Приложение № 18

к Приказу № 3-ИБ от 16.01.2017

**ПОЛОЖЕНИЕ**

**об обработке и защите персональных данных пациентов ОГБУЗ «Починковская ЦРБ»**

**I. Общие положения**

1.1. Настоящим Положением определяется порядок получения, обработки, хранения, передачи и любого другого использования персональных данных пациентов, а также ведения их медицинских карт.

1.2. Цель настоящего Положения – обеспечение в соответствии с законодательством Российской Федерации обработки, хранения и защиты персональных данных пациентов, содержащихся в документах, заведенных в ЦРБ, полученных из других организаций, в обращениях граждан.

1.3. Настоящее Положение разработано в соответствии с Конституцией РФ, Федеральным законом от 27.07.06г. № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.06г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 29.07.04г. №98-ФЗ «О коммерческой тайне», Федеральным законом от 22.10.04г. № 125-ФЗ «Об архивном деле в Российской Федерации», законодательством в сфере охране здоровья.

 1.4. В настоящем Положении используются следующие термины и определения:

Оператор персональных данных (далее оператор) - юридическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных. В рамках настоящего положения оператором является ОГБУЗ «Починковская ЦРБ» (далее ЦРБ).

**Субъект персональных данных – далее пациент**. 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.

**Персональные данные (ПД)** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПД), в том числе: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация*,* определяемая нормативно-правовыми актами Российской Федерации в области здравоохранения, Положением об обработке и защите персональных данных и приказами ОГБУЗ «Починковская ЦРБ».

**Обработка персональных данных** – действия (операции) с персональными данными, включая систематизацию, накопление, хранение, комбинирование, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

**Защита персональных данных** – деятельность уполномоченных лиц по обеспечению с помощью локального регулирования порядка обработки персональных данных и обеспечение организационно-технических мер защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения.

**Конфиденциальная информация** – это информация (в документированном или электронном виде), доступ к которой ограничивается в соответствии с законодательством РФ.

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

**Использование персональных данных** - действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

**Блокирование персональных данных** - временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

**Уничтожение персональных данных** - действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

**II. Сбор и обработка персональных данных пациентов**

2.1. Информационные системы классифицируются ЦРБ организующей и (или) осуществляющей обработку персональных данных, а также определяющей цели и содержание обработки персональных данных (далее – ЦРБ), в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности. Сбор и обработка персональных данных осуществляется исключительно с письменного согласия пациента, полученного при заключении договора на оказание медицинских услуг. Образцы форм заявления о согласии на обработку персональных данных и отказа от нее, размещены в Приложении №1, Приложении № 2 и Приложении № 3. Согласие также может быть включено в текст договора на оказание медицинских услуг, при этом подписав договор пациент дает согласие на обработку персональных данных. Персональные данные пациента относятся к конфиденциальной информации.

2.2. В целях обеспечения прав и свобод человека и гражданина ЦРБ и его представители при обработке персональных данных субъекта ПД обязаны соблюдать следующие общие требования:

2.2.1. Обработка персональных данных субъекта может осуществляться исключительно в целях обеспечения личной безопасности сотрудников ЦРБ, количества и качества выполняемой работы, обследования, наблюдения и лечения пациентов и обеспечения сохранности имущества ЦРБ, сотрудника, пациента и третьих лиц.

2.2.2. Обработка персональных данных может осуществляться для статистических или иных научных целей при условии обязательного обезличивания защиты персональных данных.

2.2.3. При определении объема и содержания, обрабатываемых персональных данных ЦРБ руководствуется федеральными законами и локальными документами по данному разделу работы.

2.2.4. Информация о персональных данных пациента предоставляется ЦРБ устно, путем заполнения медицинских карт для пациентов, которые хранятся в регистратуре, лечебных кабинетах и архиве. Если персональные данные пациента возможно получить только у третьей стороны, то пациент должен быть уведомлен об этом и от него должно быть получено письменное согласие (либо письменный отказ). В письменном уведомлении оператор должен сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных (например, оформление запроса в медицинское учреждение о прохождении обследования и лечения и т.п.) и последствиях отказа субъекта дать письменное согласие на их получение.

2.2.5. ЦРБ не имеет права получать и обрабатывать персональные данные субъекта, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений и частной жизни.

2.2.6. ЦРБ не имеет права получать и обрабатывать персональные данные субъекта о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральными законами.

2.2.7. При принятии решений, затрагивающих интересы пациента, ЦРБ не имеет права основываться на персональных данных пациента, полученных исключительно в результате их автоматизированной обработки или электронного получения. При каждом первичном обращении, при заключении договора на оказание медицинской помощи ЦРБ оформляет с пациентом информированное согласие или отказ на обработку персональных данных.

