – действия, направленные на передачу ПДн определенному кругу лиц (передача ПДн) или на ознакомление с ПДн неограниченного круга лиц, в том числе обнародование ПДн в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к ПДн каким-либо иным способом.

Уничтожение ПДн – действия, в результате которых невозможно восстановить содержание ПДн в информационной системе ПДн или в результате которых уничтожаются материальные носители ПДн.

3. Общие принципы и условия обработки персональных данных

3.1. Обработка персональных данных гражданина 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 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.

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

1) Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов; осуществления государственной политики в сфере здравоохранения, обеспечивающей необходимые условия для реализации конституционных прав гражданина Российской Федерации на получение медицинской помощи, лекарственного обеспечения и гигиенического воспитания; осуществления мероприятий, в части лицензирования медицинской, фармацевтической деятельности и деятельности, связанной с оборотом наркотических средств; реализации на территории Республики Мордовия приоритетных национальных проектов в сфере здравоохранения; реализации кадровой политики в сфере здравоохранения; реализации и развития системы управления в сфере здравоохранения; профилактики инвалидности и медицинской реабилитации инвалидов; организации санаторно-курортного лечения и оздоровления больных; участия в реализации государственной политики в области

обязательного медицинского страхования граждан в соответствии с законодательством Российской федерации и Республики Мордовия; контроля количества и качества оказанной гражданину медицинской помощи в соответствии с законодательством Российской Федерации.

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

3) При определении объема и содержания обрабатываемых персональных данных гражданина Учреждение 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 и иными локальными нормативными актами в области защиты персональных данных.

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

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

6) Решение, порождающее юридические последствия в отношении гражданина 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 гражданина или в случаях, предусмотренных Федеральным законодательством, устанавливающим также меры по обеспечению соблюдения прав и законных интересов субъекта персональных данных.

7) Учреждение обязано разъяснить гражданину 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 гражданином своих прав и законных интересов.

8) Учреждение обязано рассмотреть возражение в течение тридцати дней со дня его получения и уведомить гражданина о результатах рассмотрения такого возражения.

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

3.3. Учреждение вправе поручить обработку персональных данных другому лицу с согласия гражданина, 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). Лицо, осуществляющее обработку персональных данных по поручению Учреждения, обязано соблюдать принципы и правила обработки персональных данных, предусмотренные Федеральным законом № 152-ФЗ. В поручении Учреждения 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.

3.4. Лицо, осуществляющее обработку персональных данных по поручению Учреждения, не обязано получать согласие гражданина на обработку его персональных данных.

3.5. В случае если Учреждение поручает обработку персональных данных другому лицу, ответственность перед гражданином за действия указанного лица несет Учреждение. Лицо, осуществляющее обработку персональных данных по поручению Учреждения, несет ответственность перед Учреждением.

3.6. Надзорно-контрольные органы имеют доступ к защищаемой информации исключительно в сфере своей компетенции.

3.7. К числу массовых потребителей персональных данных вне Учреждения относятся государственные и негосударственные функциональные структуры: налоговые инспекции, правоохранительные органы, органы статистики, страховые агентства, военкоматы, пенсионные фонды, ФОМС, подразделения муниципальных органов управления и др.

3.8. Учреждение при обработке персональных данных граждан 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.

4. Получение персональных данных граждан

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

В случаях, предусмотренных Федеральным законодательством, обработка персональных данных осуществляется только с согласия гражданина в письменной форме. Равнозначным содержащему собственноручную подпись гражданина согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с Федеральным законом № 152-ФЗ электронной подписью. Согласие гражданина 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 оператора (ГБУЗ РМ «Республиканская больница №1»), 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, если обработка будет поручена такому лицу;

7) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых Учреждением 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, дополнительное согласие на обработку не требуется.

В случае недееспособности гражданина или недостижения гражданином возраста 14 лет согласие на обработку его персональных данных дает в письменной форме его законный

представитель.

4.2. В случае необходимости проверки персональных данных гражданина Учреждение заблаговременно должно сообщить об этом гражданину, о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа гражданина дать письменное согласие на их получение.

5. Хранение и использование персональных данных граждан

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

5.2. Обработка персональных данных осуществляется Учреждением смешанным путем:

– неавтоматизированным способом обработки персональных данных;

– автоматизированным способом обработки персональных данных (с помощью ПЭВМ и специальных программных продуктов).

5.3. Персональные данные граждан хранятся на бумажных носителях и в электронном виде.

5.4. Ответственные лица за хранение документов, содержащих персональные данные граждан, назначены Приказом Главного врача Учреждения.

5.5. Хранение оконченных производством документов, содержащих персональные данные граждан, осуществляется в помещениях Учреждения, предназначенных для хранения отработанной документации.

Ответственные лица за хранение оконченных производством документов, содержащих персональные данные граждан, назначены Приказом Главного врача Учреждения.

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

5.7. Хранение персональных данных граждан 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 граждан, осуществляется в течение установленных действующими нормативными актами сроков хранения данных документов. По истечении установленных сроков хранения документы подлежат уничтожению с оформлением Акта уничтожения (Приложение 3).

5.8. Учреждение обеспечивает ограничение доступа к персональным данным граждан лицам, не уполномоченным Федеральным законодательством, либо работодателем для получения соответствующих сведений.

5.9. Доступ к персональным данным граждан имеют работники Учреждения, допущенные к работе с персональными данными Приказом Главного врача Учреждения. В должностные инструкции данных работников включается пункт об обязанности сохранения информации, являющейся конфиденциальной.

6. Передача персональных данных граждан третьим лицам

6.1. Передача персональных данных граждан третьим лицам осуществляется Учреждением только с письменного согласия гражданина, с подтверждающей визой Главного врача Учреждения за исключением случаев, если:

1) передача необходима для защиты жизни и здоровья гражданина, либо других лиц, и получение его согласия невозможно;

2) в целях обследования и лечения гражданина, не способного из-за своего состояния выразить свою волю;

3) 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 14 лет, для информирования его родителей или законных представителей;

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

6) в иных случаях, прямо предусмотренных Федеральным законодательством.

6.2. В целях соблюдения Федерального законодательства и иных нормативных правовых актов Российской Федерации возможна передача персональных данных граждан:

1) для содействия в трудоустройстве, обучении, повышения их квалификации, переподготовке, проведения аттестации на квалификационную категорию, получении грамот, наград и иных форм поощрений, ведения Федеральных регистров медицинских работников - в уполномоченные региональные и Федеральные органы исполнительной власти по отрасли здравоохранение;

2) в целях выполнения необходимых условий для реализации конституционных прав граждан на охрану здоровья, получение медицинской помощи, лекарственного обеспечения, профилактики инвалидности и медицинской реабилитации инвалидов, оказания медицинской и профилактической помощи населению, санаторно-курортного лечения - в уполномоченные региональные и федеральные органы исполнительной власти в сфере здравоохранения и социального развития, федеральные и региональные Фонды, страховые медицинские организации, другие медицинские и фармацевтические организации, участвующие в реализации Программы государственных гарантий оказания гражданам бесплатной медицинской помощи, приоритетных национальных проектов и целевых программ в сфере здравоохранения, обеспечении отдельных категорий граждан необходимыми лекарственными средствами;

3) в иных случаях, прямо предусмотренных Федеральным законодательством.

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

6.3. Передача персональных данных гражданина третьим лицам осуществляется на основании запроса третьего лица с разрешающей визой Главного врача Учреждения при условии соблюдения требований, предусмотренных п. 7.1 настоящего Положения.

Учреждение обеспечивает ведение Журнала учета обращений граждан по вопросам обработки персональных данных (Приложение 6) по запросам третьих лиц, в котором регистрируются поступившие запросы, фиксируются сведения о лице, направившем запрос, дата передачи персональных данных, а также отмечается, какая именно информация была передана.

В случае если лицо, обратившееся с запросом, не уполномочено Федеральным законодательством на получение персональных данных гражданина, либо отсутствует письменное согласие гражданина на передачу его персональных данных, Учреждение 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 в Учреждении.