2.3. При приеме к врачу пациент представляет следующие документы, содержащие персональные данные о себе:

- паспорт или иной документ, удостоверяющий личность, гражданство;

- полис ОМС;

- страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС);

* в отдельных случаях с учетом специфики обследования в учреждение здравоохранения действующим законодательством РФ может предусматриваться необходимость предъявления дополнительных документов.
* При оформлении договоров на оказание медицинской помощи в экстренных случаях или повторно постоянному пациенту предъявление документов не обязательно.

2.4. При оформлении документов о временной нетрудоспособности или лечении по полису добровольного медицинского страхования, ЦРБ требует у пациента следующие документы, содержащие персональные данные о себе:

- паспорт или иной документ, удостоверяющий личность;

- страховое свидетельство добровольного медицинского страхования.

2.5. В целях информационного обеспечения в рамках ЦРБ созданы общедоступные источники персональных данных (в том числе справочники, электронные базы). В общедоступные источники персональных данных включены фамилия, имя, отчество, данные паспорта или другого документа, удостоверяющего личность, год рождения, адрес проживания, должность, место работы или учебы, служебные и личные телефоны и адрес электронной почты, информация, изложенная в истории болезни. Вышеперечисленные персональные данные, являются общедоступными и не нуждаются в персональной защите внутри ЦРБ, если пациент дал на это согласие.

2.6. К числу массовых потребителей персональных данных вне учреждения относятся государственные и негосударственные функциональные структуры: налоговые инспекции; правоохранительные органы; органы статистики; страховые агентства; военкоматы; органы социального страхования; пенсионные фонды; подразделения федеральных, областных и муниципальных органов управления. Надзорно - контрольные органы имеют доступ к информации только в сфере своей компетенции, в порядке и на условиях, установленных законодательством РФ.

**III. Хранение и защита персональных данных субъектов персональных данных**

 3.1. Персональные данные субъектов хранятся на бумажных и электронных носителях в регистратуре и кабинетах ЦРБ. Для этого используются специально оборудованные шкафы. Медицинские карты, прошедших обследование, лечение в ЦРБ пациентов хранятся в течении 5 лет с даты последнего посещения в регистратуре, затем передаются в архив ЦРБ для хранения в течении 5 лет. После истечения указанных сроков проводится уничтожение как бумажных, так и электронных носителей в соответствии с локальными документами.

3.2. Конкретные обязанности по ведению, хранению историй болезни пациентов, заполнению, хранению и передаче их и иных документов, отражающих персональные данные пациента, возлагаются на сотрудников ЦРБ, а по хранению и уничтожению историй болезни и иных документов (обследованных, пролеченных) пациентов – на работников регистратуры, что закреплено в должностных инструкциях.

3.3. Персональные данные субъектов хранятся не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в их достижении. Документы, содержащие персональные данные, подлежат хранению и уничтожению в порядке, предусмотренном [архивным законодательством](http://base.garant.ru/12137300.htm#0) Российской Федерации.

3.4. Сведения о пациентах ЦРБ хранятся также на электронных носителях – в базах данных « регистратура», «Дент-офис», « Дигора», Системе электронного документооборота Клиент страховой компании, Электронная отчетность» (передача сведений в виде реестров в страховую компанию.

3.5. При получении сведений, составляющих персональные данные пациентов, заинтересованные лица имеют право получать только те персональные данные, которые необходимы для выполнения конкретных функций и заданий.

3.6. Защита информации о персональных данных.

3.6.1. Сотрудники ЗАО «Стоматологическая ЦРБ №1», имеющие доступ к персональным данным, обязаны принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, модифицирования, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении данной информации.

3.6.2. Сотрудники обеспечивающие электронную информационную защиту принимают следующие меры по защите хранящейся на сервере информации:

- ограничение сетевого доступа на сервер для определенных пользователей;

- организацию в отдельном сегменте сети всех компьютеров пользователей и серверов с ограниченным доступом из локальной сети.

- организацию контроля технического состояния серверов и уровней защиты и восстановления информации;

- проведение регулярного резервного копирования информации;

-ведение аудита действий пользователей и своевременное обнаружение фактов несанкционированного доступа к информации;

3.6.3. Сотрудники ЦРБ, имеющие доступ к персональным данным, при пользовании доступом в сеть Интернет обязаны принимать максимальные меры по обеспечению безопасности:

- установить и использовать антивирусное ПО (с обновлением баз вирусов);

- устанавливать обновление для операционной системы.

3.6.4. Защита персональных данных пациентов в ЦРБ возлагается на:

* главного врача ЦРБ;
* зам. главного врача по экономическим вопросам;
* зам. главного врача по лечебным вопросам;
* зав. структурными подразделениями;
* уполномоченного по информационной безопасности;
* системного администратора
* работников бухгалтерии (ведение документации по учету данных пролеченных пациентов);
* программистов;
* главную и старших медицинских сестер ЦРБ;
* врачей и средний медицинский персонал;
* работников секретариата.

**IV. Передача персональных данных субъектов ПД**

 4.1. При передаче персональных данных субъектов сотрудники ЦРБ, имеющие доступ к персональным данным, должны соблюдать следующие требования:

4.1.1. Не сообщать персональные данные пациента третьей стороне без письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта, а также в других случаях, предусмотренных федеральными законами. Учитывая, что действующее законодательство РФ не определяет критерии ситуаций, представляющих угрозу жизни или здоровью пациента, ЦРБ в каждом конкретном случае делает самостоятельную оценку серьезности, неминуемости, степени такой угрозы. Если же лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных пациента, либо отсутствует письменное согласие пациента на предоставление его персональных сведений, либо, по мнению сотрудника, отсутствует угроза жизни или здоровью пациента, ЦРБ отказывает в предоставлении персональных данных .

4.1.2. Запрещено сообщать персональные данные пациента в коммерческих целях без его письменного согласия.

4.1.3. Предупредить лиц, получающих персональные данные пациента, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено.

 4.1.4. Разрешается доступ к персональным данным пациентов только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные субъектов, которые необходимы для выполнения конкретных функций.

 4.1.5. Все сведения о передаче персональных данных субъекта регистрируются в **Журнале** **учета передачи персональных данных,** в целях контроля правомерности использованияданной информации лицами, ее получившими. В журнале фиксируются сведения о лице, направившим запрос, дата передачи персональных данных или дата уведомления об отказе в их предоставлении, а также отмечается какая именно информация была передана. Форма журнала учета передачи персональных данных представлена в приложении № 5 к настоящему Положению. В случае передачи истории болезни от врача к врачу или из кабинета в кабинет данная передача проводится в интересах пациента **и только через регистратуру.**

 4.2. Требования п.4.1. Положения не подлежат изменению, исключению, так как являются обязательными для медицинской организации и пациентов.

**V. Обязанности пациента и ЦРБ.**

 5.1. В целях обеспечения достоверности персональных данных пациент обязан:

5.1.1. При записи на прием к врачу предоставить ЦРБ полные достоверные данные о себе.

5.1.2. В случае изменения сведений, составляющих персональные данные, пациент должен предоставить данную информацию для внесения изменений.

5.2. ЦРБ обязана:

5.2.1. Осуществлять защиту персональных пациента.

5.2.2. Обеспечить хранение медицинской и др. документации. При этом персональные данные не должны храниться дольше, чем это оправдано выполнением задач, для которых они собирались, или дольше, чем это требуется в интересах лиц, о которых собраны данные.

5.2.3. Заполнение документации, содержащей персональные данные пациента, осуществляется в соответствии с унифицированными формами первичной учетной документации, медицинской документации, утвержденными компетентными органами.

5.2.4. ЦРБ обязана, по письменному заявлению пациента не позднее трех рабочих дней, со дня подачи этого заявления выдать копии документов, связанных с его лечением. Выписку из истории болезни безвозмездно, другие документы на возмездной основе.

5.2.5. Пациенты, их законные представители, а также представители, действующие от их имени по доверенности, должны быть ознакомлены под расписку с документами ЦРБ, устанавливающими порядок обработки персональных данных субъектов, а также их права и обязанности в этой области.

5.2.6. Все сотрудники, имеющие доступ к персональным данным субъектов, обязаны подписать соглашение о неразглашении персональных данных. Форма соглашения о неразглашении персональных данных представлена в приложении № 6 к Положению об обработке персональных данных работников ЗАО «Стоматологическая ЦРБ №1».

**VI. Права субъектов в целях защиты персональных данных**

 6.1. В целях обеспечения защиты персональных данных, хранящихся в ЦРБ, пациенты имеют право на:

6.1.1. Полную и безвозмездную информацию об их персональных данных и обработке этих данных.

6.1.2. Свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные субъекта, за исключением случаев, предусмотренных законодательством РФ..

6.1.3. Определение своих представителей для защиты своих персональных данных.

6.1.4. Требовать об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушениями. При отказе ЦРБ исключить или исправить персональные данные пациента он имеет право заявить в письменной форме ЦРБ о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера пациент имеет право дополнить заявлением, выражающим его собственную точку зрения.

6.1.5. Требовать об извещении ЦРБ всех лиц, которым ранее были сообщены неверные или неполные персональные данные пациента, обо всех произведенных в них исключениях, исправлениях или дополнениях.

6.1.6. Обжалование в суд любых неправомерных действий или бездействий ЦРБ при обработке и защите его персональных данных.

**VII. Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъекта**

7.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных пациента, привлекаются к ответственности в порядке, установленном Трудовым кодексом РФ и иными федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

**VIII. Заключительные положения**

8.1. Настоящее Положение вступает в силу с момента его утверждения главным врачом ЦРБ..

8.2. Настоящее Положение доводится до сведения всех сотрудников ЦРБ под роспись в журнале инструктажа.