7. Общедоступные источники персональных данных.

7.1. Включение персональных данных гражданина в общедоступные источники персональных данных возможно только при наличии его письменного согласия.

7.2. При обезличивании персональных данных согласие гражданина на включение персональных данных в общедоступные источники персональных данных не требуется.

7.3. Сведения о гражданине могут быть исключены из общедоступных источников персональных данных по требованию самого гражданина, либо по решению суда или иных уполномоченных государственных органов.

8. Обеспечение безопасности персональных данных при их обработке в ИСПДН.

8.1. Методы и способы защиты информации в информационных системах Учреждения.

8.1.1. методы и способы защиты информации, обрабатываемой техническими средствами информационной системы, от несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий (далее — методы и способы защиты информации от несанкционированного доступа);

8.1.2. методы и способы защиты речевой информации, а также информации, представленной в виде информативных электрических сигналов, физических полей, от несанкционированного доступа к персональным данным, результатом которого может стать копирование, распространение персональных данных, а также иных несанкционированных действий (далее — методы и способы защиты информации от утечки по техническим каналам).

Для выбора и реализации методов и способов защиты информации в информационной системе Учреждения может назначаться структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных.

Для выбора и реализации методов и способов защиты информации в информационной системе может привлекаться организация, имеющая оформленную в установленном порядке лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Выбор и реализация методов и способов защиты информации в информационной системе осуществляются на основе определяемых Учреждением угроз безопасности персональных данных (модели угроз) и в зависимости от класса информационной системы, определенных в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным Приказом Федеральной службы по техническому и экспертному контролю, Федеральной службы безопасности Российской Федерации и Министерства информационных технологий и связи Российской Федерации от 13 февраля2008 года№55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных» (зарегистрирован Минюстом России 3 апреля 2008 года, регистрационный № 11462).

Модель угроз разрабатывается на основе методических документов, утвержденных в соответствии с пунктом 2 Постановления Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении положения об обеспечении безопасности персональных данных при обработке в информационных системах персональных данных».

Выбранные и реализованные методы и способы защиты информации в информационной системе должны обеспечивать нейтрализацию предполагаемых угроз безопасности персональных данных при их обработке в информационных системах в составе создаваемой Учреждением системы защиты персональных данных.

Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения технических средств.

Лица, доступ которых к персональным данным, обрабатываемым в информационной системе Учреждения, необходим для выполнения служебных (трудовых) обязанностей,

допускаются к соответствующим персональным данным на основании списка (перечня должностных лиц), утвержденного приказом Главного врача Учреждения.

8.2. Основные мероприятия по организации обеспечения безопасности персональных данных.

Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на предотвращение и (или) минимизацию ущерба от возможной реализации угроз безопасности ПДн.

Обязанности по реализации необходимых организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними в Учреждении возлагаются на ответственного за организацию обработки ПДн и администратора безопасности ИСПДн.

Технические и программные средства, используемые для обработки ПДн в ИСПДн, должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в ИСПДн Учреждения, должны быть в установленном порядке сертифицированы на соответствие требованиям по безопасности информации.

Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных, технических и программных мероприятий, реализуемых в рамках создаваемой системы защиты персональных данных (далее - СЗПДн), 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.

8.3. Этапы осуществления мероприятий по организации обеспечения безопасности персональных данных.

- Обследование и классификация информационной системы персональных данных (ИСПДн);
- Проектирование системы защиты персональных данных;
- Внедрение системы защиты персональных данных;
- Аттестация информационной системы персональных данных на соответствие требованиям.

На этапе обследования ИСПДн проводятся следующие виды работ:

- Сбор необходимых сведений об ИСПДн;

– Анализ способов, режимов, целей и оснований по обработке ПДн;

– Выявление существующих информационно-организационных и технических мер защиты ПДн;

– Разработка организационно-распорядительной документации (ОРД) по обеспечению безопасности ПДн.

На этапе проектирования СЗПДн проводятся следующие виды работ:

– Конкретизация мероприятий и требований по обеспечению безопасности ПДн;

– Выбор способов, мер и классов средств защиты ПДн в соответствии с требованиями по защите.

На этапе внедрения СЗПДн проводятся следующие виды работ:

– Поставка средств защиты информации;

– Внедрение элементов СЗПДн (монтаж, настройка пуско-наладка, испытания средств защиты);

– Опытная эксплуатация средств защиты ПДн в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн.

На этапе аттестации ИСПДн проводятся аттестационные испытания по утвержденной и согласованной программе и методике испытаний, оформляется заключение по результатам проведения аттестации и Аттестат соответствия требованиям по безопасности информации.

8.4. Обязанности сотрудников Учреждения при обработке персональных данных.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документами и базами данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий руководителями и специалистами учреждения. Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

– ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;

– строгое избирательное и обоснованное распределение документов и информации между сотрудниками;

– рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;

– знание сотрудниками требований нормативно–методических документов по защите персональных данных;

– наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;

– определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;

– организация порядка уничтожения информации;

– своевременное выявление нарушения требований разрешительной системы доступа сотрудниками подразделения;

– воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;

– не допускается выдача личных дел сотрудников на рабочие места руководителей. Личные дела могут выдаваться на рабочие места только Главному врачу, и в исключительных случаях, по письменному разрешению Главного врача, руководителю структурного подразделения (виза на служебной записке).

Запрещается передавать информацию, содержащую ПДн, по открытым каналам связи, т.е. без применения соответствующих технических средств защиты и выполнения организационных мер.

Запрещается обрабатывать персональные данные на личных ПЭВМ (ноутбуках) и неучтенных съемных носителях.

Размещение информационных систем, специальное оборудование 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 в эти помещения посторонних лиц.

Для защиты персональных данных создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ и овладеть информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания и реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности Учреждения, посетители, сотрудники других организационных структур.

Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе персонала.

Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим организации;
- порядок охраны территории, здания, помещений, транспортных средств.

Лица, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании раздела 4 настоящего Положения.

Обеспечение безопасности персональных данных при их неавтоматизированной обработке (без использования средств вычислительной техники) осуществляется в соответствии с постановлением Правительства РФ от 15.09.2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

9. Порядок обработки персональных данных без использования средств вычислительной техники

9.1. Обработка персональных данных без использования средств вычислительной техники (далее – неавтоматизированная обработка персональных данных) осуществляется в виде документов на бумажных носителях.

9.2. При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

9.3. При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо несовместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;

– дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

9.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовые формы), должны соблюдаться следующие условия:

– типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

– типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получения письменного согласия на обработку персональных данных;

– типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

– типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо несовместимы.

9.5. 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, вымарывание). Уничтожение персональных данных производится с составлением Акта уничтожения (Приложение 3).

10. Права и обязанности гражданина в области защиты его персональных данных

10.1. В целях обеспечения защиты персональных данных, хранящихся в Учреждении, граждане имеют право на:

– полную информацию о составе и содержимом их персональных данных, а также способе обработки этих данных;

– свободный доступ к своим персональным данным.

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

1) подтверждение факта обработки персональных данных Учреждением;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые Учреждением способы обработки персональных данных;

4) наименование и место нахождения Учреждения, сведения о лицах (за исключением работников Учреждения), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Учреждением 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, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные Федеральным законом № 152-ФЗ или Федеральным законодательством.

Сведения должны быть предоставлены гражданину Учреждением 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 гражданину или его законному представителю Учреждением при обращении, либо при получении запроса гражданина или его законного представителя. Запрос должен содержать номер основного документа, удостоверяющего личность гражданина или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие гражданина в отношениях с Учреждением (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Учреждением, подпись гражданина или его законного представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

В случае если сведения, а также обрабатываемые персональные данные были предоставлены для ознакомления гражданину по его запросу, гражданин вправе обратиться повторно к Учреждению 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.

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

10.2. В случае выявления неправомерной обработки персональных данных при обращении гражданина или его законного представителя, либо по запросу гражданина или его законного представителя, либо уполномоченного органа по защите прав субъектов персональных данных, Учреждение 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) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении гражданина или его законного представителя, либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных, Учреждение 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) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы гражданина или третьих лиц.

10.3. В случае подтверждения факта неточности персональных данных Учреждение на основании сведений, представленных гражданином 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) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

10.4. В случае выявления неправомерной обработки персональных данных, осуществляемой Учреждением (или лицом, действующим по поручению Учреждения), Учреждение в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Учреждения. В случае если обеспечить правомерность обработки персональных данных невозможно, Учреждение 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 обязано уведомить гражданина или его законного представителя, а в случае, если обращение гражданина 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.

10.5. В случае достижения цели обработки персональных данных Учреждение обязано прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) 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 гражданин, иным соглашением между Учреждением и гражданином, либо если Учреждение не вправе осуществлять обработку персональных данных без согласия гражданина на основаниях, предусмотренных Федеральным законом № 152-ФЗ или Федеральным законодательством.

10.6. В случае отзыва гражданином согласия на обработку его персональных данных Учреждение обязано прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению Учреждения) 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) 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 и гражданином, либо если Учреждение не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных Федеральным законом № 152-ФЗ или Федеральным законодательством.

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

10.8. Для своевременной и полной реализации своих прав, гражданин обязан предоставить Учреждению достоверные персональные данные.

10.9. Если гражданин или его законный представитель считает, что Учреждение 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 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.

10.10. Гражданин 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 гражданину 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.

11. Ответственность за нарушение законодательства об охране ПДн

11.1. Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональных данных и является обязательным условием обеспечения эффективности этой системы.

Руководитель, разрешающий доступ сотрудника к персональным данным (конфиденциальному документу), несет персональную ответственность за данное разрешение.

Каждый сотрудник Учреждения, получающий доступ к персональным данным, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

11.2. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

К сотруднику, ответственному за обработку персональных данных, может быть применено одно из дисциплинарных взысканий, предусмотренных ст.192 ТК РФ, а именно: замечание, выговор, увольнение. К дисциплинарной ответственности привлекаются только те работники, которые по условиям своих трудовых договоров обязаны соблюдать правила работы с персональными данными.

К административной ответственности могут быть привлечены как сотрудники, так и организация в целом на основании статей 2.4. КоАП РФ и 13.11. КоАП РФ.

Уголовная ответственность за нарушение неприкосновенности частной жизни предусмотрена статьей 137 УК РФ. В качестве наказания за это преступление предусмотрено наложение штрафа в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо обязательные работы на срок от ста двадцати до ста восьмидесяти часов, либо исправительные работы на срок до одного года, либо арест на срок до четырех месяцев.

Если же преступление совершено с использованием служебного положения, то наказанием может быть штраф в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, лишение права занимать определенные должности или заниматься определенной деятельность на срок от двух до пяти лет, либо арест на срок от четырех до шести месяцев (часть 2 статьи 137 УК РФ).

Приложение 1

Согласие на обработку персональных данных

(в медицинских целях)

Я, нижеподписавшийся(аяся), проживающий(ая) по адресу: _____ _____ паспорт серия _____ номер _____, выдан _____

(наименование выдавшего органа, дата)

в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» подтверждаю свое согласие на обработку ГБУЗ РМ «Республиканская клиническая больница №1» (далее – Оператор), моих персональных данных, включающих: фамилию, имя, отчество, пол, дату и место рождения, адрес места жительства, контактный телефон, паспортные данные, реквизиты полиса ОМС, страховой номер индивидуального лицевого счета в Пенсионном Фонде РФ (СНИЛС), данные о состоянии здоровья, заболеваниях, случаях обращения за медицинской помощью – в медико-профилактических целях, в целях установления медицинского диагноза и оказания медицинских услуг при условии, что обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну.

В процессе оказания мне Оператором медицинской помощи я предоставляю право медицинским работникам передавать мои персональные данные, содержащие сведения, составляющие врачебную тайну, другим должностным лицам Оператора, в интересах моего обследования и лечения.

Предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение. Оператор вправе обрабатывать мои персональные данные посредством внесения их в электронную базу данных, включения в списки (реестры) и отчетные формы, предусмотренные документами, регламентирующими предоставление отчетных данных (документов) по ОМС.

Оператор имеет право во исполнение своих обязательств по работе в системе ОМС на обмен (прием и передачу) моими персональными данными со страховой медицинской организацией _____ и территориальным фондом ОМС с использованием цифровых носителей или по каналам связи, с соблюдением мер, обеспечивающих их защиту от несанкционированного доступа, при условии, что их прием и обработка будут осуществляться лицом, обязанным сохранять профессиональную тайну.

Срок хранения моих персональных данных соответствует сроку хранения первичных медицинских документов и составляет двадцать пять лет для стационара и пять лет для поликлиники.

Передача моих персональных данных иным лицам или иное их разглашение может осуществляться только с моего письменного согласия.

Настоящее согласие дано мной _____и действует бессрочно.

Я оставляю за собой право отозвать свое согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

В случае получения моего письменного заявления об отзыве настоящего согласия на обработку персональных данных, Оператор обязан прекратить их обработку в течение периода времени, необходимого для завершения взаиморасчетов по оплате оказанной мне до этого медицинской помощи.

Контактный телефон _____

Почтовый адрес _____

Дата и подпись субъекта персональных данных «____» _____ 20 ___ г. _____

Приложение 2

Согласие на обработку персональных данных
(в целях исполнения прав и обязанностей сторон трудового договора)

Я, нижеподписавшийся(аяся), проживающий(ая) по адресу: _____ _____ паспорт серия _____ номер _____, выдан _____
(наименование выдавшего органа, дата)
в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 г. №152-ФЗ «О персональных данных» подтверждаю свое согласие на обработку ГБУЗ РМ «Республиканская клиническая больница №1» (далее – Оператор), моих персональных данных, включающих: фамилию, имя, отчество, пол, дату и место рождения, адрес регистрации и фактического проживания, контактный телефон, паспортные данные, реквизиты полиса ОМС, ИНН, страховой номер индивидуального лицевого счета в Пенсионном Фонде РФ (СНИЛС), семейное положение, профессия, доходы, сведения документов воинского учета, данные о состоянии здоровья.

Настоящее согласие предоставляется для реализации целей в результате вступления со мной в трудовые (гражданско-правовые, налоговые, административные и т.п.) правоотношения для использования в управленческой, административной и иной не запрещенной законом деятельности, обеспечения соблюдения требований законов и иных нормативно-правовых актов, а также предоставления сторонним лицам (включая органы государственного и муниципального управления) в рамках требований законодательства Российской Федерации.

Настоящее согласие предоставляется для осуществления Оператором любых действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей, включая (без ограничений) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение, а также осуществление любых иных действий с учетом федерального законодательства.

Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока. Согласие может быть отозвано мною в любое время на основании моего письменного заявления.

Субъект персональных данных:

_____ (_____) «____» _____ 20__ г.

Приложение 3

УТВЕРЖДАЮ
Главный врач
ГБУЗ РМ «Республиканская
клиническая больница №1»
_____Д.А.Амелькин
«____» _____ 20___ г.

АКТ №___
УНИЧТОЖЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

Комиссия, назначенная Приказом от ___.___.20___ г. №____ в составе:

Председатель комиссии:

Члены комиссии:

руководствуясь перечнем документальных материалов и сроками их хранения, составили настоящий акт о том, что «____» _____ 20___ г. произведено уничтожение следующих документов, содержащих персональные данные:

№	№ и дата документа	Наименование документа или дела	№№ экз.	Кол-во листов в экз.	Всего листов
1.					
2.					
3.					
4.					
5.					
6.					

Всего подлежит уничтожению _____ (_____) наименований документов. Записи Акта с учетными данными сверены. После утверждения настоящего Акта, перечисленные документы уничтожили путем _____. Отметки об уничтожении произведены _____ (должность/Ф.И.О.)

Председатель комиссии:
Члены комиссии:

Приложение 4

Журнал учета носителей информации

№ п/п	Рег. номер, дата	Тип/ёмкость машинного носителя персональных данных	Сер. №	Состав ПДН	Место установки (использования)/дата установки	Ответственное должностное лицо (ФИО)	Расписка в получении (ФИО, подпись, дата)	Расписка в обратном приеме (ФИО, подпись, дата)	Место хранения машинного носителя персональных данных	Сведения об уничтожении машинных носителей персональных данных, стирании информации (подпись, дата)
1										
2										
3										

Приложение 5

ЛИСТ ОЗНАКОМЛЕНИЯ

Сотрудников ГБУЗ РМ « Республиканская клиническая больница № 1 » с Положением о защите персональных данных, с инструкцией пользователя информационной системы персональных данных и согласие на работу с персональными данными

№ n/n	ФИО	Должность
	Амелькин Дмитрий Алексеевич	Главный врач
	Зинченко Людмила Николаевна	Заместитель главного врача по медицинской части, заведующая терапевтическим отделением № 1, врач -терапевт
	Ветлова Ольга Валентиновна	Врач - терапевт
	Ефремов Сергей Юрьевич	Заведующий палатой реанимации и интенсивной терапии
	Тесля Валерий Владимирович	Врач – анестезиолог -реаниматолог
	Буткеева Анна Геннадьевна	Врач – анестезиолог - реаниматолог
	Папасов Валерий Федорович	Заведующий хирургическим отделением
	Дерябин Александр Михайлович	Врач - хирург
	Ивенина Ольга Николаевна	Заведующая терапевтическим отделением № 2
	Аленцина Наталия Ивановна	Врач – кардиолог
	Шуляев Сергей Николаевич	Заведующий неврологическим отделением
	Лисюшкина Ирина Геннадьевна	Врач - невролог
	Грибанова Марина Александровна	Заместитель главного врача по поликлиническому разделу
	Кержеманкина Ирина Михайловна	Врач – невролог
	Айзатулова Лидия Михайловна	Врач ультразвуковой диагностики
	Пужаева Екатерина Анатольевна	Врач - эндокринолог
	Антипов Александр Петрович	Врач - хирург
	Милованцева Юлия Александровна	Врач - офтальмолог
	Баранова Ирина Игоревна	Врач- оториноларинголог
	Соколова Лидия Ивановна	Врач -терапевт
	Храмова Марина Владимировна	Врач-акушер-гинеколог
	Кудаева Тамара Владимировна	Заведующая физиотерапевтическим отделением
	Родионова Юлия Владимировна	Заведующая клинико – диагностической лабораторией
	Ермишева Ольга Михайловна	Врач - уролог
	Сипягина Мария Константиновна	Врач функциональной диагностики
	Кирюхина Галина Александровна	Медицинский регистратор
	Жесткова Наталия Александровна	Медицинский регистратор
	Кутьенкова Ольга Петровна	Медицинский регистратор
	Усманова Ленара Раильевна	Медицинская сестра приемного покоя
	Сучкова Ирина Евгеньевна	Заведующий рентгенологическим отделением
	Ягодина Лариса Юрьевна	Главная медицинская сестра
	Кондрашова Юлия Николаевна	Врач-терапевт
	Карповцева Анна Илларионовна	Врач –терапевт участковый
	Мещерякова Наталья Александровна	Врач – терапевт участковый

	Сысуева Галина Рюриковна	Врач –терапевт участковый
	Шемякина Любовь Николаевна	Медицинская сестра участковая
	Рябова Нина Дмитриевна	Медицинская сестра участковая
	Дворецкова Наталья Александровна	Медицинская сестра участковая
	Салькаева Наталья Николаевна	Начальник отдела кадров
	Лашманова Любовь Алексеевна	Медицинский статистик
	Бедина Светлана Васильевна	Медицинский статистик
	Борисова Анна Петровна	Медицинский статистик
	Батырева Любовь Васильевна	Главный бухгалтер
	Янгляева Садия Юнировна	Бухгалтер по учету материальных ценностей
	Марсова Ольга Николаевна	Бухгалтер по учету материальных ценностей
	Комкова Татьяна Андреевна	Заместитель руководителя по экономическим вопросам
	Косолапова Любовь Александровна	Бухгалтер по расчету с рабочими и служащими
	Абрамова Алена Алексеевна	Экономист по финансовой работе
	Штанова Татьяна Васильевна	Старшая медицинская сестра

Приложение 6

Журнала учета обращений граждан по вопросам обработки персональных данных

№ п/п	Сведения о запрашивающем лице	Состав запрашиваемых ПДн	Цель получения ПДн	Отметка о передаче или отказе в передаче ПДн	Дата передачи / отказа в передаче ПДн	Подпись ответственного лица	Примечание

Утверждена постановлением Госкомстата России
От 05.01.2004 г. № 1

Государственное бюджетное учреждение здравоохранения
Республики Мордовия
« Республиканская клиническая больница № 1»

	Код
Форма по ОКУД	0301006
по ОКПО	12345678

Номер документа	Дата
89	09.01.2018

ПРИКАЗ

Во исполнение Федерального закона от 27.07.2006 года № 152 – ФЗ « О персональных данных », с изменениями и дополнениями Федеральный закон от 22 февраля 2017 г. N 16-ФЗ "О внесении изменений в главу 5 Федерального закона "О персональных данных"

ПРИКАЗЫВАЮ:

1. Утвердить Инструкцию пользователя информационных систем персональных данных (Приложение № 1 к настоящему приказу).
2. Утвердить Регламент по учету, хранению и уничтожению носителей персональных данных (Приложение № 2 к настоящему приказу).
3. Утвердить Регламент по допуску сотрудников и третьих лиц к обработке персональных данных (Приложение № 3 к настоящему приказу).
4. Утвердить Регламент по реагированию на запросы субъектов персональных данных (Приложение № 4 к настоящему приказу).
5. Утвердить Регламент по взаимодействию с органами государственной власти в области персональных данных (Приложение № 5 к настоящему приказу).
6. Утвердить Регламент по резервному копированию персональных данных (Приложение № 6 к настоящему приказу).
7. Утвердить Регламент об реагировании на инциденты информационной безопасности (Приложение № 7 к настоящему приказу).
8. Утвердить Регламент по криптографической защите (Приложение № 8 к настоящему приказу).
9. Утвердить Регламент по порядку обезличивания персональных данных (ПДн) в информационной системе персональных данных (Приложение № 9 к настоящему приказу).
10. Утвердить модель угроз безопасности персональных данных при их обработке в информационных данных (Приложение № 10 к настоящему приказу).
11. Утвердить Политику компании в отношении обработки персональных данных (Приложение № 11 к настоящему приказу).
12. Утвердить Положение о защите персональных данных (Приложение № 12 к настоящему приказу).

13. Утвердить Положение об обработке персональных данных (Приложение № 13 к настоящему приказу).
14. Утвердить Инструкцию лица, ответственного за обработку персональных данных (Приложение № 14 к настоящему приказу).
15. Утвердить Инструкцию Администратора информационной безопасности (Приложение № 15 к настоящему приказу).

16. Возложить на Администратора безопасности информационных систем персональных данных функции лица, ответственногоза эксплуатацию средств криптографической защиты информации (далее – СКЗИ).
17. Ответственному за эксплуатацию СКЗИ при организации и обеспечении работы с СКЗИ и криптографическими ключами руководствоваться «Регламентом по обеспечению безопасности использования сертифицированных средств криптографической защиты информации»
18. Менеджеру обработки персональных данных донести до сотрудников, участвующих в обработке персональных данных, правила работы с персональными данными, изложенные в Инструкции пользователя информационных систем персональных данных.
19. Считать утратившим силу приказ главного врача от 09.01.2017 г. № 31/1.
20. Контроль за исполнением настоящего Приказа оставляю за собой.

Главный врач **Д.А. Амелькин**